Software Engineering Institute
Carnegie Mellon University

Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0

Pamela Curtis
Nader Mehravari
James Stevens

April 2015

TECHNICAL REPORT
CMU/SEI-2015-TR-009

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by Department of Energy under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Energy or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

Table of Contents

List of Figures

List of Tables

Acknowledgements

The Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services) was derived from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [DOE 2014c] and the associated core Model (C2M2) [DOE 2014a]. The original ES-C2M2 was developed in support of a White House initiative led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), and in collaboration with private- and public-sector experts.

The development of this information technology (IT) services variant was sponsored by the DOE Office of Chief Information Officer (OCIO). As for all other variants of the C2M2 family of models, the CERT Division of the Software Engineering Institute (SEI) at Carnegie Mellon University served as the model architect. The DOE OCIO and authors of this variant acknowledge the dedication, technical expertise, and contribution of all the organizations and individuals who participated in the development of the original ES-C2M2 and the core Model (C2M2).

Abstract

Cyber threats are one of the most serious and challenging types of operational risk facing modern organizations. The national and economic security of the United States depends on the reliable functioning of the information technology (IT) services that serve the Nation's critical infrastructure in the face of such threats. Beyond critical infrastructure, the economic vitality of the Nation depends on the sustained operation of enterprise IT services of organizations of all types. This report describes the Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), which helps IT service delivery organizations of all sectors, types, and sizes evaluate and make improvements to their cybersecurity programs.

1 Introduction

Cyber threats are one of the most serious and challenging types of operational risk facing modern organizations. The national and economic security of the United States depends on the reliable functioning of the information technology services that serve the Nation's critical infrastructure in the face of such threats. Beyond critical infrastructure, the economic vitality of the Nation depends on the sustained operation of the enterprise information technology (IT) services of organizations of all types. The Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services) is provided to help IT service delivery organizations of all sectors, types, and sizes evaluate make improvements to their cybersecurity programs.

C2M2 for IT Services focuses on the implementation, management, and assessment of cybersecurity practices associated with typical enterprise IT services, along with related enabling information technology assets and the environments in which they operate. It is based on a combination of existing cybersecurity standards, frameworks, programs, and initiatives. The model can be used to

- strengthen enterprise cybersecurity capabilities
- enable IT service organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities
- share knowledge, best practices, and relevant references across IT service organizations as a means to improve cybersecurity capabilities
- enable IT service organizations to prioritize actions and investments to improve cybersecurity
- enable IT service organizations to communicate capability levels in meaningful terms

C2M2 for IT Services is designed for use with a self-evaluation methodology for an organization to measure and improve its cybersecurity program. A self-evaluation can be completed in one day, but the model could be adapted for a more rigorous evaluation and improvement effort. Additionally, the model can inform the development of a new cybersecurity program.

The model guidance is descriptive rather than prescriptive and is intentionally presented at a high level of abstraction so that it can be interpreted by the IT service delivery units of organizations of various types, structures, sizes, and industries.

1.1 Intended Audience

This document is intended specifically for people in the following organizational roles:

- **Decision makers** (executives) who control the allocation of resources and the management of cybersecurity risk associated with enterprises IT services; these are typically senior leaders
- **Leaders** with responsibility for managing organizational resources and operations associated with the domains of this model as they relate to enterprise IT services (see Section 3.1 for more information on the content of each C2M2 for IT Services 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)

- **Facilitators** with responsibility for leading a self-evaluation of the organization based on this model and analyzing the self-evaluation results

1.1 Document Organization

This document is intended to support enterprises in the effective use of C2M2 for IT Services. It introduces the model and describes its main structure and content.

Stakeholders in the roles described in Section 1.1 may benefit by focusing their attention on specific sections of this document, as outlined in Table 1. Stakeholders may also want to read the domain content for any domain related to their areas of responsibility. Beyond these recommendations, all readers may benefit from understanding the entire document.

Table 1: Recommended Document Sections for Various Organizational Roles

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

Chapter 2 describes several core concepts that are important for interpreting the content and structure of C2M2 for IT Services. Chapter 3 describes the architecture of the model. Chapter 4 provides guidance on how to use the model. Chapter 5 contains the model itself—the model's objectives and practices, organized into 10 domains.

2 Core Concepts

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

2.1 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 represents best practices shared by practitioners of the discipline 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, and 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 for IT Services uses a scale of maturity indicator levels [MILs] 0–3, which are described in Section 3.2.) A set of attributes defines each level; if an organization demonstrates these attributes, it is said to have 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

2.2 C2M2 Constructs

The model makes regular references to the objectives of enterprise IT services and the organizational unit that is responsible for delivery of such services. These objectives include planning, establishing, delivery, monitoring, and maintaining security information technology systems and services for the enterprise (see Figure 1).

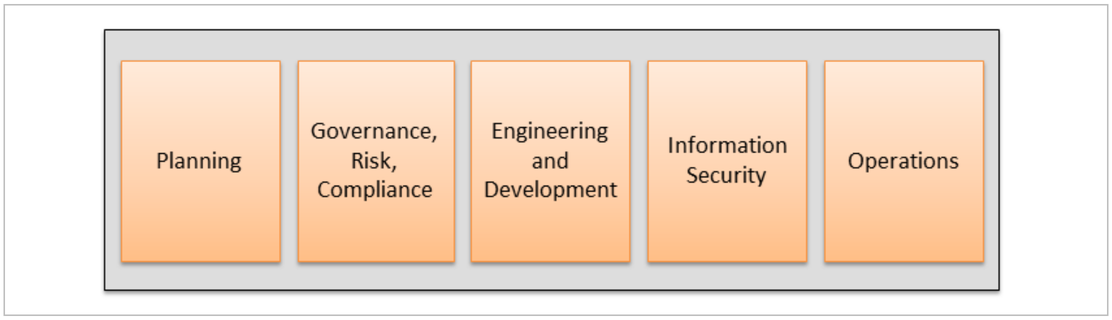


Figure 1: The Enterprise IT Service Delivery Organization

A key tenet of C2M2 for IT Services is the importance of the relationship of an enterprise's mission, the vital IT services that support that mission, and the identification of assets that support those enterprise IT services (see Figure 2). Organizational mission achievement is dependent on vital IT services meeting their missions; IT service delivery mission achievement is dependent on keeping related assets productive; and asset productivity is dependent on preventing exposure to threats and vulnerabilities and making assets sustainable under stress and changing risk conditions. Cybersecurity practices in the model enable organizations to protect and sustain assets in a manner that aligns with their importance in supporting IT service delivery and organization missions.

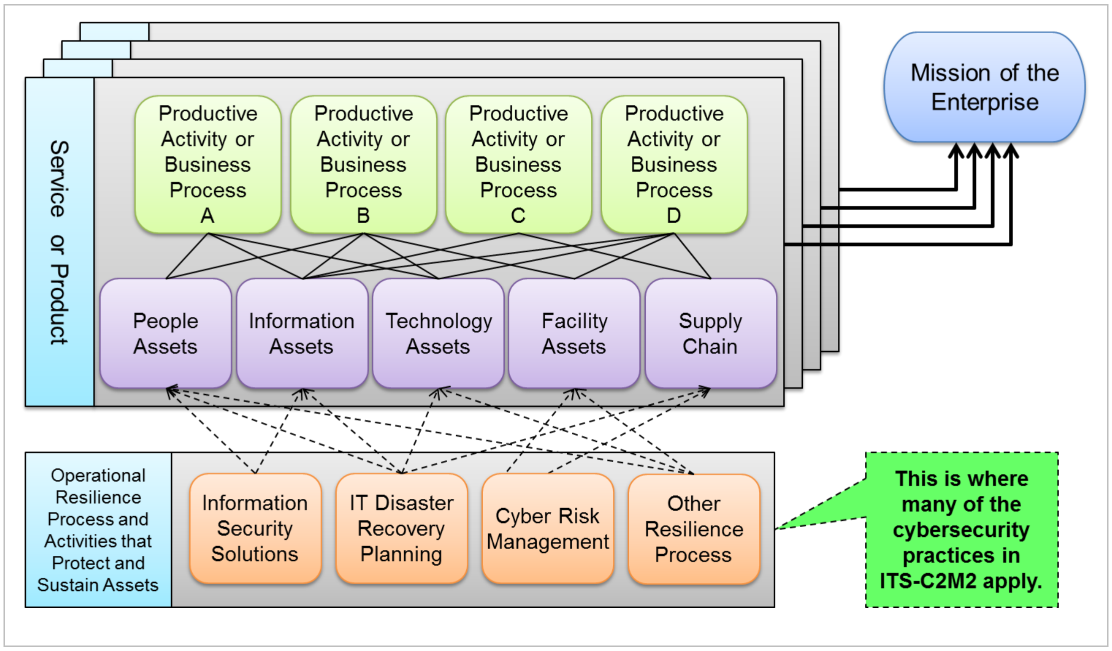

Service or Product
Productive Activity or Business Process A
Productive Activity or Business Process B
Productive Activity or Business Process C
Productive Activity or Business Process D
Mission of the Enterprise
People Assets
Information Assets
Technology Assets
Facility Assets
Supply Chain
Operational Resilience Process and Activities that Protect and Sustain Assets
Information Security Solutions
IT Disaster Recovery Planning
Cyber Risk Management
Other Resilience Process
This is where many of the cybersecurity practices in ITS-C2M2 apply.

Figure 2: Application of Practices in C2M2 for IT Services

Many C2M2 for IT Services practices refer to assets. Generically, the model identifies several key asset types as typical assets that an organization deploys to deliver vital services: people, information, technology, facilities, and externally supplied assets as shown in Figure 2. Information and technology assets are a particular focus of the model. Information assets could be digital (e.g., stored in a computer system), physical (e.g., written on a piece of paper), or logical (e.g., what we store in our brains). Information assets could represent operational data, intellectual property, customer information, contracts, and any other type of information that is of value to the enterprise and/or critical to delivery of services. Technology assets range from individual hardware, software, or firmware components used by the organization in the delivery of services to complex systems made up of many individual components. When evaluating how completely a practice is performed, it is important to consider both traditional and emerging enterprise IT assets.

2.3 Relationship to Risk Management Activities

The phrase "commensurate with risk to critical infrastructure and organizational objectives" is used throughout the model. This phrase is included to remind the organization to tailor its implementation of the model content to address its unique risk profile. This supports the model's intent of providing descriptive rather than prescriptive guidance. To effectively follow this guidance, the organization should use the model as part of a continuous enterprise risk management process.

The C2M2 for IT Services Risk Management domain (see Section 5.1) suggests establishing a cybersecurity risk management strategy that aligns with the enterprise risk management strategy. Cybersecurity risk is an important component of the overall business risk environment. The model's cybersecurity risk management activities should align with and support the enterprise risk management strategy and program so that cybersecurity risk is considered in and benefits from corporate decisions based on risk impact, tolerance for risk, and risk response approaches.

The implementation of practices in the Risk Management domain provides supporting elements that are used by other practices in the model as part of the overall risk management process. Throughout the model, these Risk Management practices are referenced in related practices using the notation described in Section 3.3.

3 Model Architecture

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

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

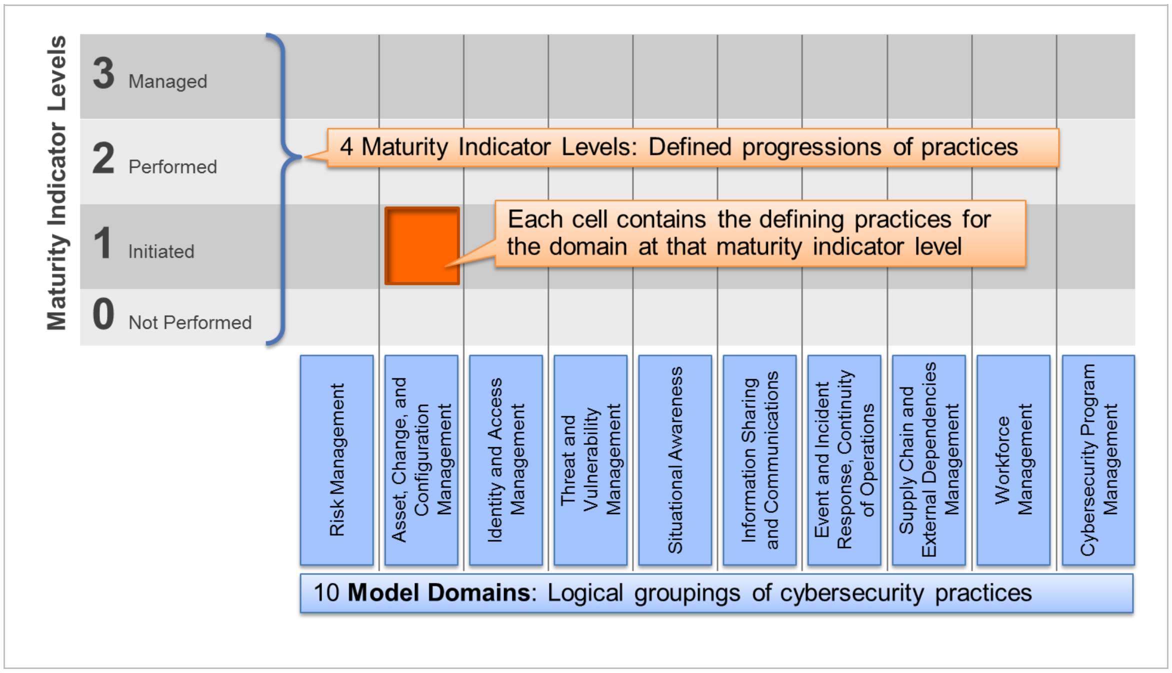

Maturity Indicator Levels
3 Managed
2 Performed
1 Initiated
0 Not Performed
4 Maturity Indicator Levels: Defined progressions of practices
Each cell contains the defining practices for the domain at that maturity indicator level
Risk Management
Asset, Change, and Configuration Management
Identity and Access Management
Threat and Vulnerability Management
Situational Awareness
Information Sharing and Communications
Event and Incident Response, Continuity of Operations
Supply Chain and External Dependencies Management
Workforce Management
Cybersecurity Program Management
10 Model Domains: Logical groupings of cybersecurity practices

Figure 3: C2M2 for IT Services Model Architecture

3.1 Domains

Each of the model's 10 domains is 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 a cybersecurity risk management capability.

For each domain, the model provides a purpose statement, which is a high-level summary of intent of the domain, followed by introductory notes, which give context for the domain and introduce its practices and its abbreviation. (The abbreviation for the Risk Management domain, for example, is RM.) The purpose statement and introductory notes provide context for interpreting the practices in the domain.

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

- Establish Cybersecurity Risk Management Strategy
- Manage Cybersecurity Risk
- Institutionalization Practices

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL.

Figure 4 summarizes the elements of each domain.

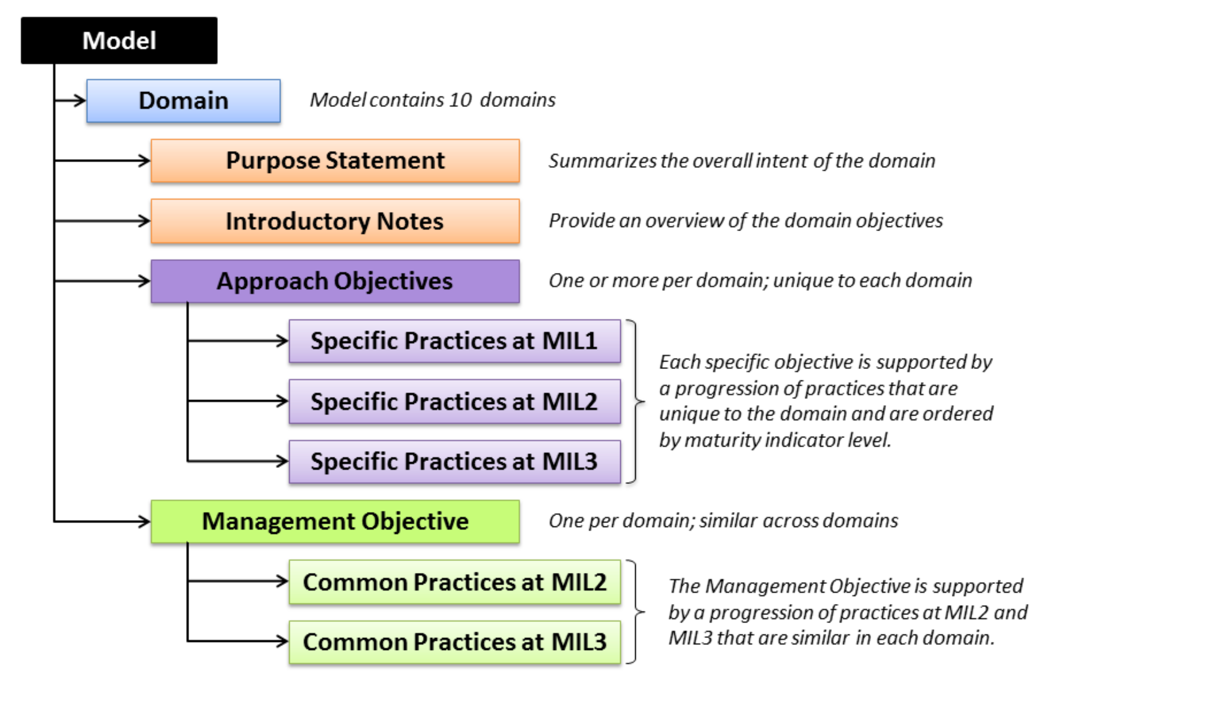

Model
Domain
Model contains 10 domains
Purpose Statement
Summarizes the overall intent of the domain
Introductory Notes
Provide an overview of the domain objectives
Approach Objectives
One or more per domain; unique to each domain
Specific Practices at MIL1
Specific Practices at MIL2
Specific Practices at MIL3
Each specific objective is supported by a progression of practices that are unique to the domain and are ordered by maturity indicator level.
Management Objective
One per domain; similar across domains
Common Practices at MIL2
Common Practices at MIL3
The Management Objective is supported by a progression of practices at MIL2 and MIL3 that are similar in each domain.

Figure 4: Model and Domain Elements

The 10 domains are briefly described below in the order in which they appear in the model.

Risk Management (RM)

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

Asset, Change, and Configuration Management (ACM)

Manage the organization’s information technology assets, including both hardware and software, commensurate with the risk to the enterprise and its mission.

Identity and Access Management (IAM)

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 the enterprise and its mission.

Threat and Vulnerability Management (TVM)

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 the enterprise and its mission.

Situational Awareness (SA)

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

Information Sharing and Communications (ISC)

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including information about threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to the enterprise and its mission.

3.2 Event and Incident Response, Continuity of Operations (IR)

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 the enterprise and its mission.

Supply Chain and External Dependencies Management (EDM)

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 the enterprise and its mission.

Workforce Management (WM)

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 the enterprise and its mission.

Cybersecurity Program Management (CPM)

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 organizational and enterprise strategic objectives and the risk to the enterprise and its mission.

3.3 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 an institutionalization progression, which are explained in the following sections.

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

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

3.3.1 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.

Table 2 provides an example of the approach progression in the Cyber 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, alignment with the overall organization’s strategy, and approval of senior management. 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 Cyber Program Management Domain

MIL0	
MIL1	a. The organization has a cybersecurity program strategy
MIL2	b. The cybersecurity program strategy defines objectives for the organization’s cybersecurity activities c. The cybersecurity program strategy and priorities are documented and aligned with the organization’s strategic objectives and risk to critical infrastructure d. The cybersecurity program strategy defines the organization’s approach to provide program oversight and governance for cybersecurity activities e. The cybersecurity program strategy defines the structure and organization of the cybersecurity program f. The cybersecurity program strategy is approved by senior management
MIL3	g. The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)

3.3.2 Institutionalization Progression

Institutionalization describes the extent to which a practice or activity is ingrained in an organization’s operations. 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 institutionalization 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 Institutionalization Practices. The progression of the practices within any domain-specific objective corresponds to the progression of the institutionalization practices, though not necessarily practice to practice. Table 3 shows an example mapping of the institutionalization practices to the practices in the second objective of the Risk Management domain.

Table 3: Mapping of Institutionalization Practices to Domain-Specific Practices

	2 Manage Enterprise Cybersecurity Risk	**Institutionalization Practices**
MIL0		
MIL1	a. Cybersecurity risks are identified, at least in an ad hoc manner b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner	1. Initial practices are performed but may be ad hoc
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy d. Identified risks are documented e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy f. Identified risks are monitored in accordance with the risk management strategy g. Current network architecture documentation is used to support risk analysis	1. Practices are documented 2. Stakeholders of the practice are identified and involved 3. Adequate resources are provided to support the process (people, funding, and tools) 4. Standards, guidelines, and best practices have been identified to guide the implementation of the practices
MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy i. Current cybersecurity architecture documentation is used to support risk analysis j. A risk register (a structured repository of identified risks) is used to support risk management activities	1. Activities are guided by policies (or other organizational directives) and governance 2. Policies include compliance requirements for specified standards, guidelines, and best practices 3. Activities are periodically reviewed to ensure they conform to policy 4. Responsibility and authority for performing the practices are assigned to personnel 5. Personnel performing the practices have adequate skills and knowledge

The management practices of each MIL are described below.

3.3.3 MIL Characteristics

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)

In each domain, MIL1 contains a set of initial practices. 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.

MIL1 is characterized by a single management practice:

1. **Initial practices are performed but may be 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 quality of the outcome may vary significantly depending on who performs the practice, when it is performed, and 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.

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. **Stakeholders of practices are identified and involved.** Stakeholders of practices are identified and involved in the performance of the practices. This could include stakeholders from within the function, from across the organization, or from outside the organization, depending on how the organization implemented the practice.
3. **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.
4. **Standards, guidelines, and best practices have been identified to guide the implementation of the practices.** The organization identified some standards, guidelines, and best practices to inform the implementation of practices in the domain. These may simply be the reference sources the organization consulted when developing the plan for performing the practices.

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. Five management practices support this progression:

1. **Activities are guided by policies (or other organizational directives) and governance.** Managed activities in a domain receive guidance from the organization in the form of organizational direction, as in policies and governance. Policies are an extension of the planning activities that are in place at MIL2.
2. **Policies include compliance requirements for specified standards, guidelines, and best practices**.
3. **Activities are periodically reviewed to ensure they conform to policy.**
4. **Responsibility and authority for performing the practices are assigned to personnel.**
5. **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.

At MIL3, the practices in a domain are further stabilized and are guided by high-level organizational directives, such as policy. 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.

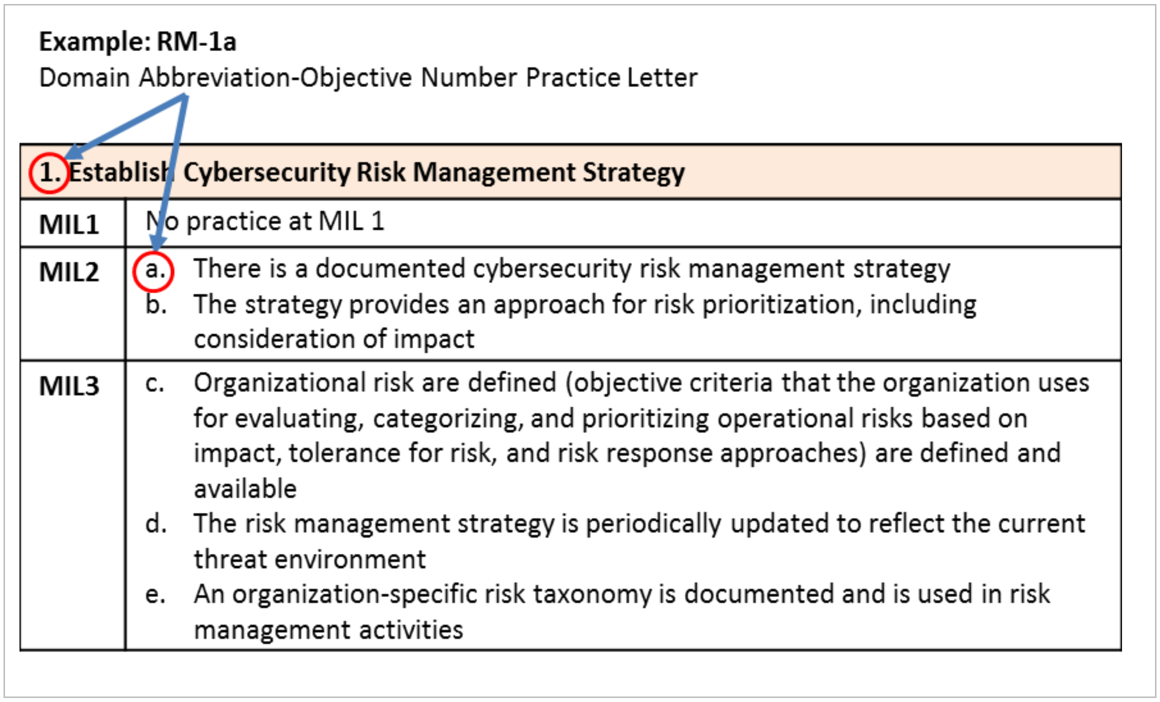
Table 4 summarizes the characteristics of each MIL. At MIL2 and MIL3, the characteristic associated with the approach progression is distinguished from the characteristics associated with the institutionalization progression.

Table 4: Summary of Maturity Indicator Level Characteristics

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	*Institutionalization characteristics* • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation *Approach characteristic* • Practices are more complete or advanced than at MIL1
MIL3	*Institutionalization characteristics* • Activities are guided by policy (or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are assigned to personnel • Personnel performing the practice have adequate skills and knowledge *Approach characteristic* • Practices are more complete or advanced than at MIL2

3.4 Practice Reference Notation

A number of practices within the domains are connected to other model practices. When this occurs, the connecting practice is referenced using a notation that begins with the domain abbreviation, a hyphen, the objective number, and the practice letter. Figure 5 shows an example from the Risk Management domain: the domain's first practice, "There is a documented cybersecurity risk management strategy," would be referenced elsewhere in the model using the notation "RM-1a."



Example: RM-1a

Domain Abbreviation-Objective Number Practice Letter

1. Establish Cybersecurity Risk Management Strategy	
MIL1	No practice at MIL 1
MIL2	a. There is a documented cybersecurity risk management strategy b. The strategy provides an approach for risk prioritization, including consideration of impact
MIL3	c. Organizational risk are defined (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available d. The risk management strategy is periodically updated to reflect the current threat environment e. An organization-specific risk taxonomy is documented and is used in risk management activities

Figure 5: Example of Referencing an Individual Practice

4 Using the Model

The C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. Figure 6 summarizes 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 in an organization and provide additional details on the activities in each step of this approach.

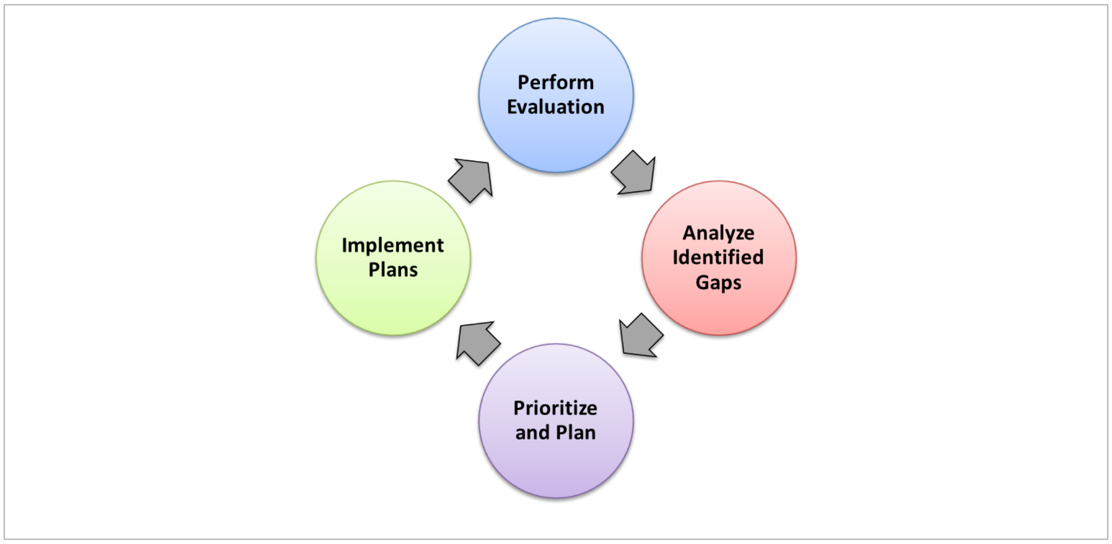


Figure 6: Recommended Approach for Using the Model

4.1 Prepare to Use the Model

A design goal of the model was to enable organizations to complete a self-evaluation for a single organization in one day without extensive study or preparation. This goal can be 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.

Another important component of successfully completing the self-evaluation in one day is the selection of an effective facilitator. Generally speaking, a C2M2 for IT Services facilitator is not only someone who is familiar with the model and its supporting artifacts but also someone 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 the survey scope—the IT service delivery organization and the corresponding assets to which the model and survey will be applied. Though C2M2 for IT Services and its supporting survey could apply to all IT service organizations in an entire enterprise, the self-evaluation survey is typically applied to a single organization to maintain focus. (See Figure 7 for examples of types of IT service organizations within a large enterprise. For some organizations using the model, the "enterprise" might be a cooperative or a national laboratory.) Selecting and documenting the scope before completing the survey ensures that users of the survey results understand to which organization the results apply.

The scoping discussion should also include consideration of assets to which the model and survey will be applied. For example, does the survey only pertain to information and technology assets that are owned and operated by the organization being evaluated or does it also include information and technology assets that are owned and managed by others but reside in the environment that is managed by the organization under review? (The latter assets may have an adverse effect on the cybersecurity properties of the environment.) The scooping discussion would also benefit from touching upon things that are explicitly *not* included in the scope.

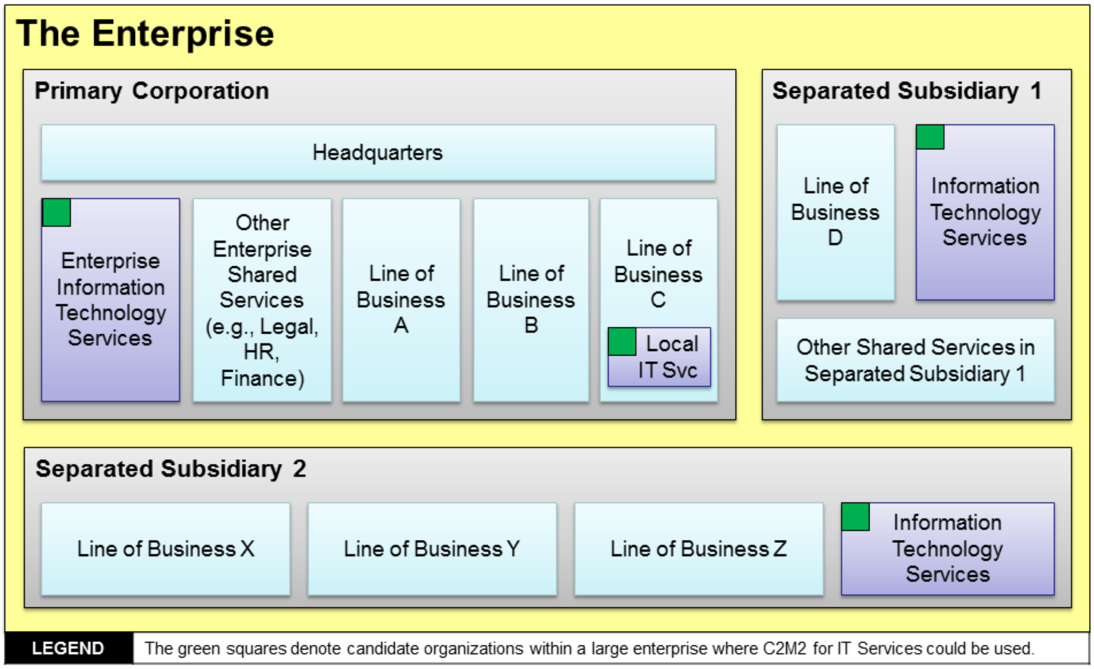

The Enterprise
Primary Corporation
Headquarters
Enterprise Information Technology Services
Other Enterprise Shared Services (e.g., Legal, HR, Finance)
Line of Business A
Line of Business B
Line of Business C
Local IT Svc
Separated Subsidiary 1
Line of Business D
Information Technology Services
Other Shared Services in Separated Subsidiary 1
Separated Subsidiary 2
Line of Business X
Line of Business Y
Line of Business Z
Information Technology Services
LEGEND
The green squares denote candidate organizations within a large enterprise where C2M2 for IT Services could be used.

Figure 7: Examples of IT Service Organizations in a Large Enterprise

More thorough guidance on using the model, selecting a facilitator, scoping an evaluation, conducting the evaluation, and scoring and reporting results can be found in the supporting *C2M2 Facilitator Guide* [DOE 2014b].

4.2 Perform an Evaluation

The organization should select the appropriate personnel to evaluate the function in scope against the model practices. Participation by a broad representation across the parts of the organization being evaluated yields the best results and enables internal information sharing about the model practices. Personnel selected to participate in the evaluation should include operational personnel, management stakeholders, and any others who could provide useful information on the organization's performance of cybersecurity practices in the model.

Upon completion of the evaluation, a scoring report is generated that shows maturity indicator level results for each domain. This report provides a picture of the current state of practices relative to the model for the unit evaluated. The report should be reviewed with the evaluation workshop participants, and any discrepancies or questions should be addressed.

4.3 Analyze Identified Gaps

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

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

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

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

4.4 Prioritize and Plan

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

Next, a plan should be developed to address the selected gaps. The plan can span a period of weeks, months, or years, depending on the extent of improvements needed to close the selected gaps and achieve the desired capability.

4.5 Implement Plans and Periodically Reevaluate

Plans developed in the previous step should be implemented to address the identified gaps. Model evaluations are particularly useful in tracking implementations and should be conducted periodically to ensure that desired progress is achieved. Reevaluations should also be considered in response to major changes in the business, technology, market, or threat environments to ensure that the current profile matches the organization's desired state.

Table 5 presents a more detailed outline of the C2M2 process as described in this chapter.

Table 5: Recommended Process for Using Evaluation Results

	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	Prioritized implementation plan	1. Track progress to plan 2. Re-evaluate periodically or in response to major change	Project tracking data

5 Model Domains

5.1 Risk Management

Purpose: Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the enterprise and its mission, 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 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 (RM) domain comprises three objectives:

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

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 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.

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. maintains a network architecture diagram that identifies critical assets and shows how they 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. Anywhere Inc. augments the risk assessment derived from the network architecture with its cybersecurity architecture. Since their network diagram includes elements like firewalls and intrusion detection devices, an asset's base risk is refined depending on how it is protected by security controls.

Risk for each IT asset is determined from a combination of the asset's importance in delivering essential IT services and its exposure based on the network and cybersecurity architectures.

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, including Event and Incident Response, Continuity of Operations, Threat and Vulnerability Management, and Situational Awareness, refer to the risk register and illustrate how the practices in the model are strengthened as they connect through a cybersecurity risk management program.

RISK MANAGEMENT **Objectives and Practices**		
1. Establish Enterprise Cybersecurity Risk Management Strategy		
MIL1		No practice at MIL1
MIL2	a.	There is a documented cybersecurity risk management strategy
MIL2	b.	The strategy provides an approach for risk prioritization, including consideration of impact and resource requirements
MIL3	c.	Organizational risk criteria (criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available
MIL3	d.	The risk management strategy is periodically updated to reflect the current threat environment
MIL3	e.	An organization-specific risk taxonomy is documented and is used in risk management activities
2. Manage Enterprise Cybersecurity Risk		
MIL1	a.	Cybersecurity risks are identified, at least in an ad hoc manner
	b.	Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner
MIL2	c.	Risk assessments are performed to identify risks in accordance with the risk management strategy
MIL2	d.	Identified risks are documented
MIL2	e.	Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy
MIL2	f.	Identified risks are monitored in accordance with the risk management strategy
MIL2	g.	Current network and/or system architecture documentation is used to support risk analysis
MIL3	h.	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy
MIL3	i.	Current cybersecurity architecture documentation is used to support risk analysis
MIL3	j.	A risk register (a structured repository of identified risks) is used to support risk management activities
3. Institutionalization Activities for RM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for risk management activities
MIL2	b.	Stakeholders for risk management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support risk management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform risk management activities

RISK MANAGEMENT **Objectives and Practices**		
MIL3	e.	Risk management activities are guided by documented policies or other organizational directives
MIL3	f.	Risk management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Risk management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of risk management activities are assigned to personnel
MIL3	i.	Personnel performing risk management activities have the skills and knowledge needed to perform their assigned responsibilities

5.2 Asset, Change, and Configuration Management

Purpose: Manage the organization’s information technology assets, including both hardware and software, commensurate with the risk to the enterprise and its mission.

An asset is something of value to an organization. For the purposes of this model, assets to be considered are information technology hardware and software assets, as well as information essential to operating enterprise IT services.

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

1. Manage Asset Inventory
2. Manage Asset Configuration
3. Manage Changes to Assets
4. Institutionalization Activities

An inventory of assets important to the delivery of enterprise IT services 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 technology assets and ensuring that assets are configured according to the baseline. Most commonly, this practice applies to ensuring that similar assets are configured in the same way. However, in cases where assets are either unique or must have individual configurations, managing asset configuration involves controlling the configuration baseline of the asset when it is deployed for operation and ensuring that the asset remains configured according to the baseline.

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

Example

Asset Change and Configuration Management

Anywhere Inc. is consolidating multiple information repositories into a single IT asset database that will be maintained by the enterprise IT service organization. Within this database, information and technology assets will be identified and prioritized based on importance to the delivery of enterprise IT services. The database will eventually include 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. This information is lacking for many of the IT assets that will be included in the database, but a plan is being developed to identify and capture missing information as the system is deployed.

Anywhere Inc. will use this information for cybersecurity risk management activities, including identifying which IT systems may be affected by software vulnerabilities, prioritizing cybersecurity incident response, and planning disaster recovery. At this time, much of this information has to be gathered during an event, which has led to delays and inconsistencies in response.

To maintain change traceability and consistency, Anywhere Inc.’s change management activities will require that the asset database remain current as configurations change. The new change management process ensures that all important decisions about assets are communicated to stakeholders, including the asset owner, so that potential impacts to the IT service delivery are efficiently managed.

ASSET, CHANGE, AND CONFIGURATION MANAGEMENT **Domain Objectives and Practices**		
1. Manage Asset Inventory		
MIL1	a.	There is an inventory of technology assets (e.g., computers and telecommunication equipment, data centers, and emergency power generators) that are important to the delivery of IT services; management of the inventory may be ad hoc
MIL1	b.	There is an inventory of information assets (e.g., customer information, financial data, and configuration items) that are important to the delivery of IT services; management of the inventory may be ad hoc
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)
MIL2	d.	Inventoried assets are prioritized based on their importance to the delivery of IT services
MIL3	e.	The asset inventory describes (physical and logical) connections among technology assets
MIL3	f.	The asset inventory is current (as defined by the organization) at least for assets of importance to enterprise IT services
2. 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
MIL1	b.	Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment
MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configurations of assets are monitored for consistency with baselines throughout the assets' lifecycles
MIL3	e.	Configuration baselines are reviewed and updated at an organization-defined frequency
3. Manage Changes to Assets		
MIL1	a.	Proposed changes to inventoried assets are evaluated, at least in an ad hoc manner, before being implemented
MIL1	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
MIL2	d.	Change management practices address the full lifecycle of assets (i.e., acquisition, deployment, operation, retirement)
MIL3	e.	Changes to assets are tested for cybersecurity impact prior to being deployed
MIL3	f.	Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)
4. Institutionalization Activities for ACM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for asset inventory, configuration, and change management activities
MIL2	b.	Stakeholders for asset inventory, configuration, and change management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform asset inventory, configuration, and change management activities
MIL3	e.	Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives

ASSET, CHANGE, AND CONFIGURATION MANAGEMENT **Domain Objectives and Practices**		
MIL3	f.	Asset inventory, configuration, and change management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel
MIL3	i.	Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities

5.3 Identity and Access Management

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

For the purposes of this domain, access control applies to logical access to assets used in the delivery of enterprise IT services, physical access to cyber assets relevant to enterprise IT services, and automated access control systems (logical or physical) relevant to enterprise IT services. 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 (IAM) domain comprises three objectives:

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

Establishing and maintaining identities begins with the provisioning and deprovisioning of identities to entities. Entities may include individuals (internal or external to the organization), 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 (removing available identities when they are no longer required).

Example
Identity and Access Management

Anywhere Inc. decides to upgrade its IT service platforms from multiple identity and access management (IAM) systems to a single sign-on system that is capable of supporting multifactor authentication. The organization believes that reducing the number of IAM systems that it manages and increasing the authentication capability 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 current 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.

It 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 preplanned 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 enterprise IT services, and regular reviews of access are conducted.

IDENTITY AND ACCESS MANAGEMENT **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)
MIL1	b.	Credentials (e.g., passwords, smart cards, certificates, keys, lock combinations) are issued to identities that require access to assets, at least in an ad hoc manner
MIL1	c.	Identities are deprovisioned and credentials revoked, at least in an ad hoc manner, when no longer required
MIL2	d.	Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)
MIL2	e.	Credentials are periodically reviewed to ensure that they are associated with the correct person or entity
MIL2	f.	Identities are deprovisioned within organization-defined time thresholds when no longer required
MIL3	g.	Requirements for credentials are informed by the organization’s risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)
2. Control Access		
MIL1	a.	Access requirements, including those for remote access, are determined, at least in an ad hoc manner (i.e., 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)
MIL1	b.	Access is granted, at least in an ad hoc manner, to identities based on requirements
MIL1	c.	Access is revoked, at least in an ad hoc manner, when no longer required
MIL2	d.	Access requirements incorporate least privilege and separation of duties principles
MIL2	e.	Access requests are reviewed and approved by the asset owner
MIL2	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 validity, at an organization-defined frequency
MIL3	h.	Access to assets is granted by the asset owner based on risk to IT services
MIL3	i.	Anomalous access attempts are monitored as indicators of cybersecurity events
3. Institutionalization Activities for IAM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed to establish and maintain identities and control access
MIL2	b.	Stakeholders for identity and access management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support identity and access management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform identity and access management activities
MIL3	e.	Identity and access management activities are guided by documented policies or other organizational directives
MIL3	f.	Identity and access management policies include compliance requirements for specified standards, guidelines, and best practices

IDENTITY AND ACCESS MANAGEMENT **Objectives and Practices**		
MIL3	g.	Identity and access management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of identity and access management activities are assigned to personnel
MIL3	i.	Personnel performing identity and access management activities have the skills and knowledge needed to perform their assigned responsibilities

5.4 Threat and Vulnerability Management

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

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 technology or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, and/or denial of IT service. Threats to technology and communication infrastructure assets are varied and may include malicious actors, malware (e.g., viruses and worms), Distributed Denial of Service (DDoS) attacks, and the like.

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

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

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

Threat identification and response begins with collecting useful threat information from reliable sources, interpreting that information in the context of the organization and enterprise IT services, 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 enterprise IT services (see the example in Table 6). 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 COP described in the Situational Awareness domain.

Example
Threat and Vulnerability Management

Anywhere Inc. has 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 and document a threat profile for Anywhere Inc.'s enterprise IT services. Anywhere Inc. has identified reliable sources of information to enable rapid threat identification and is able to consume and analyze published threat information to begin effective response, from sources such as the United States Computer Emergency Readiness Team (US-CERT), industry associations, and vendors.

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.

Table 6: Threat Profile Example

Asset	Access Type	Actor	Motive	Outcome
Server baseline configurations	Network access	Outsider	Deliberate	Server configuration details disclosed
		Outsider	Deliberate	Server configuration information is lost
	Physical access	Insider	Accidental	Server configuration information is corrupted
		Insider	Deliberate	Server configuration information is corrupted

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 enterprise IT services. Vulnerabilities may be addressed by implementing mitigating controls, monitoring threat status, or applying cybersecurity patches, or through other activities.

THREAT AND VULNERABILITY MANAGEMENT **Objectives and Practices**		
1. Identify and Respond to Threats		
MIL1	a.	Information sources to support threat management activities are identified (e.g., US-CERT, industry associations, vendors, federal briefings), at least in an ad hoc manner
MIL1	b.	Cybersecurity threat information is gathered and interpreted for IT services, at least in an ad hoc manner
MIL1	c.	Threats that are considered important to IT services are addressed (e.g., implement mitigating controls, monitor threat status), at least in an ad hoc manner
MIL2	d.	A threat profile for IT services is established that includes characterizations of likely intent, capability, and targets
MIL2	e.	Threat information sources that address all components of the threat profile are prioritized and monitored
MIL2	f.	Identified threats are analyzed and prioritized
MIL2	g.	Threats are addressed according to the assigned priority
MIL3	h.	The threat profile for IT services is validated at an organization-defined frequency
MIL3	i.	Analysis and prioritization of threats are informed by the defined risk criteria (RM-1c)
MIL3	j.	Threat information is added to the risk register (RM-2j)
2. Reduce Cybersecurity Vulnerabilities		
MIL1	a.	Information sources to support cybersecurity vulnerability discovery are identified (e.g., US-CERT, industry associations, vendors, federal briefings), at least in an ad hoc manner
MIL1	b.	Cybersecurity vulnerability information is gathered and interpreted for IT services, at least in an ad hoc manner
MIL1	c.	Cybersecurity vulnerabilities that are considered important to IT services are addressed (e.g., implement mitigating controls, apply cybersecurity patches, plan for software end of life), at least in an ad hoc manner
MIL2	d.	Cybersecurity vulnerability information sources that address all assets important to IT services are monitored

THREAT AND VULNERABILITY MANAGEMENT **Objectives and Practices**		
MIL2	e.	Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification using specialized tools)
MIL2	f.	Identified cybersecurity vulnerabilities are analyzed and prioritized (e.g., NIST Common Vulnerability Scoring System could be used for software vulnerabilities)
MIL2	g.	Cybersecurity vulnerabilities are addressed according to the assigned priority
MIL2	h.	Operational impact to IT services is evaluated prior to deploying cybersecurity patches
MIL3	i.	Cybersecurity vulnerability assessments are performed for all assets important to the delivery of IT services, at an organization-defined frequency
MIL3	j.	Cybersecurity vulnerability assessments are informed by the defined risk criteria (RM-1c)
MIL3	k.	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of IT services
MIL3	l.	Analysis and prioritization of cybersecurity vulnerabilities are informed by the defined risk criteria (RM-1c)
MIL3	m.	Cybersecurity vulnerability information is added to the risk register (RM-2j)
MIL3	n.	Risk monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches)
3. Institutionalization Activities for TVA Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for threat and vulnerability management activities
MIL2	b.	Stakeholders for threat and vulnerability management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support threat and vulnerability management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform threat and vulnerability management activities
MIL3	e.	Threat and vulnerability management activities are guided by documented policies or other organizational directives
MIL3	f.	Threat and vulnerability management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Threat and vulnerability management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of threat and vulnerability management activities are assigned to personnel
MIL3	i.	Personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities

5.5 Situational Awareness

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

Situational awareness involves developing near-real-time knowledge of a dynamic operating environment. In part, this is accomplished through the logging and monitoring of information technology infrastructure assets essential for the delivery of enterprise IT services. It is equally important to maintain knowledge of relevant, current cybersecurity events external to the enterprise. Once an organization develops a common operating picture (COP), 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 (SA) domain comprises four objectives:

1. Perform Logging
2. Perform Monitoring
3. Establish and Maintain a Common Operating Picture
4. Institutionalization Activities

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

The condition of assets, as discovered through monitoring, contributes to an operating picture. Effectively communicating the operating picture to relevant decision makers is the essence of a COP. While many implementations of a COP may include visualization tools (e.g., dashboards, maps, and other graphical displays), they are not necessarily required to achieve the goal. Organizations may use other methods to share IT services' current state of cybersecurity.

Example
Situational Awareness

Anywhere Inc. has determined that indicators of an emerging threat often reside in different parts of the organization. Building security staff track visitors, the help desk 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 its own data, and produces a COP for the rest of the organization. This COP is a simple heat map that summarizes the current state of operations across the organization using a color-coded scale and is continuously displayed on a monitor in the IT operations centers as well as on the corporate intranet site.

When the COP suggests a need for heighted security (for example, the FBI has reported increasing interest from criminal groups in organizations like Anywhere, Inc. and the network operations center is reporting unusual amounts of off-hour network scanning activity), the organization responds. Visitors are screened more carefully, the help desk conducts malware scans on misbehaving laptops, HR sends out reminders about phishing, and network logs are reviewed more frequently and thoroughly.

Senior management reviews the COP and is prepared should extraordinary action—such as shutting down the enterprise 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.

SITUATIONAL AWARENESS **Objectives and Practices**		
1. Perform Logging		
MIL1	a.	Logging is occurring, at least in an ad hoc manner, for assets important to IT services where possible
MIL2	b.	Logging requirements have been defined for all assets important to IT services (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])
MIL2	c.	IT services' log data are being aggregated
MIL3	d.	Logging requirements are based on the risk to IT services
MIL3	e.	Log data support other business and security processes (e.g., incident response, asset management)
2. Monitor IT Services		
MIL1	a.	Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner
MIL1	b.	IT services' operational environments are monitored, at least in an ad hoc manner, for anomalous behavior that may indicate a cybersecurity event (e.g., web response rates are exceptionally slow)
MIL2	c.	Monitoring and analysis requirements have been defined for IT services and address timely review of event data
MIL2	d.	Alarms and alerts are configured to aid the identification of cybersecurity events (IR-1b)
MIL2	e.	Indicators of anomalous activity have been defined and are monitored across the operational environment
MIL2	f.	Monitoring activities are aligned with IT services' threat profile (TVA-1d)
MIL3	g.	Monitoring requirements are based on the risk to IT services
MIL3	h.	Monitoring is integrated with other business and security processes (e.g., incident response, asset management, vulnerability and threat management)
MIL3	i.	Continuous monitoring is performed across the operational environment to identify anomalous activity
MIL3	j.	Risk register (RM-2j) content is used to identify indicators of anomalous activity
MIL3	k.	Alarms and alerts are configured according to indicators of anomalous activity
3. Establish and Maintain a Common Operating Picture		
MIL1		No practice at MIL 1
MIL2	a.	Methods of communicating the current state of cybersecurity for IT services are established and maintained
MIL2	b.	Monitoring data are aggregated to provide near-real-time understanding of the operational state of IT services (i.e., a common operating picture; a COP may or may not include visualization)
MIL2	c.	Information from across the organization is available to enhance the common operating picture
MIL3	d.	Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for IT services to enhance the common operating picture
MIL3	e.	Information from outside the organization is collected to enhance the common operating picture
MIL3	f.	Predefined states of operation are documented and invoked (manual or automated process) based on the common operating picture
4. Institutionalization Activities for SA Domain		
MIL1		No practice at MIL 1

SITUATIONAL AWARENESS **Objectives and Practices**		
MIL2	a.	Documented practices are followed for logging, monitoring, and COP activities
MIL2	b.	Stakeholders for logging, monitoring, and COP activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform logging, monitoring, and COP activities
MIL3	e.	Logging, monitoring, and COP activities are guided by documented policies or other organizational directives
MIL3	f.	Logging, monitoring, and COP policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel
MIL3	i.	Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities

5.6 Information Sharing and Communications

Purpose: Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including information about threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to the enterprise and its mission.

The objective of information sharing is to strengthen cybersecurity in an organization, enterprise, or industry by establishing and maintaining a framework for interaction within an organization, among organizations in an enterprise, among enterprises in an industry, and between enterprises in an industry and the government.

The Information Sharing and Communications (ISC) domain comprises two objectives:

1. Share Cybersecurity Information
2. Institutionalization Activities

Sharing cybersecurity information begins with gathering cybersecurity information relevant to enterprise IT services. This information is available from many sources, including vendors, government entities, and peers. Essential to the security posture of any organization is the sharing of different types of risk-related information, which makes the secure distribution of this information important to the security of the organization. As threats are responded to and vulnerabilities are discovered, organizations should ensure that relevant data are effectively and appropriately shared so that peers may also reduce their risk and improve resilience. Forums, such as the Information Sharing and Analysis Centers in many critical infrastructure sectors, can facilitate this sharing for private sector organizations. US-CERT provides this forum for public sector organizations at the federal level.

Example
Information Sharing and Communications

Anywhere Inc. has worked with trade groups to find and maintain informal connections with other organizations. This has worked sufficiently well for a variety of issues without critical deadlines. However, new security and cyber-related issues with critical deadlines have strained this informal method of sharing and communications.

Recognizing the need for more significant relationships, the organization has decided to formalize ties to industry groups that will inform it of news and issues; engage with vendors with whom it has significant investment; and participate with regional, state, and government organizations that advance thought leadership and practical guidance.

As part of this effort, Anywhere Inc. has partnered with others to establish a secure, confidential information-sharing environment that enables organizations to share cybersecurity information without attribution. Within this environment, organizations are free to disclose cybersecurity information as well as share technical expertise to overcome cybersecurity challenges.

INFORMATION SHARING AND COMMUNICATIONS **Objectives and Practices**		
1. Share Cybersecurity Information		
MIL1	a.	Cybersecurity information is collected from and provided to selected individuals and/or organizations, at least in an ad hoc manner
MIL1	b.	Responsibility for cybersecurity reporting obligations is assigned to personnel (e.g., internal reporting, US-CERT, law enforcement), at least in an ad hoc manner
MIL2	c.	Information-sharing stakeholders are identified based on their relevance to the continued operation of IT services (e.g., connected organizations, vendors, internal entities)
MIL2	d.	Information is collected from and provided to identified information-sharing stakeholders
MIL2	e.	Technical resources are identified that can be consulted on cybersecurity issues
MIL2	f.	Provisions are established and maintained to enable secure sharing of sensitive cybersecurity information
MIL2	g.	Information-sharing practices address both standard operations and emergency operations
MIL3	h.	Information-sharing stakeholders are identified based on common interests and risks
MIL3	i.	The organization participates with external information sharing and analysis organizations
MIL3	j.	Information-sharing requirements have been defined for IT services and address timely dissemination of cybersecurity information
MIL3	k.	Procedures are in place to analyze and deconflict received information
MIL3	l.	A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events
2. Institutionalization Activities for ISC Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for information-sharing activities
MIL2	b.	Stakeholders for information-sharing activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support information-sharing activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform information-sharing activities
MIL3	e.	Information-sharing activities are guided by documented policies or other organizational directives
MIL3	f.	Information-sharing policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Information-sharing policies address protected information, ethical use and sharing of information, including sensitive information as appropriate
MIL3	h.	Information-sharing activities are periodically reviewed to ensure conformance with policy
MIL3	i.	Responsibility and authority for the performance of information-sharing activities are assigned to personnel
MIL3	j.	Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities

5.7 Event and Incident Response, Continuity of Operations

Purpose: Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to the enterprise and its mission.

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 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.

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

1. Detect Cybersecurity Events
2. Escalate Cybersecurity Events and Declare Incidents
3. Respond to Incidents and Escalated Cybersecurity Events
4. Plan for Continuity
5. Institutionalization 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. They should 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.

Example

Event and Incident Response, Continuity of Operations

Anywhere Inc. has purchased a help desk tracking system to improve logging and tracking of all events that are reported to the IT service help desk, including important cybersecurity events. At every help desk workstation, Anywhere Inc. has posted a chart that identifies criteria for escalating cybersecurity events, which include who must be notified and response time objectives. This information is available on the organization’s intranet as well.

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 common operating picture described in the Situational Awareness domain.

Anywhere Inc. tests its disaster recovery plans for each enterprise IT service annually to ensure that it can continue to meet recovery time objectives for the functional and organizational units it supports. Staff responsible for disaster recovery have a good understanding of the restoration path for the assets that support each service.

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 escalated cybersecurity events and cybersecurity incidents should be managed according to a response plan. Escalated 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 escalated cybersecurity events requires the organization to have a process to limit the impact of cybersecurity events. 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 part of cybersecurity event and incident response helps the organization eliminate the exploited vulnerability that led to the incident.

Planning for continuity involves the necessary activities to sustain the critical operations of the organization in the event of an interruption such as a severe cybersecurity incident or a disaster. Business impact analyses enable the organization to identify essential assets and associated recovery time objectives. Continuity plans should be tested and adjusted to ensure they remain operable.

EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS **Objectives and Practices**		
1. Detect Cybersecurity Events		
MIL1	a.	A point of contact (person or role) to whom cybersecurity events can be reported has been identified, at least in an ad hoc manner
MIL1	b.	Detected cybersecurity events are reported, at least in an ad hoc manner
MIL1	c.	Cybersecurity events are logged and tracked, at least in an ad hoc manner
MIL2	d.	Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events)
MIL2	e.	There is a repository where cybersecurity events are logged based on the established criteria
MIL3	f.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features
MIL3	g.	Cybersecurity event detection activities are adjusted based on information from the organization’s risk register (RM-2j) and threat profile (TVA-1d) to help monitor for identified risks and detect known threats
MIL3	h.	The common operating picture for IT services is monitored to support the identification of cybersecurity events (SA-3a)
2. Escalate Cybersecurity Events		
MIL1	a.	Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria, at least in an ad hoc manner
MIL1	b.	Cybersecurity events are analyzed, at least in an ad hoc manner, to support escalation and the declaration of cybersecurity incidents
MIL1	c.	Escalated cybersecurity events and incidents are logged and tracked, at least in an ad hoc manner
MIL2	d.	Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are established based on the potential impact to IT services
MIL2	e.	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency
MIL2	f.	There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure
MIL3	g.	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization’s risk register (RM-1c, RM-2j) and threat profile (TVM-1d)
MIL3	h.	Escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (SA-3a) for IT services

EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS **Objectives and Practices**		
MIL3	i.	Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features
3. Respond to Escalated Cybersecurity Events		
MIL1	a.	Cybersecurity event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner
MIL1	b.	Responses to escalated cybersecurity events and incidents are implemented, at least in an ad hoc manner, to limit impact to IT services and restore normal operations
MIL1	c.	Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, IS-CERT), at least in an ad hoc manner
MIL2	d.	Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident lifecycle (e.g., triage, handling, communication, coordination, and closure)
MIL2	e.	Cybersecurity event and incident response plans are exercised at an organization-defined frequency
MIL2	f.	Cybersecurity event and incident response plans address all assets important to the delivery of IT services
MIL2	g.	Training is conducted for cybersecurity event and incident response teams
MIL3	h.	Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed and corrective actions are taken
MIL3	i.	Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including evidence collection and preservation
MIL3	j.	Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents)
MIL3	k.	Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency
MIL3	l.	Cybersecurity event and incident response activities are coordinated with relevant external entities
MIL3	m.	Cybersecurity event and incident response plans are aligned with defined risk criteria (RM-1c) and threat profile (TVA-1d)
MIL3	n.	Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements
MIL3	o.	Restored assets are configured appropriately and inventory information is updated following execution of response plans
4. Plan for Continuity		
MIL1	a.	The activities necessary to sustain minimum operations of IT services are identified, at least in an ad hoc manner
MIL1	b.	The sequence of activities necessary to return IT services to normal operation is identified, at least in an ad hoc manner
MIL1	c.	Continuity plans are developed, at least in an ad hoc manner, to sustain and restore IT services
MIL2	d.	Business impact analyses inform the development of continuity plans
MIL2	e.	Recovery time objectives and recovery point objectives for IT services are incorporated into continuity plans
MIL2	f.	Continuity plans are evaluated and exercised
MIL3	g.	Business impact analyses are periodically reviewed and updated

EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS **Objectives and Practices**		
MIL3	h.	Recovery time objectives and recovery point objectives are aligned with defined risk criteria (RM-1c)
MIL3	i.	The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly
MIL3	j.	Continuity plans are periodically reviewed and updated
MIL3	k.	Restored assets are configured appropriately and inventory information is updated following execution of continuity plans
5. Institutionalization Activities for IR Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for cybersecurity event and incident response and continuity of operations activities
MIL2	b.	Stakeholders for cybersecurity event and incident response and continuity of operations activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response and continuity of operations activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform cybersecurity event and incident response and continuity of operations activities
MIL3	e.	Cybersecurity event and incident response and continuity of operations activities are guided by documented policies or other organizational directives
MIL3	f.	Cybersecurity event and incident response and continuity of operations policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Cybersecurity event and incident response and continuity of operations activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of cybersecurity event and incident response and continuity of operations activities are assigned to personnel
MIL3	i.	Personnel performing cybersecurity event and incident response and continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities

5.8 Supply Chain and External Dependencies Management

Purpose: Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to the enterprise and its mission.

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 enterprise IT services.

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

Consideration of supplier and customer dependencies should not be limited to the dependent parties and should include the full spectrum of the relationship. Asset-level dependencies such as system interconnections should be considered as well. For example, the successful operation of a function may be dependent on the ability of one organization's IT assets to process another organization's information within a specific set of constraints.

Supply chain risk is a noteworthy example of this type of 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. Requests for proposal (RFPs) 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 enterprises 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 (EDM) domain comprises three objectives:

1. Identify Dependencies
2. Manage Dependency Risk
3. Institutionalization Activities

Example

Supply Chain and External Dependencies Management

Anywhere Inc. receives IT services and support from multiple vendors. Recently, the organization began to work with a new vendor that will be a providing proprietary cloud platform. During the normal course of business, this vendor will have access to systems operating on sensitive data.

Within the contract for the project, Anywhere Inc. mandated the nondisclosure of sensitive data. It 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 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 cloud service delivery platform, and plans to conduct periodic audits of the system to ensure that the vendor continues to meet its obligations.

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

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 (SLAs) can specify monitoring and audit processes to verify that vendors and service providers meet cybersecurity and other performance measures.

SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT **Objectives and Practices**		
1. Identify Dependencies		
MIL1	a.	Important supplier dependencies are identified (i.e., internal and external parties on which the delivery of IT services depends), at least in an ad hoc manner
MIL1	b.	Important customer dependencies are identified (i.e., internal and external parties that depend on the delivery of IT services), at least in an ad hoc manner
MIL2	c.	Supplier dependencies are identified according to established criteria
MIL2	d.	Customer dependencies are identified according to established criteria
MIL2	e.	Single-source and other essential dependencies are identified
MIL2	f.	Dependencies are prioritized
MIL3	g.	Dependency prioritization and identification are based on defined risk criteria (RM-1c)
2. Manage Dependency Risk		
MIL1	a.	Significant cybersecurity risks due to suppliers and customers are identified and addressed, at least in an ad hoc manner
MIL1	b.	Cybersecurity requirements are considered, at least in an ad hoc manner, when establishing relationships with suppliers and customers
MIL2	c.	Identified cybersecurity dependency risks are entered into the risk register (RM-2j)
MIL2	d.	Contracts and agreements with suppliers and customers incorporate sharing of cybersecurity threat information
MIL2	e.	Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate
MIL2	f.	Agreements with suppliers and customers include cybersecurity requirements
MIL2	g.	Evaluation and selection of suppliers includes consideration of their ability to meet cybersecurity requirements
MIL2	h.	Agreements with suppliers require notification of cybersecurity incidents related to the delivery of their products or services
MIL2	i.	Suppliers are periodically reviewed for their ability to meet the cybersecurity requirements
MIL3	j.	Cybersecurity risks due to external dependencies are managed according to the organization’s risk management criteria and process
MIL3	k.	Cybersecurity requirements are established for supplier dependencies based on defined risk criteria (RM-1c)
MIL3	l.	Agreements with suppliers require notification of product vulnerabilities throughout the intended lifecycle of the products

SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT **Objectives and Practices**		
MIL3	m.	Acceptance testing of procured assets includes testing for cybersecurity requirements
MIL3	n.	Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services)
3. Institutionalization Activities for EDM Domain		
MIL1		No practice at MIL 1
MIL2	a.	Documented practices are followed for managing dependency risk
MIL2	b.	Stakeholders for managing dependency risk are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support dependency risk management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform managing dependency risk
MIL3	e.	Dependency risk management activities are guided by documented policies or other organizational directives
MIL3	f.	Dependency risk management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Dependency risk management activities are periodically reviewed to ensure conformance with policy
MIL3	h.	Responsibility and authority for the performance of dependency risk management are assigned to personnel
MIL3	i.	Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities

5.9 Workforce Management

Purpose: Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to the enterprise and its mission.

As organizations increasingly adopt advanced digital technology and as cyber threats become more pervasive and relentless, maintaining an IT services workforce with the appropriate level of cybersecurity experience, education, and training is a serious challenge and potentially a major area of risk. IT service organizations must ensure that cybersecurity responsibilities are defined and are assigned to competent, trustworthy personnel. IT service organizations are also responsible for developing a culture of cybersecurity awareness in the enterprise to help prevent and mitigate cyber attacks.

An organization's workforce management objectives define what it aims to achieve, with respect to growth and development of the workforce, within a given time frame and with available resources. These objectives support the organization's larger goals and should include cybersecurity considerations.

The Workforce Management (WM) domain comprises five objectives:

1. Assign Cybersecurity Responsibilities
2. Control the Workforce Lifecycle
3. Develop Cybersecurity Workforce
4. Increase Cybersecurity Awareness
5. Institutionalization 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.

Controlling the workforce lifecycle includes personnel vetting (e.g., background checks) and assigning risk designations to positions that have access to assets needed to deliver an essential service. For example, system administrators (who typically have the ability to change configuration

Example
Workforce Management

Anywhere Inc. recognizes that technology underlying its enterprise IT services is constantly evolving and that it must continually invest in advanced technology to meet increasingly demanding service delivery requirements. Part of this investment will be a long-term program for workforce training and management to help personnel keep up to date with new technologies and so that they can keep the IT services 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, it finds that its newly deployed 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 IT services external to the organization (e.g., partners or vendors with IT services connected to Anywhere Inc.).

settings, modify or delete log files, create new accounts, and change passwords) on critical systems are given a higher risk designation, and specific measures are taken for protection of these systems from accidental or malicious behavior by this category of personnel.

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

Increasing the cybersecurity awareness of the workforce is as important as technological approaches for improving the cybersecurity of the organization. The organization should share information with the enterprise workforce on methods and techniques to identify suspicious behavior, avoid spam or 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.

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 are compatible with those agreements.

WORKFORCE MANAGEMENT **Objectives and Practices**		
1. Assign Cybersecurity Responsibilities		
MIL1	a.	Cybersecurity responsibilities for IT services are identified, at least in an ad hoc manner
MIL1	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)
MIL2	d.	Cybersecurity responsibilities are documented (e.g., in position descriptions)
MIL3	e.	Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate
MIL3	f.	Cybersecurity responsibilities are included in job performance evaluation criteria
MIL3	g.	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage
2. Control the Workforce Lifecycle		
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 IT services
MIL1	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 IT services
MIL2	d.	Personnel transfer procedures address cybersecurity
MIL3	e.	Risk designations are assigned to all positions that have access to the assets required for delivery of IT services

WORKFORCE MANAGEMENT **Objectives and Practices**		
MIL3	f.	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation
MIL3	g.	Succession planning is performed for personnel based on risk designation
MIL3	h.	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures
3. Develop Cybersecurity Workforce		
MIL1	a.	Cybersecurity training is made available, at least in an ad hoc manner, to personnel with assigned cybersecurity responsibilities
MIL2	b.	Cybersecurity knowledge, skill, and ability gaps are identified
MIL2	c.	Identified gaps are addressed through recruiting and/or training
MIL2	d.	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of IT services (e.g., new personnel training, personnel transfer training)
MIL3	e.	Cybersecurity workforce management objectives that support current and future operational needs are established and maintained
MIL3	f.	Recruiting and retention are aligned to support cybersecurity workforce management objectives
MIL3	g.	Training programs are aligned to support cybersecurity workforce management objectives
MIL3	h.	The effectiveness of training programs is evaluated at an organization-defined frequency and improvements are made as appropriate
MIL3	i.	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities
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
MIL2	c.	Cybersecurity awareness content is based on the defined threat profile (TVA-1d)
MIL3	d.	Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f)
MIL3	e.	The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate
5. Institutionalization Activities for WM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for cybersecurity workforce management activities
MIL2	b.	Stakeholders for cybersecurity workforce management activities are identified and involved
MIL2	c.	Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities
MIL2	d.	Standards, guidelines, and best practices have been identified to inform cybersecurity workforce management activities
MIL3	e.	Cybersecurity workforce management activities are guided by documented policies or other organizational directives
MIL3	f.	Cybersecurity workforce management policies include compliance requirements for specified standards, guidelines, and best practices
MIL3	g.	Cybersecurity workforce management activities are periodically reviewed to ensure conformance with policy

WORKFORCE MANAGEMENT **Objectives and Practices**		
MIL3	h.	Responsibility and authority for the performance of cybersecurity workforce management activities are assigned to personnel
MIL3	i.	Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities

5.10 Cybersecurity Program Management

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

A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization and/or enterprise IT services. A cybersecurity program may be implemented at either the organization 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 (CPM) domain comprises five objectives:

1. Establish Cybersecurity Program Strategy
2. Sponsor Cybersecurity Program
3. Establish and Maintain Cybersecurity Architecture
4. Perform Secure Software Development
5. Institutionalization 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. It also includes organizational support for establishing and implementing policies or other organizational directives to guide the program.

A cybersecurity architecture is an integral part of the enterprise architecture. It describes the structure and behavior of an enterprise's security processes, cybersecurity systems, personnel, and sub-

Example
Cybersecurity Program Management

Anywhere Inc. decided to establish an enterprise cybersecurity program. To begin, it has formed a board with representation from each of the functional areas. This cybersecurity governance board will develop a cybersecurity 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 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 are counting 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 are expecting guidance on systems development and methods to mitigate risks.

ordinate organizations and aligns them with the organization’s mission and strategic plans. An important element of a cybersecurity architecture is often effective isolation and segregation of IT systems.

Performing and/or requiring secure software development for assets that are important to the delivery of enterprise IT services is important to help reduce vulnerability-inducing software defects.

CYBERSECURITY PROGRAM MANAGEMENT **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 objectives for the organization’s cybersecurity activities
MIL2	c.	The cybersecurity program strategy and priorities are documented and aligned with the organizational and enterprise strategic objectives and risk to the enterprise and its mission
MIL2	d.	The cybersecurity program strategy defines the organization’s approach to provide program oversight and governance for cybersecurity activities
MIL2	e.	The cybersecurity program strategy defines the structure and organization of the cybersecurity program
MIL2	f.	The cybersecurity program strategy is approved by senior management
MIL3	g.	The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVA-1d)
2. Sponsor Cybersecurity Program		
MIL1	a.	Resources (people, funding, and tools) are provided, at least in an ad hoc manner, to support the cybersecurity program
MIL1	b.	Senior management provides sponsorship for the cybersecurity program, at least in an ad hoc manner
MIL2	c.	The cybersecurity program is established according to the cybersecurity program strategy
MIL2	d.	Adequate resources are provided to establish and operate a cybersecurity program aligned with the program strategy
MIL2	e.	Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities is regularly communicated by senior management)
MIL2	f.	If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program
MIL2	g.	The development and maintenance of cybersecurity policies is sponsored
MIL2	h.	Responsibility for the cybersecurity program is assigned to a role with requisite authority
MIL3	i.	The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy
MIL3	j.	The cybersecurity program is independently reviewed for achievement of cybersecurity program objectives
MIL3	k.	The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate
MIL3	l.	The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives

CYBERSECURITY PROGRAM MANAGEMENT **Objectives and Practices**		
3. Establish and Maintain Cybersecurity Architecture		
MIL1	a.	A strategy to segment and isolate IT service delivery systems, where feasible, is implemented, at least in an ad hoc manner
MIL2	b.	A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy
MIL2	c.	Architectural segmentation and isolation is maintained according to a documented plan
MIL3	d.	Cybersecurity architecture is updated at an organization-defined frequency to keep it current
4. Perform Secure Software Development		
MIL1		No practice at MIL1
MIL2	a.	Software to be deployed on assets that are important to the delivery of IT services is developed using secure software development practices
MIL3	b.	Policies require that software to be deployed on assets that are important to the delivery of IT services be developed using secure software development practices
5. Institutionalization Activities for CPM Domain		
MIL1		No practice at MIL1
MIL2	a.	Documented practices are followed for managing cybersecurity program activities
MIL2	b.	Stakeholders for cybersecurity program management activities are identified and involved
MIL2	c.	Standards, guidelines, and best practices have been identified to inform cybersecurity program management activities
MIL3	d.	Cybersecurity program management activities are guided by documented policies or other organizational directives
MIL3	e.	Cybersecurity program management activities are periodically reviewed to ensure conformance with policy
MIL3	f.	Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities

References

[DOE 2014a]

U.S. Department of Energy. *Cybersecurity Capability Maturity Model*. DOE, February 2014. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

[DOE 2014b]

U.S. Department of Energy. *Cybersecurity Capability Maturity Model (C2M2)—Facilitator Guide*. DOE, February 2014. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-facilitator-guide-february-2014

[DOE 2014c]

U.S. Department of Energy. *Electricity Subsector Cybersecurity Capability Maturity Model V1.1*. DOE, February 2014. http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. **AGENCY USE ONLY**
   (Leave Blank)
2. **REPORT DATE**
   April 2015
3. **REPORT TYPE AND DATES COVERED**
   Final
4. **TITLE AND SUBTITLE**
   Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0
5. **FUNDING NUMBERS**
   FA8721-05-C-0003
6. **AUTHOR(S)**
   Pamela Curtis, Nader Mehravari, & James Stevens
7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
   Software Engineering Institute
   Carnegie Mellon University
   Pittsburgh, PA 15213
8. **PERFORMING ORGANIZATION REPORT NUMBER**
   CMU/SEI-2015-TR-009
9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
   AFLCMC/PZE/Hanscom
   Enterprise Acquisition Division
   20 Schilling Circle
   Building 1305
   Hanscom AFB, MA 01731-2116
10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**
    n/a
11. **SUPPLEMENTARY NOTES**

12A **DISTRIBUTION/AVAILABILITY STATEMENT**
Unclassified/Unlimited, DTIC, NTIS

12B **DISTRIBUTION CODE**

13. **ABSTRACT (MAXIMUM 200 WORDS)**

Cyber threats are one of the most serious and challenging types of operational risk facing modern organizations. The national and economic security of the United States depends on the reliable functioning of the information technology services that serve the Nation’s critical infrastructure in the face of such threats. Beyond critical infrastructure, the economic vitality of the Nation depends on the sustained operation of the enterprise information technology (IT) services of organizations of all types. This report describes the Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), which helps IT service delivery organizations of all sectors, types, and sizes evaluate make improvements to their cybersecurity programs.

14. **SUBJECT TERMS**
    Cyber threats, C2M2 for IT Services, information technology services cybersecurity capability maturity model
15. **NUMBER OF PAGES**
    64
16. **PRICE CODE**

17. **SECURITY CLASSIFICATION OF REPORT**
    Unclassified
18. **SECURITY CLASSIFICATION OF THIS PAGE**
    Unclassified
19. **SECURITY CLASSIFICATION OF ABSTRACT**
    Unclassified
20. **LIMITATION OF ABSTRACT**
    UL