Dams Sector Cybersecurity Capability Maturity Model (C2M2)

2016

Homeland Security

Acknowledgements

This document was developed with input, advice, and assistance from the Dams Sector Cybersecurity Working Group and council members of the Dams Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), which included representatives from the public and private sector.

Intended Scope and Use of This Publication

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

Note on Model Development

This material is based on the *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), Version 1.1, which was originally developed as part of a White House initiative in 2012 by Carnegie Mellon University and the U.S. Department of Energy (DOE), in close consultation with owners and operators and cybersecurity experts in the Energy Sector. This version of the Dams-C2M2 is being released and maintained by the U.S. Department of Homeland Security (DHS), in partnership with the Dams GCC and SCC.

Table of Contents

1. Introduction

Numerous cyber intrusions across critical infrastructure sector organizations demonstrate the urgent need for improved cybersecurity in the United States. Cyber threats continue to grow and represent one of the most serious operational risks facing modern organizations. National security and economic vitality depend on the reliability of the Nation's critical infrastructure to withstand such threats. Strong cybersecurity is particularly essential for organizations that use cyber systems to manage or control critical physical processes. The Dams Sector Cybersecurity Capability Maturity Model (Dams-C2M2) can help Dams Sector organizations evaluate and improve their cybersecurity programs, regardless of the type or size of the organization.

The Dams-C2M2 was developed to address the distinct operational characteristics of the Dams Sector. The model is a highly flexible tool that owners and operators can *choose* to use in one or more ways:

- **Identify a progressive, step-wise approach to build strong cybersecurity capabilities** based on industry-wide best practices, existing standards, and cross-sector cyber expertise.
- **Effectively evaluate and benchmark** their cybersecurity capabilities in a clear and organized way.
- **Prioritize step-wise actions and investments** to improve cybersecurity.
- **Consistently measure and demonstrate progress over time** toward organization-specific goals.

The Dams-C2M2 is NOT designed to issue a grade or a rating to an organization's cybersecurity program.

The Dams-C2M2 is designed for self-evaluation of an organization's cybersecurity program. The Dams Sector Cybersecurity Working Group is currently developing a self-evaluation Implementation Guide that will help asset owners assess their organization using the C2M2. Additionally, the model can inform the development of a new cybersecurity program.

The model is organized into 10 domains, each containing a logical grouping of structured cybersecurity practices. Together these domains and practices describe a robust program for cybersecurity and risk management. There is considerable convergence among the practices in each domain. For example, protecting against insider threats will require practices in the Identity and Access Management, Threat and Vulnerability Management, and Workforce Management domains.

The Dams-C2M2 provides *descriptive* rather than *prescriptive* guidance based on best practices and standards specific to the industry. The model describes high-level capabilities that can be interpreted by organizations of all types, structures, and sizes. These attributes also make the Dams-C2M2 an easily scalable tool for the sector's implementation of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. Sector-specific guidance can be found in the *Dams Sector Cybersecurity Framework Implementation Guidance*.

1.1 Intended Audience

The Dams-C2M2 enables Dams Sector organizations to evaluate cybersecurity capabilities consistently, communicate capability levels in meaningful terms, and prioritize cybersecurity investments. The model can be used by any Dams Sector organization, regardless of ownership, structure, or size. Within the organization, various stakeholders may benefit from familiarity with the model. This document specifically targets people in the following organizational roles:

- Decision-makers (executives) who control the allocation of resources and the management of risk in organizations; these are typically senior leaders.

- Leaders responsible for managing organizational resources and operations associated with the domains of this model (see Section 5.1 for more information on the content of each Dams-C2M2 domain).
- Practitioners responsible for supporting the organization in the use of this model (planning and managing changes in the organization based on the model).
- Facilitators who may be tasked to lead a self-evaluation of the organization based on this model and analyze the self-evaluation results.

1.2 Document Organization

This document introduces the model and provides the Dams-C2M2's main structure and content.

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

TABLE 1.—Recommended Document Sections for Key Stakeholders.

Role	Recommended Document Sections
Decision-makers	Chapters 1 and 2
Leaders or managers	Chapters 1, 2, 3, 4, and 5
Practitioners	Entire document
Facilitators	Entire document

Chapter 2 presents background information on the model and its development. Chapter 3 provides an overview of the U.S. Dams Sector. Chapter 4 describes several core concepts that are important for interpreting the content and structure of the Dams-C2M2. Chapter 5 describes the architecture of the Dams-C2M2. Chapter 6 provides guidance on how to use the model. **Chapter 7 contains the model itself—the model's objectives and practices, organized into 10 domains.** Appendix A includes references that were either used in the development of this document or provide further information about the practices identified within the model. Appendix B is the Glossary. Appendix C defines the acronyms used in this document.

2. Background

The Dams-C2M2 was developed by owners and operators and government stakeholders in the Dams Sector Cybersecurity Working Group at the direction of the Dams Sector Joint Council. The model aims to advance the practice of cybersecurity risk management across the Dams Sector by providing all Dams Sector organizations, regardless of size or type, with a flexible tool to help them evaluate, prioritize, and improve their cybersecurity capabilities.

The model content was based on the *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), Version 1.1, which was originally developed as part of a White House initiative in 2012 by Carnegie Mellon University and the U.S. Department of Energy (DOE), working in close consultation with owners and operators and cybersecurity experts in the Energy Sector. The Dams Sector also considered cybersecurity guidance developed by partners in the Water Sector.

The Dams-C2M2 leverages and builds upon existing efforts, models, and cybersecurity best practices and is aligned with the NIST *Cybersecurity Framework* and the *Roadmap to Secure Control Systems in the Dams Sector*. It also supports implementation of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636).

2.1 Model Development Approach

The model was developed under the following principles of development:

- **Public–private partnership**: Numerous government, industry, and academic organizations participated in the development of this model, bringing a broad range of knowledge, skills, and experience to the team.
- **Best practices and sector alignment**: The model builds upon and ties together a number of existing cybersecurity resources and initiatives and was informed by a review of cyber threats to the sector. Leveraging relevant sector resources helped ensure that the model would be relevant and beneficial to the sector.
- **Descriptive, not prescriptive**: This model was developed to provide descriptive, not prescriptive, guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be abstract so they can be interpreted by facilities and organizations of various structures, functions, and sizes.

3. The Dams Sector Cyber Landscape

The Dams Sector encompasses dam projects, hydropower plants, navigation locks, levees, mine tailings, industrial waste impoundments, dikes, hurricane barriers, and other similar water retention and water control facilities throughout the Nation.

Cybersecurity in the Dams Sector is primarily focused on the industrial control systems (ICS) that monitor, automate, and control critical physical processes, such as electric generation and transmission, water level and transport, and physical access control. These control systems typically collect information about facility operations and specific component status (e.g., gate position, reservoir level, hydroelectric generator output, water flowrate) to monitor, manage, command, direct, or regulate the behavior of devices or components. Data on component status are sent as electrical signals over digital networks (including the Internet and wired/wireless networks) to control systems and operators. Automated or operator commands may be sent back through the same network to manage operations.[1]

An ICS includes the facilities, systems, equipment, services, and diagnostics that enable the functional monitoring, control, and protection capabilities necessary for effective and reliable operation. Control systems are typically considered operations technology (OT). A cyber event affecting OT—whether caused by an external adversary, an insider threat, or inadequate policies and procedures—can initiate a loss of system control, resulting in negative consequences.

A cyber disruption in a business information technology (IT) system or its connecting networks and information could also compromise the security of the facility and its personnel. As such, an effective cybersecurity program accounts for threats to both OT and IT systems, including their connecting networks and information.

Each Dams Sector organization has a distinct mix and design of cyber infrastructure from multiple vendors. Owners and operators can develop internal tools, such as asset identification templates, as mechanisms to efficiently identify and inventory their organization's cyber assets.

3.1 Critical Functions

Throughout this model, the term "function" is used to describe the set of activities performed by the organization or facility to which the model is being applied.

The roles and functions that cyber systems serve can affect the reliable operation of critical functions. Addressing cyber-physical dependencies is critical, as control systems can be compromised and manipulated to operate equipment in ways that cause damage and inflict onsite and offsite causalities. When identifying cyber systems, consider the following types of critical functions:

- Provides operation information in real-time.
- Controls manual or automated parameters.
- Calculates parameters or limits.
- Generates or displays prompts or alarms.
- Provides connectivity between cyber systems.
- Supports continuity of operations for the critical functions or local recovery plans.

In addition to identifying critical functions, cyber asset identification can include secondary or supporting cyber systems whose loss, degradation, or compromise could affect the operation of critical cyber systems and associated critical

[1] In some cases, an ICS may consist of non-electronic, relay-based components without cyber assets connected to them. These systems, therefore, have a relatively low risk of being affected by a cyber event.

functions. This identification is based on whether a failure or compromise of these assets would affect the safety, reliability, functionality, and/or performance of cyber systems and would lead to issues with the safety and/or reliability of a Dams Sector asset. Secondary or supporting systems may include:

- Assets that facilitate the recovery and restoration process such as generators, spare parts, and spare systems.
- Stand-alone virus and malware scanners; archival, backup, and restoration systems; and log monitoring systems (except for cyber assets used in the access control and/or monitoring of logical and/or physical security zones).
- Environmental systems such as heating, ventilation, and air conditioning (HVAC).
- Support systems such as uninterruptable power supplies and alarm systems.
- Cyber systems supporting value chain activities.

However, the model can be applied to other functions or subfunctions performed by the organization.

3.2 Key Cybersecurity Concerns

Many of the ICSs used today were designed for operability and reliability during an era when there were fewer security concerns than there are today. These systems operated in fairly isolated environments and typically relied on vendor-specific or proprietary software, hardware, and/or communications technologies. Infiltrating and compromising these systems often required specific knowledge of individual system architectures and physical access to system components.

In contrast, modern ICSs are highly network-based and use common and open communication protocols; many controllers are also Internet Protocol addressable. Owners and operators have gained immediate benefits by extending the connectivity of their ICS. They have increasingly adopted commercial off-the-shelf (COTS) technologies that provide the higher levels of interoperability required among today's modern infrastructure. Standard operating systems such as Windows or UNIX are increasingly being used in central supervisory stations that are typically connected to remote controllers via private and/or public networks provided by telecommunications companies. In addition, common telecommunications technologies, such as the Internet, public-switched telephone networks, cable, or wireless networks, are often used.

Known cybersecurity risks that affect ICSs include:

- **Increased use of digital controls:** Replacement of analog and electromechanical controllers with digital and/or microprocessor-based controllers has caused increased exposure to cyber threats.
- **Supply chain:** Vendor access to ICSs has not always included procedures for granting authorized personnel logical access to systems. Systems may be inherently vulnerable as a result of programming errors.
- **System updates:** System updates and patches available on some manufacturer and vendor websites have contained malware. Proper patch management may be difficult if not readily accessible from the vendor due to ICS network isolation. In addition, patching may be hindered by ICS network high availability requirements.
- **Removable data storage devices:** Increased use of portable devices capable of transferring data can bypass network defenses and exploit potential vulnerabilities.
- **Insider threats:** Systems are increasingly susceptible to insider threats, including social engineering attacks, disgruntled employees, and intentional or unintentional actions.

3.3 Key Dams Sector Cyber Resources

The Dams Sector has developed a number of resources that should serve as critical companion documents to the Dams-C2M2. These documents can be accessed on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal or by emailing the Dams Sector at dams@hq.dhs.gov.

- The ***Dams Sector Cybersecurity Program Guidance*** consolidates effective industry practices into a framework for owners and operators to develop and/or improve a cybersecurity program. The Cybersecurity Program Guidance will provide owners and operators with more detailed guidance on how to conduct many of the activities in the model domains.
- The ***Dams Sector Security Guidelines*** consolidate effective industry security practices into a framework for owners and operators to select and implement both cyber and physical security activities and measures that promote the protection of personnel, public health, public safety, and public confidence.
- The ***Roadmap to Secure Control Systems in the Dams Sector*** provides a complete description of the cybersecurity landscape, and a plan and strategic vision for voluntary improvement of the cybersecurity posture of control systems within the Dams Sector.
- The ***Dams Sector Cybersecurity Framework Implementation Guide*** identifies existing Dams Sector cybersecurity tools and resources that can support implementation of the NIST Cybersecurity Framework and outlines detailed implementation steps tailored for Dams Sector owners and operators. The Dams-C2M2 provides an easily scalable tool for implementing the NIST Cybersecurity Framework.

A more in-depth description of typical ICSs and their vulnerabilities and currently available general security enhancements can be found on the United States Computer Emergency Readiness Team (US-CERT) Control System website and in the NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology*.

4. Core Concepts of the Maturity Model

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

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

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

To measure progression, maturity models typically have "levels" along a scale—Dams-C2M2 uses a scale of maturity indicator levels (MILs) 0-3, which are described in Section 5.2. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities the level represents. Having measurable transition states between 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.

4.1 Critical Infrastructure Objectives

The model regularly references critical infrastructure objectives. These objectives are from the Sector-Specific Plans of the 16 U.S. critical infrastructure sectors, defined in PPD-21. The functions provided by potential adopters of this model support the Nation's critical infrastructure and consider broader cybersecurity objectives in the Sector-Specific Plans.

4.2 IT and OT Assets

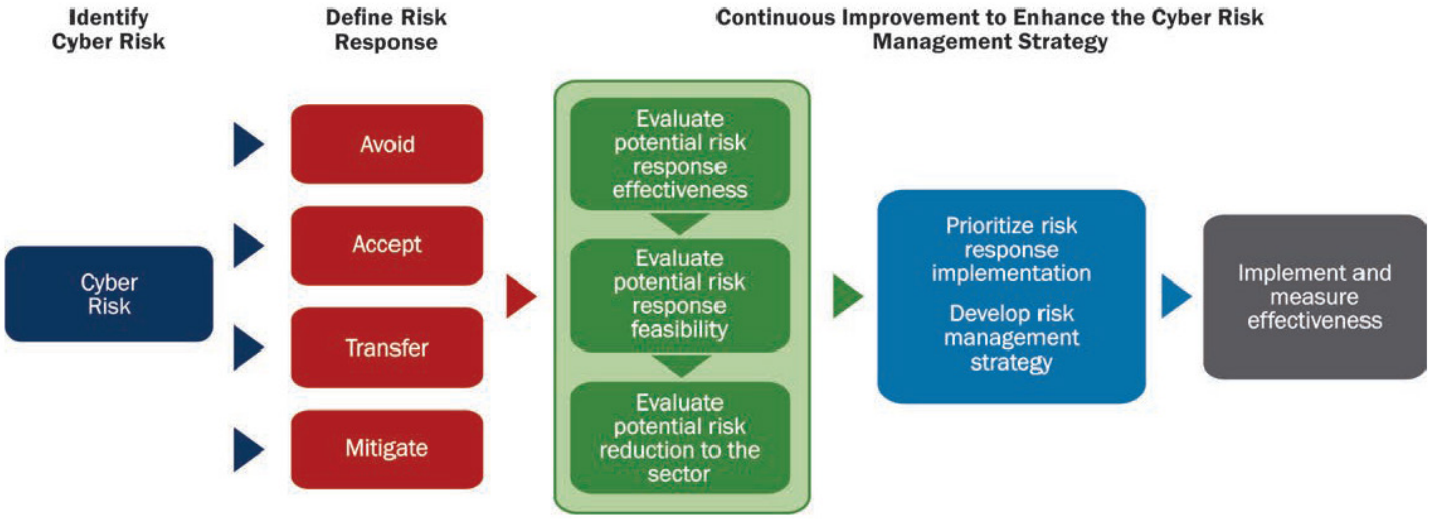
Many Dams-C2M2 practices refer to assets. When evaluating how completely a practice is performed, be sure to consider both traditional and emerging enterprise IT assets and all OT assets—including ICS, process control systems, supervisory control and data acquisition (SCADA) systems, and other OT.

Though IT and OT assets may perform different functions and have different levels of criticality within an organization, similar practices, approaches, and standards can be used to secure both types of assets. The progressive cybersecurity approaches outlined in each C2M2 domain can be used to assess or inform cybersecurity programs for both IT and OT.

4.3 Relationship to the Risk-Management Process

The phrase "commensurate with risk to critical infrastructure and organizational objectives" is used throughout the model. This phrase reminds 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 can use the model as part of a continuous enterprise risk-management process, such as depicted in Figure 1.

FIGURE 1.—Risk Management Process.



The Dams-C2M2 Risk Management domain (see Section 7.1) suggests establishing a cybersecurity risk-management strategy that aligns with an organization's enterprise risk-management strategy. Cybersecurity risk is an important component of the overall business risk environment. Dams-C2M2's cybersecurity risk-management activities should feed into the enterprise risk-management strategy and program so that cybersecurity risk is considered in and benefits from corporate decisions based on risk effect, tolerance for risk, and risk-response approaches.

The implementation of practices in the Risk Management domain provides supporting elements 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 5.3.

4.4 Function

In this model, the term "function" is used as a scoping mechanism; it refers to the organization's operations that are being evaluated based on the model.

It is common for an organization to use the model to evaluate a particular subset of its operations. This subset, or function, will often align with organizational boundaries. Therefore, common examples of functions for evaluation include departments, lines of business, or distinct facilities. Organizations have also successfully used the model to evaluate a specific system or technology thread that crosses departmental boundaries.

Take, for example, an organization that uses the model to evaluate its enterprise IT services, including email, Internet connectivity, and Voice over Internet Protocol (VoIP) telecommunication. In the Threat and Vulnerability Management domain, practice 2b states, "Cybersecurity vulnerability information is gathered and interpreted for the function." When evaluating the implementation of this practice, the organization should interpret function to mean the operations of the enterprise IT services. In this example, the practice means cybersecurity vulnerability information is gathered and interpreted for the enterprise IT services—information about vulnerabilities that would affect the enterprise email services, network devices, and the VoIP system.

5. Model Architecture

The model arises from a combination of existing cybersecurity standards, frameworks, programs, and initiatives, and provides flexible guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be abstract so they can be interpreted for organizations of various structures and sizes.

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, or target achievements that support the domain. Within each objective, the practices are ordered by MIL.

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

5.1 Domains

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

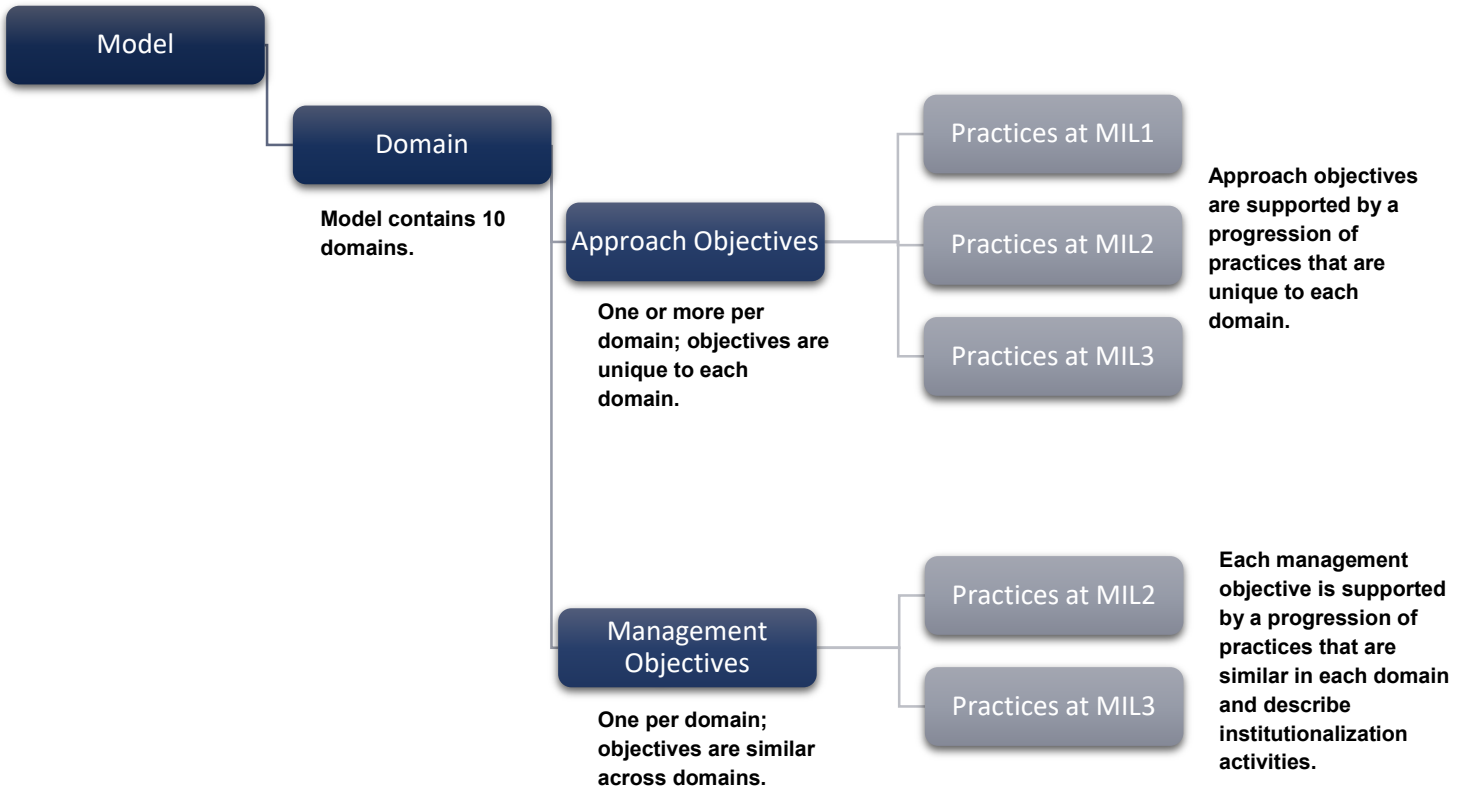
For each domain, the model provides a purpose statement, which is a high-level summary of the domain's intent, followed by introductory notes, which give context for the domain and introduce its practices. The purpose statement and introductory notes offer context for interpreting the practices in the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

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

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

Each of the objectives in a domain is composed of a set of practices that are ordered by MIL. Figure 2 summarizes the elements of each domain.

FIGURE 2.—Model and Domain Elements.



A brief description of the 10 domains follows in the order in which they appear in the model.

Risk Management

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

Asset Identification, Change, and Configuration Management

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

Identity and Access Management

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

Threat and Vulnerability Management

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

Situational Awareness

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

Information Sharing and Communications

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience commensurate with the risk to critical infrastructure and organizational objectives.

Event and Incident Response, Continuity of Operations, and Service Restoration

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

Vendor Security Management

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

Workforce Management

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

Cybersecurity Program Management

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

5.2 Maturity Indicator Levels

The model defines four maturity indicator levels, MIL0 through MIL3, that 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.

5.2.1 Approach Progression

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

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.

Maturity Indicator Level	Approach Progression
MIL0	Practices are not performed.
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).

5.2.2 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 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 Management Objective and Practices. The progression of the practices within a domain-specific objective corresponds to the progression of the management practices, though not necessarily practice-to-practice. Table 3 shows an example mapping of the management practices to the practices in the second objective of the Risk Management domain.

TABLE 3.—Mapping of Management Practices to Domain-Specific Practices.

Maturity Indicator Level	Management Practices	Domain-Specific Practices
MIL0	This model contains no practices for MIL0.	This model contains no practices for MIL0.
MIL1	a) Cybersecurity risks are identified. b) Identified risks are mitigated, accepted, tolerated, or transferred.	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) Risk analysis is supported by network (IT and/or OT) architecture.	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 and/or guidelines 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) A current cybersecurity architecture is used to support risk analysis. j) A risk register (a structured repository of identified risks) is used to support risk management.	1. Activities are guided by policies (or other organizational directives) and governance. 2. Policies include compliance requirements for specified standards and/or guidelines. 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.

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

Maturity Indicator Level 0 (MIL0)

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

Maturity Indicator Level 1 (MIL1)

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 an 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 to 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 that 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 the practice 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 and/or guidelines have been identified to guide the implementation of the practices.** The organization identified some standards and/or guidelines 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 and/or guidelines.**
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.

5.2.3 Summary of MIL Characteristics

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

TABLE 4.—Summary of Maturity Indicator Level Characteristics.

Level	Characteristic
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.

5.3 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. Table 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."

TABLE 5.—Referencing an Individual Practice, Example: RM-1a.

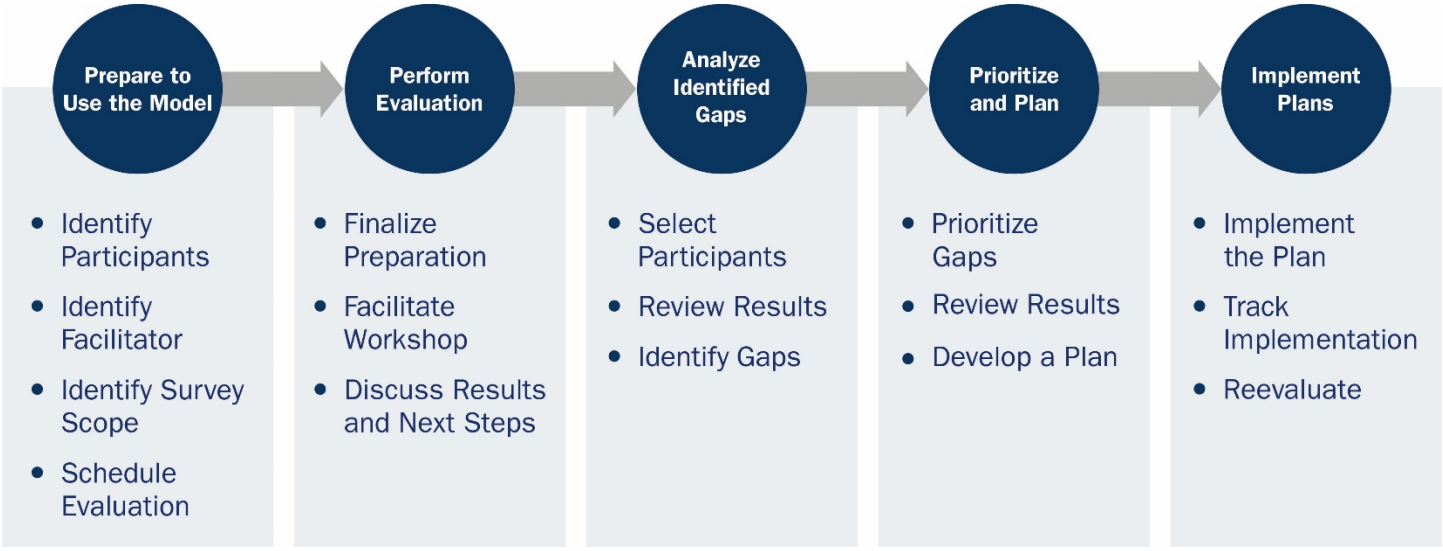
1. Establish Cybersecurity Risk-Management Strategy	
MIL1	No practice at MIL1.
MIL2	a) There is a documented cybersecurity risk-management strategy. b) The strategy provides an approach for risk prioritization, including consideration of effect.
MIL3	c) Organizational risk criteria tolerance for risk and risk-response approaches are defined. 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.

The notation for the above example includes the domain abbreviation (RM); objective number (1); and practice letter (a).

6. Using the Model

The Dams-C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. Figure 3 summarizes the recommended approach for using the model. An organization performs an evaluation against the model, uses that evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated. The following sections discuss the preparation activities required to begin using the model in an organization and provide additional details on the activities in each step of this approach. The Dams Sector C2M2 Implementation Guide (under development, expected fall 2016) provides additional details, suggested approaches, and templates to complete each of these steps.

FIGURE 3.—Recommended Approach for Using the Model.



6.1 Prepare to Use the Model

A design goal of the model was to enable organizations to complete a self-evaluation for a single function in less than one day for experienced users of the model, and two days or less for organizations new to the model. This goal is achieved in part because the Dams-C2M2 model is supported by an evaluation survey and documentation templates (including an After-Action Report), and the evaluation survey itself is performed in a workshop setting led by a facilitator who is familiar with the model content. The survey is included in Chapter 7 of this document and the templates are found in the Dams Sector C2M2 Implementation Guide. Preparing to use the model includes identifying the appropriate participants, identifying a qualified facilitator to lead and guide the participants, and identifying the scope of the survey.

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

Identify Facilitator: Generally speaking, a Dams-C2M2 facilitator is not only someone who is familiar with the model and its supporting reference material, 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.

Determine Scope: Though the Dams-C2M2 and its supporting survey apply to an entire organization, the self-evaluation survey is typically applied to a single function to maintain focus (i.e., a subset of the operations of the organization that is being evaluated). The facilitator works with the organization to determine the survey scope—the part of the organization's operations to which the model and survey will be applied and the organization's supporting IT and OT. Selecting and documenting the scope before completing the survey ensures that users of the survey results understand to which part of the organization the results apply.

6.2 Perform an Evaluation

Following the detailed planning and preparation by the organization to commit to implementing the C2M2, the facilitator and participants gather to conduct the evaluation in a workshop setting. The workshop entails the participants providing responses to the model's survey across 10 cybersecurity domains (logical groupings of cybersecurity practices) and the discussion of results and next steps.

Facilitate Workshop: The facilitator leads the participants through each of the 10 domains, associated objectives and practices, and MIL options. It is not typically optimal for an organization to strive to achieve the highest MIL in all domains. Rather, the organization determines the level of practice performance and MIL achievement for each domain that best enables it to meet its business objectives and cybersecurity strategy (called the current profile). The organization also identifies its desired capability profile—a target MIL rating for each domain in the model. This collection of desired capabilities is the organization's target capability 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.

Document and Review Results: While the facilitator is guiding participants through the C2M2, a member(s) of the evaluation team documents the decisions and discussion. Completion of the evaluation will yield an After-Action Report that shows MIL results for each domain and the successes and gaps supporting the MIL selections. This report provides a picture of the current state of practices relative to the model for the function evaluated and the gaps requiring mitigation to reach the target MIL. The report is reviewed with the evaluation workshop participants, and any discrepancies or questions addressed before completing the workshop and proceeding to gap analysis.

6.3 Analyze Identified Gaps

The completion of the C2M2 evaluation and the establishment of maturity profiles (current and capability) allow the organization to begin analyzing their cybersecurity maturity for the selected function. Through analysis of the evaluation results, gaps between where the organization currently stands in cybersecurity maturity and the desired level of maturity are readily identified. Once identified, the gaps are analyzed to prepare the organization for prioritizing which gaps to address.

Review Results: A post-evaluation group is selected to continue through the steps of the model, starting with reviewing the evaluation results. The group might prefer to convene in a workshop setting, or may wish to conduct this step over time through multiple meetings. The primary source of information to review is the draft After-Action Report, which will have been populated with all the relevant information from the evaluation, including the Maturity Profile Table (includes the current and capability profiles). By doing so, the post-evaluation group can become familiar with the evaluation and supporting discussion.

Identify Meaningful Gaps: The current and capability profiles provde the fundamental basis for the identifciation and analysis of gaps. Specifically, the gaps exist where the actual MIL falls short of the target MIL. An important consideration is the type and/or size of gap on which the organization wishes to focus. The organization might focus

primarily on gaps with high-level, strategic relevance, or focus on more technical issues relating to the objectives and practices of the gaps. While some gaps may be small and require implementing few practices, others may be more substantial. Any gap may represent meaningful hindrences to meeting the organization's business objectives and cybersecurity strategy.

6.4 Prioritize and Plan

After the gap analysis is complete, the organization prioritizes the gaps and identifies actions needed to fully implement the practices that enable achievement of the desired capability in specific domains. The selection of criteria can ensure the prioritization process is efficient and supports decisions. Examples of criteria include how gaps affect organizational objectives and compliance with regulations and rules, 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. The development of a gap mitigation plan can be useful to articulate and address the selected gaps. The plan may span a period of weeks, months, or years, depending on the extent of improvements needed to close the selected gaps and achieve the desired maturity indicator level.

6.5 Implement Plans and Periodically Reevaluate

Plans developed in the previous step are 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 may 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 6 presents a more detailed outline of the Dams-C2M2 process as described in this chapter.

TABLE 6.—Recommended Process for Using Evaluation Results.

	Inputs →	Activities →	Outputs
Prepare to Use the Model	1. Self-evaluation survey and documentation templates	1. Select appropriate personnel and facilitator perform the C2M2 evaluation 2. Determine the function(s) in scope	**Identified participants, facilitator, and survey scope**
Perform Evaluation	1. Dams-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct Dams-C2M2 Self-Evaluation Workshop with appropriate attendees	**Dams-C2M2 Self-Evaluation Report**

	Inputs	Activities	Outputs
Analyze Identified Gaps	1. Dams-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Effect on 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 prioritized actions	**Prioritized implementation plan**
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	**Project tracking data**

7. Model Domains

7.1 Risk Management

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

Cybersecurity risk is defined as risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations. This risk is due to the potential for unauthorized access; use; disclosure; disruption; modification; or destruction of information, IT, and/or OT. 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 has three objectives:

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

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 an organization-wide 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

Example: Risk Management

Anywhere USA Hydro 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 USA Hydro 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 ones with direct exposure, like the database server behind a web server, are in the second risk tier and so on. Anywhere USA Hydro augments the risk assessment derived from the network architecture with its cybersecurity architecture. Since its 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.

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

risk-management program. The DOE *Cybersecurity Risk Management Process* guidelines document provides a flexible risk-management process for framing, assessing, responding to, and monitoring risk across all levels of an organization.

TABLE 7.—Objectives and Practices for the Risk Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Establish Cybersecurity Risk-Management Strategy		
MIL1	No practice at MIL1	
MIL2	a) There is a documented cybersecurity risk-management strategy. b) The strategy provides an approach for risk prioritization, including consideration of effect.	• Risk Management Plan (p.11) • Risk Management Strategies (p. 12) • Risk Management Guidelines and Frameworks (p.18)
MIL3	c) Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on effect, 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.	• (See above)
2. Manage Cybersecurity Risk		
MIL1	a) Cybersecurity risks are identified. b) Identified risks are mitigated, accepted, tolerated, or transferred.	• Risk Management Strategies (p. 12)
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) Risk analysis is informed by network (IT and/or OT) architecture.	• (See above)
MIL3	h) The risk-management program defines and operates risk-management policies and procedures that implement the risk-management strategy. i) A current cybersecurity architecture is used to inform risk analysis. j) A risk register (a structured repository of identified risks) is used to support risk-management activities.	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for risk-management activities. b) Stakeholders for risk-management activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support risk-management activities. d) Standards and/or guidelines have been identified to inform risk-management activities.	
MIL3	e) Risk-management activities are guided by documented policies or other organizational directives. f) Risk-management policies include compliance requirements for specified standards and/or guidelines. g) Risk-management activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of risk-management activities are assigned to personnel. i) Personnel performing risk-management activities have the skills and knowledge needed to perform their assigned responsibilities.	

7.2 Asset Identification, Change, and Configuration Management

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

Identifying an organization's cyber assets—including critical cyber assets—is the starting point from which owners and operators design a cybersecurity program. An asset is something of value to an organization. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.

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

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

Owners and operators should review their organization's assets to identify and inventory critical and noncritical cyber assets, taking into consideration business value and applicable regulations (See "Asset Identification" in the *Dams Sector Cybersecurity Program Guidance* for a definition of critical and noncritical cyber assets). 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 IT and OT 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.

Example: Asset Identification, Change, and Configuration Management

Anywhere USA Hydro has an asset database. Within that database, technology assets are identified and prioritized based on importance to the generation function. The database includes attributes that support cybersecurity operations, such as hardware and software versions, physical location, security requirements (business needs for the asset's confidentiality, integrity, and availability), asset owner, and version of applied configuration baseline. Anywhere USA Hydro uses this information for cybersecurity risk-management activities, including identifying which systems may be affected by software vulnerabilities, prioritizing cybersecurity incident response, and planning disaster recovery.

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

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

TABLE 8.—Objectives and Practices for the Asset Identification, Change, and Configuration Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Manage Asset Inventory		
MIL1	a) There is an inventory of OT and IT assets[2] that are important to the delivery of the function. b) There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data).	• Cyber Asset Identification (p.3)
MIL2	c) Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, criticality of the asset,[3] service dependencies, service level agreements, and conformance of assets to relevant industry standards). d) Inventoried assets are prioritized based on their importance to the delivery of the function.	• Cyber Asset Criticality (p. 4) • Criticality Determination (p. 5) • Criticality Determination Guidance Documents (p. 6)
MIL3	e) There is an inventory for all connected[4] IT and OT assets related to the delivery of the function. f) The asset inventory is current (as defined by the organization).	• (See above)
2. Manage Asset Configuration		
MIL1	a) Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly. b) Configuration baselines are used to configure assets at deployment.	• Cybersecurity Functions: Baselining (p. 13)
MIL2	c) The design of configuration baselines includes cybersecurity objectives.	• (See above)
MIL3	d) Configuration of assets is monitored for consistency with baselines throughout the assets' life cycle. e) Configuration baselines are reviewed and updated at an organizationally defined frequency.	• (See above)

[2] The asset inventory may be a combined inventory or two separate inventories of IT and OT assets, respectively. However, progressing in maturity will require an inventory that includes information on how IT assets support the critical functions of OT assets.

[3] Critical cyber assets are those that are essential to the safety and/or reliability objectives of the facility. Many tools are available to help sector owners and operators identify critical assets. The "Criticality Determination" section of the *Dams Sector Cybersecurity Program Guidance* includes a discussion of criticality and presents common guidelines for determining asset criticality.

[4] Connected IT and OT assets are those in which the IT asset is required for the OT asset to properly function, or those IT assets whose loss, degradation, or compromise could affect both the operation of critical OT systems and their associated critical functions.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Manage Changes to Assets		
MIL1	a) Changes to inventoried assets are evaluated before being implemented. b) Changes to inventoried assets are logged.	• Security Measures (p. 14)
MIL2	c) Changes to assets are tested prior to being deployed, whenever possible. d) Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement).	• (See above)
MIL3	e) Changes to assets are tested for cybersecurity effect prior to being deployed. f) Change logs include information about modifications that affect the cybersecurity requirements of assets (availability, integrity, confidentiality).	• (See above)
4. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for asset inventory, configuration, and change management activities. b) Stakeholders for asset inventory, configuration, and change management activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change management activities. d) Standards and/or guidelines 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. f) Asset inventory, configuration, and change management policies include compliance requirements for specified standards and/or guidelines. g) Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel. i) Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities.	

7.3 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 critical infrastructure and organizational objectives.

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

The Identity and Access Management (IAM) domain has three objectives:

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

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

Controlling 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 the function and conducting regular reviews of access.

Example: Identity and Access Management

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

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

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

Anywhere USA Hydro also institutes a quarterly review to ensure that access granted to the facility's assets aligns with access requirements.

TABLE 9.—Objectives and Practices for the Identity and Access Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Establish and Maintain Identities[5]		
MIL1	a) Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities). b) Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys). c) Identities are deprovisioned when no longer required.	• Information System Security Controls (p. 14)
MIL2	d) Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access). e) Credentials are periodically reviewed to ensure they are associated with the correct person or entity. f) Identities are deprovisioned within organizationally defined time thresholds when no longer required.	• (See above)
MIL3	g) Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c).	• (See above)
2. Control Access		
MIL1	a) Access requirements, including those for remote access, are determined (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). b) Access is granted to identities based on requirements. c) Access is revoked when no longer required.	
MIL2	d) Access requirements incorporate least privilege and separation of duties principles. e) Access requests are reviewed and approved by the asset owner. 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 organizationally defined frequency. h) Access to assets is granted by the asset owner based on risk to the function. i) Anomalous access attempts are monitored as indicators of cybersecurity events.	

[5] Additional practices that support managing insider threats are included in the Workforce Management domain.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed to establish and maintain identities and control access. b) Stakeholders for access and identity management activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support access and identity management activities. d) Standards and/or guidelines have been identified to inform access and identity management activities.	
MIL3	e) Access and identity management activities are guided by documented policies or other organizational directives. f) Access and identity management policies include compliance requirements for specified standards and/or guidelines. g) Access and identity management activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of access and identity management activities are assigned to personnel. i) Personnel performing access and identity management activities have the skills and knowledge needed to perform their assigned responsibilities.	

7.4 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 organizational objectives.

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

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

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

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

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

Example: Threat and Vulnerability Management

Anywhere USA Hydro 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 Anywhere USA Hydro's documented threat profile.

Anywhere USA Hydro identified reliable sources of information to enable rapid threat identification and is able to consume and analyze published threat information from sources such as the Electricity Information Sharing and Analysis Center (E-ISAC) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and to begin an effective response.

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

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

TABLE 10.—Objectives and Practices for the Threat and Vulnerability Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Identify and Respond to Threats		
MIL1	a) Information sources to support threat management activities are identified (e.g., E-ISAC, ICS-CERT, US-CERT, InfraGard, industry associations, other public-private partnerships, vendors, Federal briefings). b) Cybersecurity threat information is gathered and interpreted for the function. c) Threats considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status).	• Cybersecurity Risk Assessment (p. 7)
MIL2	d) A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function. e) Threat information sources that address all components of the threat profile are prioritized and monitored. f) Identified threats are analyzed and prioritized. g) Threats are addressed according to the assigned priority.	• Assessment Tools and Methodologies (p. 8)
MIL3	h) The threat profile for the function is validated at an organization-defined frequency. i) Analysis and prioritization of threats are informed by the function's (or organization's) risk criteria (RM-1c). j) Threat information is added to the risk register (RM-2j).	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
2. Monitoring and Mitigating Cybersecurity Vulnerabilities		
MIL1	a) Information sources to support cybersecurity vulnerability discovery are identified (e.g., E-ISAC, ICS-CERT, US-CERT, InfraGard, industry associations, vendors, Federal briefings, internal assessments). b) Cybersecurity vulnerability information is gathered and interpreted for the function. c) Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches).	• Risk Management Strategies
MIL2	d) Cybersecurity vulnerability information sources that address all assets important to the function are monitored. e) Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools). f) Identified cybersecurity vulnerabilities are analyzed and prioritized (e.g., NIST Common Vulnerability Scoring System could be used for patches, internal guidelines could be used to prioritize other types of vulnerabilities). g) Cybersecurity vulnerabilities are addressed according to the assigned priority. h) Operational effect to the function is evaluated prior to deploying cybersecurity patches.	
MIL3	i) Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency. j) Cybersecurity vulnerability assessments are informed by the function's (or organization's) risk criteria (RM-1c). k) Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function. l) Analysis and prioritization of cybersecurity vulnerabilities are informed by the function's (or organization's) risk criteria (RM-1c). m) Cybersecurity vulnerability information is added to the risk register (RM-2j). n) Risk-monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches or other activities).	

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for threat and vulnerability management activities. b) Stakeholders for threat and vulnerability management activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support threat and vulnerability management activities. d) Standards and/or guidelines have been identified to inform threat and vulnerability management activities.	
MIL3	e) Threat and vulnerability activities are guided by documented policies or other organizational directives. f) Threat and vulnerability management policies include compliance requirements for specified standards and/or guidelines. g) Threat and vulnerability management activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of threat and vulnerability management activities are assigned to personnel. i) Personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities.	

7.5 Situational Awareness

Purpose: Establish and maintain activities and technologies to collect, analyze, alarm, present, and use cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP) commensurate with the risk to critical infrastructure and organizational objectives.

Situational awareness involves developing near real-time knowledge of a dynamic operating environment. In part, this is accomplished through the logging and monitoring of IT, OT, and communication infrastructure assets essential for the delivery of the function. It is equally important to maintain knowledge of relevant, current cybersecurity events external to the enterprise. Once an organization develops a COP, it can align predefined states of operation to changes in the operating environment. Rapid shifts among predetermined emergency operations can enable faster and more effective response to cybersecurity events.

The Situational Awareness (SA) domain has four objectives:

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

Logging should be enabled based on the assets' potential effect to the function. For example, the greater the potential effect 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 a function's current state of cybersecurity.

Example: Situational Awareness

Anywhere USA Hydro identified the assets that are essential to the delivery of the organization's functions. Additionally, the personnel monitor a number of resources that provide reliable cybersecurity information, including their vendors, ES-ISAC, and US-CERT.

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

When the COP suggests a need for heightened security, visitors are screened more carefully, the Helpdesk conducts malware scans on misbehaving laptops, and HR sends out reminders about phishing. Senior management reviews the COP and is prepared should extraordinary action—such as shutting down the website—be required. At the highest state of alert, they change firewall rule sets to restrict nonessential protocols such as video conferencing, delay all but emergency change requests, and put the cybersecurity incident response team on standby.

TABLE 11.—Objectives and Practices for the Situational Awareness Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Perform Logging		
MIL1	a) Logging is occurring for assets important to the function where possible.	
MIL2	b) Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability]). c) Log data are being aggregated within the function.	
MIL3	d) Logging requirements are based on the risk to the function. e) Log data support other business and security processes (e.g., incident response, asset management).	
2. Perform Monitoring		
MIL1	a) Cybersecurity monitoring activities are performed (e.g., regular/daily reviews of log data). b) Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event.	
MIL2	c) Monitoring and analysis requirements have been defined for the function and address timely review of event data. d) Alarms and alerts are configured to aid in the identification of cybersecurity events (IR-1b). e) Indicators of anomalous activity have been defined and are monitored across the operational environment. f) Monitoring activities are aligned with the function's threat profile (TVM-1d).	
MIL3	g) Monitoring requirements are based on the risk to the function. h) Monitoring is integrated with other business and security processes (e.g., incident response, asset management). i) Continuous monitoring is performed across the operational environment to identify anomalous activity. j) Risk register (RM-2j) content is used to identify indicators of anomalous activity. k) Alarms and alerts are configured according to indicators of anomalous activity.	

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Establish and Maintain a Common Operating Procedure (COP)		
MIL1	No practice at MIL1	
MIL2	a) Methods of communicating the current state of cybersecurity for the function are established and maintained. b) Monitoring data are aggregated to provide an understanding of the operational state of the function (i.e., a COP; a COP may or may not include visualization or be presented graphically). c) Information from across the organization is available to enhance the COP.	
MIL3	d) Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the COP. e) Information from outside the organization is collected to enhance the COP. f) Predefined states of operation are defined and invoked (manual or automated process) based on the COP.	
4. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for logging, monitoring, and COP activities. b) Stakeholders for logging, monitoring, and COP activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities. d) Standards and/or guidelines 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. f) Logging, monitoring, and COP policies include compliance requirements for specified standards and/or guidelines. g) Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel. i) Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities.	

7.6 Information Sharing and Communications

Purpose: Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience commensurate with the risk to critical infrastructure and organizational objectives.

The objective of information sharing is to strengthen cybersecurity by establishing and maintaining a framework for interaction among utilities, as well as between utilities and the government.

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

1. Share Cybersecurity Information
2. Management Activities

Sharing cybersecurity information begins with gathering cybersecurity information relevant to the function. This information is available from many sources, including vendors, government entities, and peers. Secure sharing of different types of risk-related information is essential to the well-being of individual organizations and the sector. As threats are responded to and vulnerabilities are discovered, utilities should ensure that relevant data is effectively and appropriately shared so that peers may also reduce their risk and improve grid resilience. Many forums can facilitate this sharing:

- HSIN-CI Dams Portal
- ICS-CERT
- US-CERT
- E-ISAC and Multi-State Information Sharing & Analysis Center (MS-ISAC)
- InfraGard
- Federal Bureau of Investigation (FBI) Joint Terrorism Task Force
- FBI eGuardian unclassified threat tracking system
- State and major urban area fusion centers
- Cyber Information Sharing and Collaboration Program (CISCP)
- Other public-private partnerships

Example: Information Sharing and Communications

Anywhere USA Hydro worked with its regional entity, its regional transmission organization, and trade groups to find and maintain informal connections with other utilities. This 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 facility decided to formalize ties to industry groups that will inform it of news and issues; engage with vendors with whom they have significant investment; and participate with regional, State, and Federal government organizations that advance thought leadership and practical guidance.

As part of this effort, Anywhere USA Hydro partners with others to establish a secure, confidential, information-sharing environment that enables utilities to share cybersecurity information without attribution. Within this environment, utilities are free to disclose cybersecurity information and to share technical expertise to overcome cybersecurity challenges.

TABLE 12.—Objectives and Practices for the Information Sharing and Communications Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Share Cybersecurity Information		
MIL1	a) Information is collected from and provided to selected individuals and/or organizations (see list of forums on previous page) as applicable to the organization, considering regulatory reporting obligations and voluntary sharing among industry associations. b) Responsibility for cybersecurity reporting obligations (e.g., internal reporting, Federal Energy Regulatory Commission (FERC) Standards Authorization Request (SAR), DOE Form OE-417, law enforcement) is assigned to personnel.	• Cybersecurity Awareness (p. 16) • Cybersecurity Information Sharing
MIL2	c) Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected utilities, vendors, sector organizations, regulators, internal entities). d) Information is collected from and provided to identified information-sharing stakeholders. e) Technical sources are identified that can be consulted on cybersecurity issues. f) Provisions are established and maintained to enable secure sharing of sensitive or classified information. g) Information-sharing practices address both standard operations and emergency operations.	• Information Security Classifications (p. 17)
MIL3	h) Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure. i) The function or the organization participates with information sharing and analysis centers. j) Information-sharing requirements have been defined for the function and address timely dissemination of cybersecurity information. k) Procedures are in place to analyze and de-conflict received information. l) A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events.	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
2. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for information-sharing activities. b) Stakeholders for information-sharing activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support information-sharing activities. d) Standards and/or guidelines have been identified to inform information-sharing activities.	
MIL3	e) Information-sharing activities are guided by documented policies, subject matter experts, or other organizational directives. f) Information-sharing policies include compliance requirements for specified standards and/or guidelines. g) Information-sharing activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of information-sharing activities are assigned to personnel. i) Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities. j) Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate.	

7.7 Event and Incident Response, Continuity of Operations, and Service Restoration

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

A cybersecurity event in a system or network is any observable occurrence that is related to a cybersecurity requirement (confidentiality, integrity, or availability of assets). A cybersecurity incident is an event or series of events that significantly affects or could significantly affect critical infrastructure and/or organizational assets and services and that 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, and Service Restoration (EIR) domain has 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. Management Activities

Example: Event and Incident Response, Continuity of Operations, and Service Restoration

Anywhere USA Hydro purchased a helpdesk tracking system to log and track important cybersecurity events. On the wall in their shared working area, Anywhere USA Hydro posted a chart that identifies criteria for escalating cybersecurity events, which include who must be notified and response time objectives. When the facility 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 COP described in the Situational Awareness domain.

Anywhere USA Hydro tests its disaster recovery plan annually to ensure that it can continue to meet recovery time objectives for the subsector functions and that it has a good understanding of the restoration path for its assets.

Detecting cybersecurity events includes designating a forum for reporting events and establishing criteria for event prioritization. These criteria should align with the cybersecurity risk-management strategy discussed in the Risk Management domain, ensure consistent valuation of events, and provide a structure to differentiate between cybersecurity events and cybersecurity incidents.

Escalating cybersecurity events involves applying the criteria discussed in the Detect Cybersecurity Events objective and identifying when cybersecurity events need to be managed according to a response plan. These escalated cybersecurity events, including 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 effects of cybersecurity events to sector functions. The process should describe how the organization manages all phases of the incident life cycle (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 sector function 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 realistic and practicable.

TABLE 13.—Objectives and Practices for the Event and Incident Response, Continuity of Operations, and Service Restoration Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Detect Cybersecurity Events		
MIL1	a) There is a point of contact (person or role) to whom cybersecurity events could be reported. b) Detected cybersecurity events are reported. c) Cybersecurity events are logged and tracked (see practice SA-1a).	• Incident Response (p. 19)
MIL2	d) Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events). e) There is a repository where cybersecurity events are logged based on the established criteria.	• (See above)
MIL3	f) Event information is correlated to support incident analysis by identifying patterns, trends, and other common features. g) Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RM-2j) and threat profile (TVM-1d) to help detect known threats and monitor for identified risks. h) The common operating picture for the function is monitored to support the identification of cybersecurity events (SA-3a).	• (See above)
2. Escalate Cybersecurity Events and Declare Incidents		
MIL1	a) Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria. b) Cybersecurity events are analyzed to support escalation and the declaration of cybersecurity incidents. c) Escalated cybersecurity events and incidents are logged and tracked.	• Incident Response (p. 19)
MIL2	d) Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are established based on the potential effect to the function. e) Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency. f) There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure.	• (See above)
MIL3	g) Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization's risk register (RM-2j) and threat profile (TVM-1d). h) Escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (SA-3a) for the function. i) Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features.	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Respond to Incidents and Escalated Cybersecurity Events		
MIL1	a) Cybersecurity event and incident response personnel are identified and roles are assigned. b) Responses to escalated cybersecurity events and incidents are implemented to limit effects to the function and to restore normal operations. c) Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, DOE Form OE-417, E-ISAC, ICS-CERT).	• Incident Response (p. 19)
MIL2	d) Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life cycle (e.g., triage, handling, communication, coordination, and closure). e) Cybersecurity event and incident response plans are exercised at an organization-defined frequency. f) Cybersecurity event and incident response plans address OT and IT assets important to the delivery of the function g) Training is conducted for cybersecurity event and incident response teams.	• (See above)
MIL3	h) Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken. a) Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including support for evidence collection and preservation. i) Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents). j) Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency. k) Cybersecurity event and incident response activities are coordinated with relevant external entities. l) Cybersecurity event and incident response plans are aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d). m) Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform to applicable laws, regulations, and contractual agreements. n) Restored assets are configured appropriately and inventory information is updated following execution of response plans.	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
4. Plan for Continuity		
MIL1	a) The activities necessary to sustain minimum operations of the function are identified. b) The sequence of activities necessary to return the function to normal operation is identified. c) Continuity plans are developed to sustain and restore operation of the function.	• Continuity of Operations (p. 20) • Disaster Recovery (p. 20)
MIL2	d) Business impact analyses inform the development of continuity plans. e) Recovery time objectives (RTO) and recovery point objectives (RPO) for the function are incorporated into continuity plans. f) Continuity plans are evaluated and exercised.	• (See above)
MIL3	g) Business impact analyses are periodically reviewed and updated. h) RTO and RPO are aligned with the function's risk criteria (RM-1c). i) The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly. j) Continuity plans are periodically reviewed and updated. k) Restored assets are configured appropriately and inventory information is updated following execution of continuity plans.	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
5. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for cybersecurity event and incident response as well as continuity of operations activities. b) Stakeholders for cybersecurity event and incident response as well as continuity of operations activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity of operations activities. d) Standards and/or guidelines have been identified to inform cybersecurity event and incident response as well as continuity of operations activities.	
MIL3	e) Cybersecurity event and incident response as well as continuity of operations activities are guided by documented policies or other organizational directives. f) Cybersecurity event and incident response as well as continuity of operations policies include compliance requirements for specified standards and/or guidelines. g) Cybersecurity event and incident response as well as continuity of operations activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of cybersecurity event and incident response as well as continuity of operations activities are assigned to personnel. i) Personnel performing cybersecurity event and incident response as well as continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities.	

7.8 Vendor Security Management

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

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

Supplier dependencies are external parties on which the delivery of the function depends, including operating partners. Customer dependencies are external parties that depend on the delivery of the function, including operating partners.

Supply chain risk is a noteworthy example of a supplier dependency. The cybersecurity characteristics of products and services vary widely. Without proper risk management, they pose serious threats, including software of unknown provenance and counterfeit (possibly malicious) hardware. Utilities' requests for proposal often give suppliers of high-technology systems, devices, and services only rough specifications, which may lack adequate requirements for security and quality assurance. The autonomy utilities 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 Vendor Security Management (VSM) domain has three objectives:

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

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

Managing dependency risk includes approaches, such as independent testing, code review, scanning for vulnerabilities, and reviewing demonstrable evidence from the vendor that a secure software development process has been followed. Contracts binding the facility 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.

Example: Vendor Security Management

Anywhere USA Hydro receives products and services from multiple vendors. As part of a recent initiative to support advanced metering infrastructure (AMI), the facility began to work with a new AMI vendor that, during the normal course of business, will have access to sensitive data and systems.

Within the contract for the project, Anywhere USA Hydro mandated the nondisclosure of sensitive data. Anywhere USA Hydro also specified cybersecurity requirements for the handling, communication, and storage of its information, requiring that it 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 USA Hydro's systems and data during deployment, operations, and maintenance. Additionally, Anywhere USA Hydro conducted a review of the vendor's practices (including the vendor's cybersecurity practices with respect to its suppliers), participated in a security design review of the vendor's proposed system, and plans to conduct periodic audits of the delivered AMI system to ensure that the vendor continues to meet its obligations.

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

Service level agreements can specify monitoring and audit processes to verify that vendors and service providers meet cybersecurity and other performance measures.

TABLE 14.—Objectives and Practices for the Vendor Security Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Identify Dependencies		
MIL1	a) Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners). b) Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners).	• Vendor Security (p.15)
MIL2	c) Supplier dependencies are identified according to established criteria. d) Customer dependencies are identified according to established criteria. e) Single-source and other essential dependencies are identified. f) Dependencies are prioritized.	• (See above)
MIL3	g) Dependency prioritization and identification are based on the function's or organization's risk criteria (RM-1c).	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
2. Manage Dependency Risk		
MIL1	a) Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed. b) Cybersecurity requirements are considered when establishing relationships with suppliers and other third parties.	• Vendor Security (p.15)
MIL2	c) Identified cybersecurity dependency risks are entered into the risk register (RM-2j). d) Contracts and agreements with third parties incorporate sharing of cybersecurity threat information. e) Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate. f) Agreements with suppliers and other external entities include cybersecurity requirements. g) Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements. h) Agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service. i) Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements.	• (See above)
MIL3	j) Cybersecurity risks due to external dependencies are managed according to the organization's risk-management criteria and process. k) Cybersecurity requirements are established for supplier dependencies based on the organization's risk criteria (RM-1c). l) Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products. m) Acceptance testing of procured assets includes testing for cybersecurity requirements. n) Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services).	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
3. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for managing dependency risk. b) Stakeholders for managing dependency risk are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support dependency risk-management activities. d) Standards and/or guidelines have been identified to inform managing dependency risk.	
MIL3	e) Dependency risk-management activities are guided by documented policies or other organizational directives. f) Dependency risk-management policies include compliance requirements for specified standards and/or guidelines. g) Dependency risk-management activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of dependency risk management are assigned to personnel. i) Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities.	

7.9 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 critical infrastructure and organizational objectives.

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

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

The Workforce Management (WM) domain has five objectives:

1. Assign Cybersecurity Responsibilities
2. Control the Workforce Life Cycle
3. Develop Cybersecurity Workforce
4. Increase Cybersecurity Awareness
5. Management Activities

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

Example: Workforce Management

Anywhere USA Hydro determines that it will invest in advanced digital technology. Part of this investment will be a long-term program for workforce training and management to help personnel keep the new systems running efficiently and securely. Anywhere USA Hydro 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, Anywhere USA Hydro finds that its brand of new digital technology has been compromised at another facility due to poor security practices.

Anywhere USA Hydro analyzes this information through a risk 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 USA Hydro begins investing in technical and security training and in certification for management and personnel to instill the awareness and skills necessary to manage and protect the company's assets, which may also contribute to the protection of interconnected critical infrastructure external to the facility.

Controlling the workforce life cycle 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 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 to protect these systems from accidental or malicious behavior by this category of personnel.

Developing a 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, newly recruited personnel (and contractors) should receive security awareness training to reduce their vulnerability to social engineering and other threats.

Increasing the cybersecurity awareness of the workforce is as important as implementing technological approaches to improving the cybersecurity of the organization. The threat of a cyberattack to an organization often starts with gaining

some foothold into a company's IT or OT systems—for example by gaining the trust of an unwary employee or contractor who then introduces media or devices into the facility's networks. The organization should share information with its 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 facility to potential adversaries. For example, an internal website could provide information about new threats and vulnerabilities in the Dams Sector. If information on threats, vulnerabilities, and best practices is not shared with the workforce, personnel may become more lax about security processes and procedures.

TABLE 15.—Objectives and Practices for the Workforce Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Assign Cybersecurity Responsibilities		
MIL1	a) Cybersecurity responsibilities for the function are identified. b) Cybersecurity responsibilities are assigned to specific people.	• Personnel Security Practices (Dams Sector Security Guidelines)
MIL2	c) Cybersecurity responsibilities are assigned to specific roles, including external service providers. d) Cybersecurity responsibilities are documented (e.g., in position descriptions).	• (See above)
MIL3	e) Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate. f) Cybersecurity responsibilities are included in job performance evaluation criteria. g) Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage.	• (See above)

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
2. Control the Workforce Life Cycle[6]		
MIL1	a) Personnel vetting (e.g., background checks, drug tests) is performed at hire for positions that have access to the assets required for delivery of the function. b) Personnel termination procedures address cybersecurity.	• Personnel Security Practices (Dams Sector Security Guidelines)
MIL2	c) Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of the function. d) Personnel transfer procedures address cybersecurity.	• (See above)
MIL3	e) Risk designations are assigned to all positions that have access to the assets required for delivery of the function. f) Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation. g) Succession planning is performed for personnel based on risk designation. h) A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures.	• (See above)
3. Develop Cybersecurity Workforce		
MIL1	a) Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities.	• Personnel Security Practices (Dams Sector Security Guidelines)
MIL2	b) Cybersecurity knowledge, skill, and ability gaps are identified. c) Identified gaps are addressed through recruiting and/or training. d) Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training).	• (See above)
MIL3	e) Cybersecurity workforce management objectives that support current and future operational needs are established and maintained. f) Recruiting and retention are aligned to support cybersecurity workforce management objectives. g) Training programs are aligned to support cybersecurity workforce management objectives. h) The effectiveness of training programs is evaluated at an organization-defined frequency and improvements are made as appropriate. i) Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities.	• (See above)

[6] Additional practices that support personnel access control and help to manage insider threat are included in the Identity and Access Management domain.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
4. Increase Cybersecurity Awareness		
MIL1	a) Cybersecurity awareness activities occur.	• Personnel Security Practices (Dams Sector Security Guidelines)
MIL2	b) Objectives for cybersecurity awareness activities are established and maintained. c) Cybersecurity awareness content is based on the organization's threat profile (TVM-1d).	• (See above)
MIL3	d) Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f). e) The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate.	• (See above)

Note: In the following practices, “cybersecurity workforce management activities” refers collectively to all of the above practices in this domain.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
5. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for cybersecurity workforce management activities. b) Stakeholders for cybersecurity workforce management activities are identified and involved. c) Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities. d) Standards and/or guidelines have been identified to inform cybersecurity workforce management activities.	
MIL3	e) Cybersecurity workforce management activities are guided by documented policies or other organizational directives. f) Cybersecurity workforce management policies include compliance requirements for specified standards and/or guidelines. g) Cybersecurity workforce management activities are periodically reviewed to ensure conformance with policy. h) Responsibility and authority for the performance of cybersecurity workforce management activities are assigned to personnel. i) Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities.	

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

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

The Cybersecurity Program Management (CPM) domain has five objectives:

1. Establish Cybersecurity Program Strategy
2. Sponsor Cybersecurity Program
3. Establish and Maintain Cybersecurity Architecture
4. Perform Secure Software Development
5. Management Activities

The cybersecurity program strategy is established as the foundation for the program. In its simplest form, the program strategy should include a list of cybersecurity objectives and the policies and standards required 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, education and training needed, and more involvement by senior management in the design of the program.

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

Example: Cybersecurity Program Management

Anywhere USA Hydro decided to establish an enterprise cybersecurity program. To begin, Anywhere USA Hydro formed a board with representation from each of the functional areas. This cybersecurity governance board will develop a cybersecurity strategy for the facility and will 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 USA Hydro, ensuring that it remains aligned to the facility's business strategy and addresses its risk to critical infrastructure. Once the strategy is approved by the board, the new vice president will begin implementing the program by reorganizing some existing compartmentalized cybersecurity teams and recruiting additional team members to address skill gaps in the organization.

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

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 subordinate organizations and aligns them with the organization's mission and strategic plans. An important element of the cybersecurity architecture is effective isolation of IT systems from OT systems.

Performing and requiring secure software development for assets that are important to the delivery of the function is important to help reduce vulnerability-inducing software defects.

TABLE 16.—Objectives and Practices for the Cybersecurity Program Management Domain.

Note: Organizations that do not perform MIL1 practices for an objective are evaluated as MIL0 for that objective.

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
1. Establish Cybersecurity Program Strategy		
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, including policies and standards. 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—including policies and standards—is updated to reflect business changes, changes in the operating environment and changes in the threat profile (TVM-1d).	

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
2. Sponsor Cybersecurity Program		
MIL1	a) Resources (people, tools, and funding) are provided to support the cybersecurity program. b) Senior management provides sponsorship for the cybersecurity program.	
MIL2	c) The cybersecurity program is established according to the cybersecurity program strategy. d) Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a cybersecurity program aligned with the program strategy. 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). f) If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program. g) The development and maintenance of cybersecurity policies is sponsored. 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. j) The cybersecurity program is independently reviewed (i.e., by reviewers who are not in the program) for achievement of cybersecurity program objectives. k) The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate. l) The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives.	
3. Establish and Maintain Cybersecurity Architecture		
MIL1	a) A strategy to architecturally isolate the organization's IT systems from OT systems is implemented.	
MIL2	b) A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy. c) Architectural segmentation and isolation are maintained according to a documented plan.	
MIL3	d) Cybersecurity architecture is updated at an organization-defined frequency to keep it current.	

Objectives and Practices		Dams Sector Cybersecurity Program Guidance Reference
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 the function is developed using secure software development practices.	
MIL3	b) Policies require that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices.	
5. Management Activities		
MIL1	No practice at MIL1	
MIL2	a) Documented practices are followed for cybersecurity program management activities. b) Stakeholders for cybersecurity program management activities are identified and involved. c) Standards and/or guidelines have been identified to inform cybersecurity program management activities.	
MIL3	d) Cybersecurity program management activities are guided by documented policies or other organizational directives. e) Cybersecurity program management activities are periodically reviewed to ensure conformance with policy. f) Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities.	

Appendix A: Source Documents

Sector Documents

Cybersecurity Procurement Language for Energy Delivery Systems, Washington, D.C.: U.S. Department of Energy, Energy Sector Control Systems Working Group, 2014, http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf (accessed November 14, 2016).

Dams Sector Cybersecurity Framework Implementation Guide, Washington, D.C.: U.S. Department of Homeland Security, 2015. Please contact dams@hq.dhs.gov to access the document.

Dams Sector Roadmap to Secure Control Systems, Washington, D.C.: U.S. Department of Homeland Security, 2010. Please contact dams@hq.dhs.gov to access the document.

Dams Sector Cybersecurity Guidelines, Washington, D.C.: U.S. Department of Homeland Security, 2016. Please contact dams@hq.dhs.gov to access the document.

Dams Sector Security Guidelines, Washington, D.C.: U.S. Department of Homeland Security, 2015. Please contact dams@hq.dhs.gov to access the document.

Dams Sector-Specific Plan: An Annex to the NIPP 2013, Washington, D.C.: U.S. Department of Homeland Security, 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf (accessed November 14, 2016).

Energy Sector Cybersecurity Framework Implementation Guidance, Washington, D.C.: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, 2015, http://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf (accessed November 14, 2016).

Principles and Resources for Managing Supply Chain Cybersecurity Risk, Washington, D.C.: Edison Electric Institute, 2015, http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf (accessed November 14, 2016).

Federal Agency Guidelines

Critical Infrastructure Protection Reliability Standards, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2016, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed November 14, 2016).

Electricity Subsector Cybersecurity Risk Management Process, Washington, D.C.: U.S. Department of Energy, 2012, http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf (accessed November 14, 2016).

FERC Security Program for Hydropower Projects: Revision 3A, Washington, D.C.: Federal Energy Regulatory Commission, Division of Dam Safety and Inspections, 2016, https://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf (accessed November 14, 2016).

FERC Security Program for Hydropower Projects FAQ, Washington, D.C.: Federal Energy Regulatory Commission, Division of Dam Safety and Inspections, 2016, http://www.ferc.gov/industries/hydropower/safety/guidelines/security/faq.pdf (accessed November 14, 2016).

Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0, Gaithersburg, MD: National Institute of Standards and Technology, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed November 14, 2016).

Pipeline Security Guidelines, Washington, D.C.: Transportation Security Administration, 2011, https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf (accessed November 14, 2016).

Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2010, http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf (accessed November 14, 2016).

Security Guideline for the Electricity Sector: Protecting Sensitive Information, Washington, D.C.: North American Electric Reliability Corporation (NERC), 2012, http://www.nerc.com/comm/CIPC/Protecting%20Sensitive%20Information%20Guideline%20Task1/Protecting%20Sensitive%20Information%20Guideline%20(PSIGTF).pdf (accessed November 14, 2016).

NIST Computer Security Special Publications:

Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (NIST 800-53A), Gaithersburg, MD: National Institute of Standards and Technology, 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf (accessed November 14, 2016).

Computer Security Incident Handling Guide (NIST 800-61), Gaithersburg, MD: National Institute of Standards and Technology, 2012, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (accessed November 14, 2016).

Contingency Planning Guide for Federal Information Systems: Revision 1 (NIST 800-34), Gaithersburg, MD: National Institute of Standards and Technology, 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf (accessed November 14, 2016).

Guide for Conducting Risk Assessments: Revision 1 (NIST 800-30), Gaithersburg, MD: National Institute of Standards and Technology, 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed November 14, 2016).

Guide to Industrial Control Systems (ICS) Security (NIST 800-82), Gaithersburg, MD: National Institute of Standards and Technology, 2011, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf (accessed November 14, 2016).

Appendix B: Glossary

Term	Definition	Source
access	Ability and means to enter a facility, to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	Adapted from CNSSI 4009
access control	Limiting access to organizational assets only to authorized entities (e.g., users, programs, processes, or other systems). See *asset*.	Adapted from CNSSI 4009
access management	Management processes to ensure that access granted to the organization's assets is commensurate with the risk to critical infrastructure and organizational objectives. See *access control* and *asset*.	Adapted from CERT RMM
ad hoc	In the context of this model, *ad hoc* (i.e., an ad hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. The methods, tools, and techniques used, the priority given a particular instance of the practice, and the quality of the outcome may vary significantly depending on who is performing the practice, when it is performed, and the context of the problem being addressed. With experienced and talented personnel, high-quality outcomes may be achieved even though practices are ad hoc. However, because lessons learned are typically not captured at the organizational level, approaches and outcomes are difficult to repeat or improve across the organization.	Dams-C2M2
anomalous/anomaly	Inconsistent with or deviating from what is usual, normal, or expected.	Merriam-Webster.com
architecture	See *cybersecurity architecture.*	
assessment	See *risk assessment.*	
asset	Something of value to the organization. Assets include many things, such as technology, information, roles performed by personnel, and facilities. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.	

Term	Definition	Source
asset, change, and configuration management (ACM)	The Dams-C2M2 domain with the purpose to manage the organization's OT and IT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2
asset owner	A person or organizational unit, internal or external to the organization, that has primary responsibility for the viability, productivity, and resilience of an organizational asset.	CERT RMM
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IT or ICS.	DOE RMP
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).	NIST 800-53
Availability	Ensuring timely and reliable access to and use of information. For an asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed.	DOE RMP & CERT RMM
business impact analysis	A mission impact analysis that prioritizes the effects associated with the compromise of an organization's information assets, based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets.	Adapted from NIST SP800-30
change control (change management)	A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption.	CERT RMM
common operating picture	Activities and technologies to collect, analyze, alarm, present, and use cybersecurity information, including status and summary information from the other model domains.	Dams-C2M2
computer security incident	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet. Also, see *incident.*	NIST 800-61 (computer security incident)
confidentiality	The preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. For an information asset, confidentiality is the quality of being accessible only to authorized people, processes, and devices.	DOE RMP & Adapted from CERT RMM

Term	Definition	Source
configuration baseline	A documented set of specifications for an IT or OT system or asset, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time, and which should be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.	Adapted from NIST 800-53 Glossary
configuration management	A collection of activities focused on establishing and maintaining the integrity of assets, through control of the processes for initializing, changing, and monitoring the configurations of those assets throughout their life cycle.	NIST SP 800-128
contingency plan	Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The contingency plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the continuity of operations plan or disaster recovery plan for major disruptions.	CNSSI 4009
continuous monitoring	Maintaining ongoing awareness of the current cybersecurity state of the function throughout the operational environment by collecting, analyzing, alarming, presenting, and using cybersecurity information to identify anomalous activities, vulnerabilities, and threats to the function to support incident response and organizational risk-management decisions.	Adapted from NIST 800-137
controls	The management, operational, and technical methods, policies, and procedures—manual or automated—(i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information.	DOE RMP
critical infrastructure	Assets that provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction through terrorist attack could have a debilitating effect on security and economic well-being.	HSPD-7
current	Updated at an organization-defined frequency (e.g., as in the asset inventory is kept “current”) that is selected such that the risks to critical infrastructure and organization objectives associated with being out-of-date by the maximum interval between updates are acceptable to the organization and its stakeholders.	Dams-C2M2

Term	Definition	Source
cyberattack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or for destroying the integrity of the data or stealing controlled information.	DOE RMP
cybersecurity	The ability to protect or defend the use of cyberspace from cyberattacks. Measures taken to protect a computer or computerized system (IT and OT) against unauthorized access or attack.	DOE RMP and Merriam-Webster.com
cybersecurity architecture	An integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, cybersecurity systems, personnel, and subordinate organizations, showing their alignment with the organization's mission and strategic plans. See *enterprise architecture* and *network architecture*.	DOE RMP
cybersecurity event	Any observable occurrence in a system or network that is related to a cybersecurity requirement (confidentiality, integrity, or availability). See also *event*.	Dams-C2M2
cybersecurity impact	The effect on the measures that are in place to protect from and defend against cyberattack.	Dams-C2M2
cybersecurity incident	See *incident.*	
cybersecurity incident life cycle	See *incident life cycle.*	
cybersecurity plan	Formal document that provides an overview of the cybersecurity requirements for an IT and ICS and describes the cybersecurity controls in place or planned for meeting those requirements.	DOE RMP
cybersecurity policy	A set of criteria for the provision of security services.	DOE RMP
cybersecurity program	A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization and/or the function. A cybersecurity program may be implemented at either the organization or the function level, but a higher-level implementation and enterprise viewpoint may benefit the organization by integrating activities and leveraging resource investments across the entire enterprise.	Dams-C2M2
cybersecurity program management (CPM)	The Dams-C2M2 domain with the purpose to establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.	Dams-C2M2

Term	Definition	Source
cybersecurity program strategy	A plan of action designed to achieve the performance targets that the organization sets to accomplish its mission, vision, values, and purpose for the cybersecurity program.	CERT RMM
cybersecurity requirements	Requirements levied on an IT and OT that are derived from organizational mission and business case needs (in the context of applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, procedures) to ensure the confidentiality, integrity, and availability of the services being provided by the organization and the information being processed, stored, or transmitted.	Adapted from DOE RMP
cybersecurity responsibilities	Obligations for ensuring the organization's cybersecurity requirements are met.	Dams-C2M2
cybersecurity risk	The risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS. See *risk*.	DOE RMP
cybersecurity workforce management objectives	Performance targets for personnel with cybersecurity responsibilities that the organization sets to meet cybersecurity requirements.	Adapted from CERT RMM
defined practice	A practice that is planned (i.e., described, explained, made definite and clear, and standardized) and is executed in accordance with the plan.	Adapted from CERT RMM
dependency risk	Dependency risk is measured by the likelihood and severity of damage if an IT or OT system is compromised due to a supplier or other external party on which delivery of the function depends. Evaluating dependency risk includes an assessment of the importance of the potentially compromised system and the effect of compromise on organizational operations and assets, individuals, other organizations, and the Nation. See *upstream dependencies* and *supply chain risk.*	Adapted from NIST 7622, pg. 10
deprovisioning	The process of revoking or removing an identity's access to organizational assets. See also *provisioning.*	CERT RMM
distribution	The delivery of energy to retail customers (e.g., homes, businesses, industry, government facilities).	Adapted from EIA Glossary
domain	In the context of the model structure, a domain is a logical grouping of cybersecurity practices.	Dams-C2M2
domain objectives	The practices within each domain are organized into objectives. The objectives represent achievements that support the domain (such as "Manage Asset Configuration" for the ACM domain and "Increase Cybersecurity Awareness" for the WM domain). Each of the objectives in a domain has a set of practices, which are ordered by maturity indicator level.	Dams-C2M2

Term	Definition	Source
downstream dependencies	External parties dependent on the delivery of the function, such as customers and some operating partners.	Dams-C2M2
enterprise	The largest (i.e., highest-level) organizational entity to which the organization participating in the Dams-C2M2 survey belongs. For some participants, the organization taking the survey is the enterprise itself. See organization.	Adapted from SGMM v1.1 Glossary
enterprise architecture	The design and description of an enterprise's entire set of IT and OT: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. See cybersecurity architecture and network architecture.	DOE RMP (but changed ICS to OT)
Entity	Something having separate or distinct existence.	Merriam-Webster.com
establish and maintain	The development and maintenance of the object of the practice (such as a program). For example, "Establish and maintain identities" means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements.	CERT RMM
Event	Any observable occurrence in a system or network. Depending on their potential impact, some events need to be escalated for response. To ensure consistency, criteria for response should align with the organization's risk criteria.	NIST 800-61
event and incident response, continuity of operations (IR)	The Dams-C2M2 domain with the purpose to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2
function	The high-level system activity or set of activities performed by the facility to which the model is being applied.	Dams-C2M2
generation	The process of producing electric energy by transforming other forms of energy; also, the amount of electric energy produced, expressed in kilowatt-hours.	EIA Glossary

Term	Definition	Source
governance	An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organization is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).	Adapted from CERT RMM
guidelines	A set of recommended practices produced by a recognized authoritative source representing subject matter experts and community consensus, or internally by an organization. See *standard*.	Dams-C2M2
identity	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	CNSSI 4009
identity and access management (IAM)	The Dams-C2M2 domain with the purpose to create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) critical infrastructure and/or organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse effects. See also *computer security incident* and *event.*	Adapted from CERT RMM
incident life cycle	The stages of an incident from detection to closure. Collectively, the incident life cycle includes the processes of detecting, reporting, logging, triaging, declaring, tracking, documenting, handling, coordinating, escalating and notifying, gathering and preserving evidence, and closing incidents. Escalated events also follow the incident life cycle, even if they are never formally declared to be incidents.	Adapted from CERT RMM
information assets	Information or data valuable to the organization, including diverse information such as operational data, intellectual property, customer information, and contracts.	Adapted from CERT RMM
information sharing	See *Information Sharing and Communications (ISC).*	

Term	Definition	Source
Information Sharing and Analysis Center (ISAC)	An Information Sharing and Analysis Center (ISAC) shares critical information with industry participants on infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indicators, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning.	Adapted from E-ISAC website home page
information sharing and communications (ISC)	The Dams-C2M2 domain with the purpose to establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks, and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2
information technology (IT)	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate.	DOE RMP
institutionalization	The extent to which a practice or activity is ingrained into the way an organization operates. The more an activity becomes part of how an organization operates, the more likely it is that the activity will continue to be performed over time, with a consistently high level of quality. ("Incorporated into the ingrained way of doing business that an organization follows routinely as part of its corporate culture."—CERT RMM). See also *maturity indicator level.*	Dams-C2M2
Integrity	Guarding against improper information modification or destruction. Integrity includes ensuring information nonrepudiation and authenticity. For an asset, integrity is the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner.	DOE RMP & CERT RMM

Term	Definition	Source
least privilege	A security control that addresses the potential for abuse of authorized privileges. The organization employs the concept of least privilege by allowing only authorized access for users (and processes acting on behalf of users) who require it to accomplish assigned tasks in accordance with organizational missions and business functions. Organizations employ the concept of least privilege for specific duties and systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary to achieving least privilege. Organizations also apply least privilege concepts to the design, development, implementation, and operations of IT and OT systems.	Adapted from NIST 800-53
Logging	Logging typically refers to automated recordkeeping (by elements of an IT or OT system) of system, network, or user activity. Logging may also refer to keeping a manual record (e.g., a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace. Regular review and audit of logs (manually or by automated tools) is a critical monitoring activity that is essential for situational awareness (e.g., through the detection of cybersecurity events or weaknesses).	Dams-C2M2
logical control	A software, firmware, or hardware feature (i.e., computational logic, not a physical obstacle) within an IT or OT system that restricts access to and modification of assets only to authorized entities. For contrast, see *physical control*.	Adapted from CNSSI 4009 definition of “internal security controls”
Maturity	The extent to which an organization has implemented and institutionalized the cybersecurity practices of the model.	Dams-C2M2

Term	Definition	Source
maturity indicator level (MIL)	A measure of the cybersecurity maturity of an organization in a given domain of the model. The model currently defines four maturity indicator levels (MILs) and holds a fifth level in reserve for use in future versions of the model. Each of the four defined levels is designated by a number (0 through 3) and a name, for example, "MIL3: managed." A MIL is a measure of the progression within a domain from individual and team initiative, as a basis for carrying out cybersecurity practices, to organizational policies and procedures that institutionalize those practices, making them repeatable with a consistently high level of quality. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the core activities in the domain.	Dams-C2M2
Monitoring	Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.	Adapted from CERT RMM (monitoring and risk management)
monitoring requirements	The requirements established to determine the information gathering and distribution needs of stakeholders.	CERT RMM
multifactor authentication	Authentication using two or more factors to achieve authentication. Factors include (i) something you know (e.g., password/PIN), (ii) something you have (e.g., cryptographic identification device, token), (iii) something you are (e.g., biometric), or (iv) you are where you say you are (e.g., GPS token). See *authentication*.	Adapted from NIST 800-53
network architecture	A framework that describes the structure and behavior of communications among IT and/or OT assets and prescribes rules for interaction and interconnection. See *enterprise architecture* and *cybersecurity architecture*.	Adapted from CNSSI 4009 (IA architecture)
objective(s)	*See domain objectives* and *organizational objectives*.	

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

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

Term	Definition	Source
provisioning	The process of assigning or activating an identity profile and its associated roles and access privileges. See also *deprovisioning*.	CERT RMM
recovery time objectives	Documented goals and performance targets the organization sets for recovery of an interrupted function to meet critical infrastructure and organizational objectives.	Dams-C2M2
risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.	DOE RMP
risk analysis	A risk-management activity focused on understanding the condition and potential consequences of risk, prioritizing risks, and determining a path for addressing risks. Determines the importance of each identified risk and is used to facilitate the organization's response to the risk.	Adapted from CERT RMM
risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation, resulting from the operation of an IT and ICS.	DOE RMP
risk criteria	Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on potential effects, tolerance for risk, and risk-response approaches.	Dams-C2M2
risk designation, as in "position risk designation"	An indication, such as high, medium, or low, of the position's potential for adverse impact to the efficiency, integrity, or availability of the organization's services.	Adapted from OPM
risk disposition	A statement of the organization's intention for addressing an operational risk. Typically limited to "accept," "transfer," "research," or "mitigate."	CERT RMM
risk-management program	The program and supporting processes to manage cybersecurity risk to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation. It includes (1) establishing the context for risk-related activities, (2) assessing risk, (3) responding to risk once determined, and (4) monitoring risk over time.	DOE RMP
risk management (RM)	The Dams-C2M2 domain with the purpose to establish, operate, and maintain an enterprise cybersecurity risk-management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.	Dams-C2M2
risk-management strategy	Strategic-level decisions on how senior executives manage risk to an organization's operations, resources, and other organizations.	DOE RMP
risk mitigation	Prioritizing, evaluating, and implementing appropriate risk-reducing controls.	DOE RMP

Term	Definition	Source
risk-mitigation plan	A strategy for mitigating risk that seeks to minimize the risk to an acceptable level.	CERT RMM
risk parameter/risk-parameter factors	Organization-specific risk tolerances used for consistent measurement of risk across the organization. Risk parameters include risk tolerances and risk-measurement criteria.	CERT RMM
risk register	A structured repository where identified risks are recorded to support risk management.	Dams-C2M2
risk response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, resources, and other organizations.	DOE RMP
risk taxonomy	The collection and cataloging of common risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line-of-business if operational assets and services are affected by them.	Adapted from CERT RMM
role	A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.	CNSSI 4009
secure software development	Developing software using recognized processes, secure coding standards, best practices, and tools that have been demonstrated to minimize security vulnerabilities in software systems throughout the software development life cycle. An essential aspect is to engage programmers and software architects who have been trained in secure software development.	Dams-C2M2

Term	Definition	Source
separation of duties	[A security control that] "addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Organizations with significant personnel limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls."	NIST 800-53, pp. 31, F-13
service level agreement	Defines the specific responsibilities of the service provider, including the satisfaction of any relevant cybersecurity requirements, and sets the customer's expectations regarding the quality of service to be provided.	Adapted from CNSSI 4009
situational awareness	A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity safeguards), in the context of the threat environment and risks to the system's mission, to support effective decision-making with respect to activities that depend on and/or affect how well a system functions. It involves the collection of data (e.g., via sensor networks), data fusion, and data analysis (which may include modeling and simulation) to support automated and/or human decision-making (for example, concerning operational functions). Situational awareness also involves the presentation of the results of the data analysis in a form (e.g., using data visualization techniques, appropriate use of alarms) that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision-making.	Adapted from SGMM Glossary
situational awareness (SA)	The Dams-C2M2 domain with the purpose to establish and maintain activities and technologies to collect, analyze, alarm, present, and use cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP), commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2

Term	Definition	Source
sponsorship	Enterprise-wide support of cybersecurity objectives by senior management as demonstrated by formal policy or by declarations of management's commitment to the cybersecurity program along with provision of resources. Senior management monitors the performance and execution of the cybersecurity program and is actively involved in the ongoing improvement of all aspects of the cybersecurity program.	Dams-C2M2
stakeholder	An external organization or an internal or external person or group that has a vested interest in the organization or function (that is being evaluated using this model) and its practices. Stakeholders involved in performing a given practice (or who oversee, benefit from, or are dependent on the quality with which the practice is performed) could include those from within the function, from across the organization, or from outside the organization.	Adapted from CERT RMM
standard	A standard is a document, established by consensus, that provides rules, guidelines, or characteristics for activities or their results. See *guidelines*.	Adapted from ISO/IEC Guide 2:2004
states of operation	See *pre-defined states of operation.*	
strategic objectives	The performance targets that the organization sets to accomplish its mission, vision, values, and purpose.	CERT RMM
strategic planning	The process of developing strategic objectives and plans for meeting these objectives.	CERT RMM
supply chain	The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. The supply chain encompasses the full product life cycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly affect the supply chain.	NISTIR 7622 Source of 1st paragraph cited as [NDIA ESA]

Term	Definition	Source
supply chain risk	*Supply chain risk* is measured by the likelihood and severity of damage if an IT or OT system is compromised by a supply chain attack, and takes into account the importance of the system and the effects of compromise on organizational operations and assets, individuals, other organizations, and the Nation. Supply chain attacks may involve manipulating computing system hardware, software, or services at any point during the life cycle. Supply chain attacks are typically conducted or facilitated by individuals or organizations that have access through commercial ties, leading to stolen critical data and technology, corruption of the system/ infrastructure, and/or disabling of mission-critical operations. See risks and supply chain.	Adapted from NIST 7622, pg. 7 & pg. 10
vendor security management (VSM)	The Dams-C2M2 domain with the purpose to establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2
threat	Any circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image, or reputation), resources, and other organizations through IT, OT, or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	Adapted from DOE RMP
threat and vulnerability management (TVM)	The Dams-C2M2 domain with the purpose to establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.	Dams-C2M2
threat assessment	The process of evaluating the severity of threat to an IT and ICS or organization and describing the nature of the threat.	DOE RMP
threat profile	A characterization of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT and OT of an organization and to the organization itself, delineating the feasible threats, describing the nature of the threats, and evaluating their severity.	Dams-C2M2
threat source	An intent and method targeted at the intentional exploitation of a vulnerability or a situation, or a method that may accidentally exploit a vulnerability.	DOE RMP

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

Term	Definition	Source
workforce management (WM)	The Dams-C2M2 domain with the purpose to establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.	Dams-C2M2
workforce management objectives	See *cybersecurity workforce management objectives.*	

Appendix C: Acronyms and Abbreviations

Acronym	Definition
ACM	Asset Identification, Change, and Configuration Management
AMI	advanced metering infrastructure
C2M2	Cybersecurity Capability Maturity Model
CBA	cost benefit analysis
CERT RMM	Carnegie Mellon University CERT Division Resilience Management Model
CISCP	Cyber Information Sharing and Collaboration Program
CMM	Capability Maturity Model
CNSSI	Committee on National Security Systems Instruction
COP	common operating picture
COTS	commercial off-the-shelf
CPM	Cybersecurity Program Management
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DOE	Department of Energy
Dams-C2M2	Dams Sector Cybersecurity Capability Maturity Model
EIA	U.S. Energy Information Administration
EIR	Event and Incident Response, Continuity of Operations, and Service Restoration
E-ISAC	Electricity Information Sharing and Analysis Center
EO 13636	Executive Order 13636: Improving Critical Infrastructure Cybersecurity
ES-C2M2	Energy Sector Cybersecurity Capability Maturity Model
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FERC	Federal Energy Regulatory Commission
GCC	Government Coordinating Council
HR	human resources
HSIN-CI	Homeland Security Information Network-Critical Infrastructure
HSPD	Homeland Security Presidential Directive
HVAC	heating, ventilation, and air conditioning
IAM	Identity and Access Management
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team

Acronym	Definition
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
ISC	Information Sharing and Communications
IT	Information Technology
MIL	maturity indicator level
MS-ISAC	Multi-State Information Sharing and Analysis Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Report
OPM	U.S. Office of Personnel Management
OT	operations technology
PPD-21	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
RPO	recovery point objective
RTO	recovery time objective
RM	Risk Management
RMP	Electricity Subsector Cybersecurity Risk Management Process Guideline
SA	Situational Awareness
SAR	Standards Authorization Request
SCADA	supervisory control and data acquisition
SCC	Sector Coordinating Council
SEI	Software Engineering Institute
SGMM	Smart Grid Maturity Model
TVM	Threat and Vulnerability Management
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
VSM	Vendor Security Management
WM	Workforce Management