DAMS SECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 2.0

OCTOBER 2022

Cybersecurity and Infrastructure Security Agency

Contents

Acknowledgements

The *Dams Sector Cybersecurity Capability Maturity Model* (Dams-C2M2) was developed with input, advice, and assistance from the Dams Sector Cybersecurity Work Group and council members of the Dams Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), which includes representatives from the public and private sectors.

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. In addition, 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 U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2), Version 2.1, which was developed 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) Cybersecurity and Infrastructure Security Agency (CISA), in partnership with the Dams GCC and SCC.

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

1.1 Background

The Dams-C2M2 was developed by owners and operators and government stakeholders in the Dams Sector Cybersecurity Work 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 is based on the U.S. Department of Energy (DOE) *Cybersecurity Capability Maturity Model (C2M2)*, Version 2.1, which was developed 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).

1.2 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 threat types of

concern 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.

The Dams-C2M2 is designed for self-evaluation of an organization's cybersecurity program. The Dams Sector Cybersecurity Work Group developed a companion self-evaluation Implementation Guide that helps asset owners through the assessment of their organization using the Dams-C2M2. In addition, the model can inform the development of a new cybersecurity program by identifying and prioritizing areas in which the organization can improve its cybersecurity.

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. The practices in each domain have a considerable amount of convergence. For example, protecting against insider threats will require completion of practices in the Identity and Access Management, Threat and Vulnerability Management, and Workforce Management domains. Therefore, organizations implementing the Dams-C2M2 should consider the domains and practices not as separate, rigid categories of cybersecurity maturity, but interrelated.

The Dams-C2M2 provides *descriptive* rather than *prescriptive* guidance based on best practices and standards specific to the sector. 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*.

1.3 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 type, 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.
- **Leaders** responsible for managing organizational resources and operations associated with the domains of this model (see Section 4.1 for more information on the content of each 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.

1.4 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	Chapter 1
Leaders or managers	Chapters 1, 2, 3, and 4
Practitioners	Entire document
Facilitators	Entire document

Chapter 2 provides an overview of cybersecurity in the Dams Sector. Chapter 3 describes several core concepts that are important for interpreting the content and structure of the Dams-C2M2. Chapter 4 describes the architecture of the Dams-C2M2. Chapter 5 provides guidance on how to use the model. Chapter 6 contains the model itself—the model's objectives and practices, organized into 10 domains. Appendix B includes source documents that were either used in the development of this document or provide further information about the practices identified within the model. Appendix C provides a general mapping of Dams-C2M2 objectives to other important cybersecurity references.

2. The Dams Sector Cyber Landscape

The Dams Sector delivers critical water retention and control services in the United States, including hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management, and recreation. Its key services support multiple critical infrastructure sectors and industries. Dams Sector assets include dam projects (dams), navigation locks, levees, hydropower projects, dikes, hurricane barriers, tailings dams, and other industrial waste impoundments.

Cybersecurity in the Dams Sector is focused on the control systems that monitor, automate, and control critical physical processes, (e.g., electric generation and transmission, water level and transport, and physical access control) and the enterprise information technology (IT) on which networked enterprise operations rely. The control systems—often referred to as industrial control systems (ICS)—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.

Control systems include 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 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 IT and OT systems, including their connecting networks and information.

2.1 Cyber Threats

A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Adversaries, also known as cyber threat actors, range from individual, autonomous attackers to well-resourced groups operating in a coordinated manner as part of a criminal enterprise or on behalf of a nation-state. Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to access and compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. Examples of TTPs used by threat actors to gain access to and compromise networks, systems, and devices include the following:

- Spearphishing—using email or malicious websites to solicit personal information—to obtain initial access to the organization's IT network before pivoting to the OT network
- Spearphishing personnel to deliver malicious payloads, including ransomware
- Leveraging legitimate remote monitoring and management software and remote desktop software, often by setting up trial accounts, to maintain persistence on victim networks
- Scanning target networks for critical and high vulnerabilities in major applications within days of the vulnerability's public disclosure
- Exploiting unsupported or outdated operating systems and software

- Exploiting control system devices with vulnerable firmware versions
- Exploiting the supply chain by infecting equipment prior to installation at a facility
- Masking threat actor activities by using a revolving series of virtual private servers and common open-source or commercial penetration tools

For additional information on cyber vulnerabilities, threat actor TTPs, and defensive tactics and techniques, refer to the National Cyber Awareness System alerts at us-cert.cisa.gov/ncas/alerts.

2.2 Cyberattacks

Cyber threat actors have demonstrated their continued willingness to conduct malicious cyber activity against critical infrastructure by exploiting vulnerabilities in assets. Attacks worldwide against IT and OT systems have enabled cyber espionage; theft of intellectual property and sensitive data; operational disruptions; physical consequences; and follow-on opportunities for intelligence collection, attack, or influence operations. The following summarizes the potential impacts of attacks on Dams Sector control systems and business networks, including the threat of an adversary gaining access via Internet-connected devices, the supply chain, or unpatched systems.

- **Control Systems:** Control systems are vital to the efficient and safe operation of many Dams Sector facilities because these systems typically manage, command, direct, or regulate physical processes at the facility. As the Dams Sector advances in technical complexity, increased control system automation and connectivity that can improve operability and efficiency can also introduce new cybersecurity issues. Cyberattacks on control systems are advancing in complexity, sophistication, and volume, leading to new methods of infiltration and disruption. A cyber incident affecting ICS can allow attackers to remotely direct physical processes to cause damage, disrupt operations, or cause collateral damage to essential services and nearby communities.
- **Business Networks:** A cyber incident affecting a business network (i.e., IT system) could compromise business operations or facilitate theft of sensitive business or customer information, potentially leading to operational compromises and/or significant economic losses. A skilled cyber threat actor can pivot from an IT enterprise network to an OT environment if controls are not fully implemented and monitored.
- **Internet-Connected Devices:** Commonly referred to as the Internet of Things (IoT), Internet-connected devices are becoming more commonly used in the Dams Sector for monitoring and optimizing facility processes, sharing real-time data among devices, and sending alerts for faults or deficiencies. Cyber threat actors seeking to harm or exploit Dams Sector organizations may employ external IoT devices (e.g., consumer-level appliances or network devices) in coordinated attacks for control systems surveillance, disruption of operations, or destruction of property.
- **Supply Chain:** Foreign adversaries, such as state-sponsored hackers, are increasingly using organizations and trusted suppliers as attack vectors against critical infrastructure to steal intellectual property, conduct espionage, and carry out sabotage.
  - **Vendors:** Dams Sector assets and networks are susceptible to compromised vendor communications associated with the supply chain. Email phishing attempts from presumed trusted vendor email accounts are becoming more frequent. Successful phishing attempts could allow attackers remote access to enterprise networks and the opportunity to escalate attacks to operations infrastructure. Trusted contractors and vendors may have legitimate remote access to provide services. However, this access could turn problematic if the contractor or vendor has been compromised.

  - **Software:** Information and communications technology systems underpin a broad range of critical infrastructure activities that support the delivery of project benefits. If vulnerabilities in these systems and their critical hardware and software are exploited, the consequences can have cascading impacts across organizations and sectors.

- **Unpatched Systems:** Corporate IT systems not updated with current security patches (for operating systems or software) are a significant cybersecurity issue for the Dams Sector. Some software providers might not provide software patches because the providers lack the ability to distribute patches, or the software is beyond the support life cycle and no longer supported. Owners and operators might not implement available patches to update devices because the updates would interrupt operations or have unexpected consequences in critical assets. Processing, tracking, and managing patches for alerts from multiple software vendors can be challenging, especially when coordinating internal responses to maintain IT systems' security. Regardless of the reason, unpatched assets remain exposed to known vulnerabilities, which threat actors can exploit or other cyber threat actors can use opportunistically.

The following attack types are generally used by cyber threat actors to jeopardize the integrity, confidentiality, or availability of an organization's computers, networks, information, or physical assets:

- **Advanced Persistent Threat (APT):** An APT is conducted by an adversary with sophisticated levels of expertise and significant resources, pursuing its objectives repeatedly over an extended period. Developing attacks on ICS takes time, knowledge, and expertise in the unique operating environments of the target facility. APTs therefore take advantage of vulnerabilities at multiple stages to gather information and develop and validate their attacks. These types of intrusions can lead to malicious actors taking full control of network infrastructure, allowing for further attacks on connected infrastructure (e.g., data theft, espionage, denial of service, or decreased functionality).
- **Distributed Denial-of-Service (DDoS):** During a DDoS attack, the adversary exploits Internet-connected devices to generate immense bandwidth loads to the point of disruption or to create openings for malware to be deployed. Common security devices that use high-bandwidth connections, such as security cameras and digital video recorders, are of particular concern for DDoS attacks because they can suddenly consume large volumes of Internet traffic and are commonly deployed in large batches.
- **Malware and Ransomware:** Malware (a term derived from "malicious software") is a mechanism by which cyberattacks are carried out. Ransomware is a type of malware that cyber threat actors use to deny access to systems or data by encrypting the files and data on the infected computer. Typically, the threat actor requests a ransom in exchange for decrypting the data and returning functionality. One of the most common mechanisms by which malware is delivered to IT systems and networks is phishing, which refers to malicious emails designed to trick the recipient into opening a malicious attachment, visiting a malicious website, or sharing sensitive information (e.g., passwords, account numbers, or personal information).

For additional information on cyber issues as they relate to the Dams Sector, refer to the *Dams Sector Landscape* and *Roadmap to Secure Control Systems in the Dams Sector*, available on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal. For additional information on resources available to owners and operators to identify, protect against, detect, respond to, and recover from cyberattacks visit the CISA Resources for Business webpage at us-cert.cisa.gov/resources/business.

2.3 Key Dams Sector Cybersecurity 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 HSIN-CI Dams Portal or by contacting the Dams Sector Management Team at DamsSector@cisa.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 Awareness Handbook*** provides an overview of cyber issues of interest to the sector, potential attack types, indicators, vulnerabilities, and potential consequences from cyberattacks.
- The ***Dams Sector Surveillance and Suspicious Activities Indicators Guide*** includes sections on cyberattack indicators, how to report an attack, and cyber defensive measures.
- The ***Dams Sector Crisis Management Handbook*** includes a section on building a cyber incident response plan.
- 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 CISA Central website at cisa.gov/uscert/ics and in the NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS)*. For additional information on cybersecurity recommended practices, visit CISA's Baseline Cybersecurity Performance Goals at cisa.gov/cpgs.

3. Core Concepts of the Maturity Model

This chapter describes several core concepts that are important for interpreting the content and structure of the model. This includes defining what a maturity model is, providing context on the function and scope of a C2M2 evaluation, referencing critical infrastructure security and resilience objectives, highlighting the value of defined maturity indicator levels (MILs) for the model, the significance of including IT and OT assets, and the relationship of the model to an overall risk management process.

3.1 Maturity Model Definition

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 accepted in a particular industry, organizations can benchmark their activities against an industry standard.

3.2 Function and Scope

In this model, the term "function" is used as a scoping mechanism; it refers to the subset of operations performed by the organization or facility to which the model is being applied.

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. The scope limits the focus of the evaluation to logical boundaries for defining what is and is not included in the evaluation of the function. Setting the evaluation scope defines the context in which to evaluate cybersecurity maturity and ensures consistency throughout the implementation process.

Take, for example, an organization that uses the model to evaluate its business IT services, including email, Internet connectivity, and Voice over Internet Protocol (VoIP) telecommunication. In the Threat and Vulnerability Management domain, practice 1b 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 business IT services. In this example, the practice means cybersecurity vulnerability information is gathered and interpreted for the business IT services—information about vulnerabilities that would affect the business email services, network devices, and the VoIP system. In this example, the evaluation scope is limited to business operations.

3.3 Critical Functions

The roles and functions that cyber systems serve can affect the reliable operation of critical processes. 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 assets, consider the following types of critical processes:

- 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 processes or local recovery plans.

In addition to identifying critical processes, 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 processes. 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.

3.3 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.

3.4 Maturity Indicator Level Concept and Value

To measure progression, maturity models typically have "levels" along a scale. The Dams-C2M2 uses a scale of maturity indicator levels (MILs) 0-3, which are described in Section 4.2 along with a set of attributes defining each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities the level represents. Assigning states of transition 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.

3.5 Information Technology and Operations Technology Assets

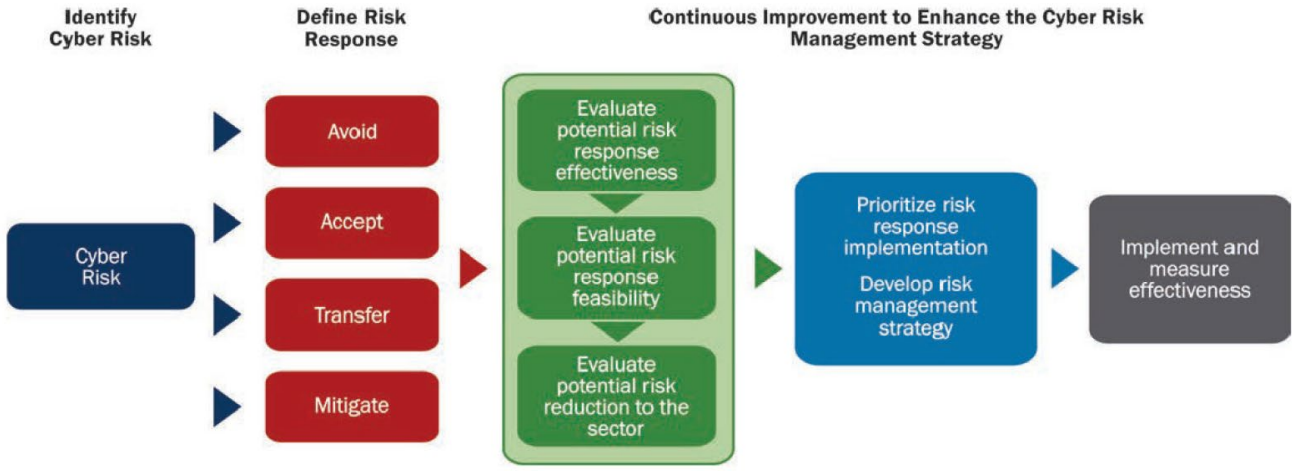
Many Dams-C2M2 practices refer to assets. When evaluating how completely a practice is performed, be sure to consider both traditional and emerging enterprise IT assets and all OT assets—including ICS, process control systems, supervisory control and data acquisition (SCADA) systems, and other OT.

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.

3.6 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 6.3) 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. Supporting cybersecurity risk management alignment with enterprise risk management, it is important to document the results (and reference justification) of the C2M2 evaluation for defensibility and implementation of improvements (see Chapter 5 for a summary on how to use the model).

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 4.6.

4. 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 maturity indicator level (MIL).

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

4.1 Domains

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

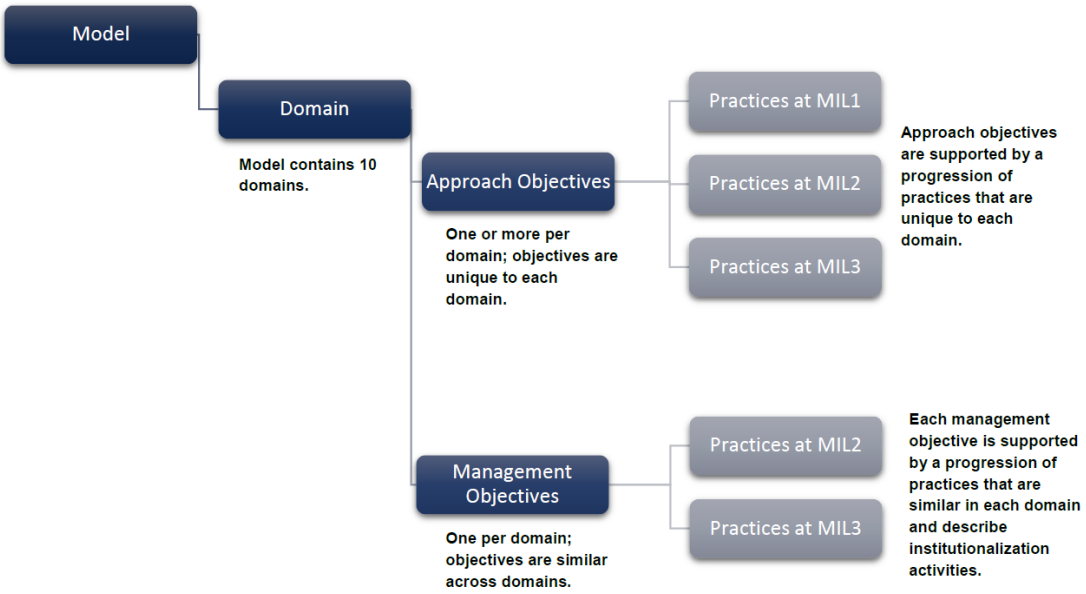
For each domain, the model provides a purpose statement, which is a high-level summary of the domain's intent, followed by introductory notes, which give context for the domain and introduce its practices. The purpose statement and introductory notes offer context for interpreting the practices in the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

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

- Establish Cybersecurity Risk Management Strategy and Program
- 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.

Asset Identification, Change, and Configuration Management

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

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.

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.

Situational Awareness

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

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

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

Third-Party Risk 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 Architecture

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

Cybersecurity Program Management

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.

4.2 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. Organizations should evaluate the costs of achieving a specific MIL against potential benefits. However, the model was developed so that all organizations, regardless of size, should be able to achieve MIL1 across all domains.

4.3 Approach Progression of Maturity Indicator Levels

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, including policies and standards. e) The cybersecurity program strategy defines the structure and organization of the cybersecurity program. f) The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program. g) The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program. h) The cybersecurity program strategy is approved by senior management.
MIL3	i) The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile.

4.4 Institutionalization Progression of Practices

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 domain-specific practices to the management practices in the second objective of the Risk Management domain.

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

Maturity Indicator Level	Domain-Specific Practices	Management 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.	a) This objective contains no practices for MIL1.
MIL2	c) Risk assessments are performed to identify risks in accordance with the cybersecurity 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 cybersecurity risk management strategy. g) Risk analysis is informed by network (IT and/or OT) architecture. h) Stakeholders from appropriate operations and business areas participate in the identification, analysis, and mitigation of cyber risks	b) Documented procedures are established, followed, and maintained for RM activities. c) Adequate resources (e.g., people, funding, and tools) are provided to support RM activities.
MIL3	i) The risk management program defines and operates risk management policies and procedures that implement the risk-management strategy. j) A current cybersecurity architecture is used to inform risk analysis. k) Cybersecurity risk identification considers risks that may arise from or affect critical infrastructure or other interconnected organizations. l) Information from other domain activities is used to update cybersecurity risks and identify new risks m) A risk register (a structured repository of identified risks) is used to support risk-management activities. n) Cybersecurity risks and risk categories are retired when they no longer require tracking or response	d) Up-to-date policies or other organizational directives define requirements for IAM activities. e) Personnel performing IAM activities have the skills and knowledge needed to perform their assigned responsibilities. f) Responsibility, accountability, and authority for the performance of IAM activities are assigned to personnel. g) The effectiveness of IAM activities is evaluated and tracked.

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

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:

- **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)

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

- **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.
- **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.
- **Adequate resources are provided to support the process.** 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.
- **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.

Maturity Indicator Level 3 (MIL3)

At MIL3, the activities in a domain have been further institutionalized and are now being managed. The practices in a domain are further stabilized at MIL3 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. Five management practices support this progression:

- **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.
- **Policies include compliance requirements for specified standards and/or guidelines.**
- **Activities are periodically reviewed to ensure they conform to policy.**
- **Responsibility and authority for performing the practices are assigned to personnel.**
- **Personnel performing the practices have adequate skills and knowledge.** The personnel assigned to perform the activities have adequate domain-specific skills and knowledge to perform their assignments.

4.5 Summary of Maturity Indicator Level 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	*Approach characteristic:* • Practices are more complete or advanced than at MIL1. *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.
MIL3	*Approach characteristic:* • Practices are more complete or advanced than at MIL2. *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.

4.6 Reference Notation for Practices

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, "The organization has a strategy for cybersecurity risk management, which may be developed and managed in an ad hoc manner," would be referenced elsewhere in the model using the notation "RM-1a."

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

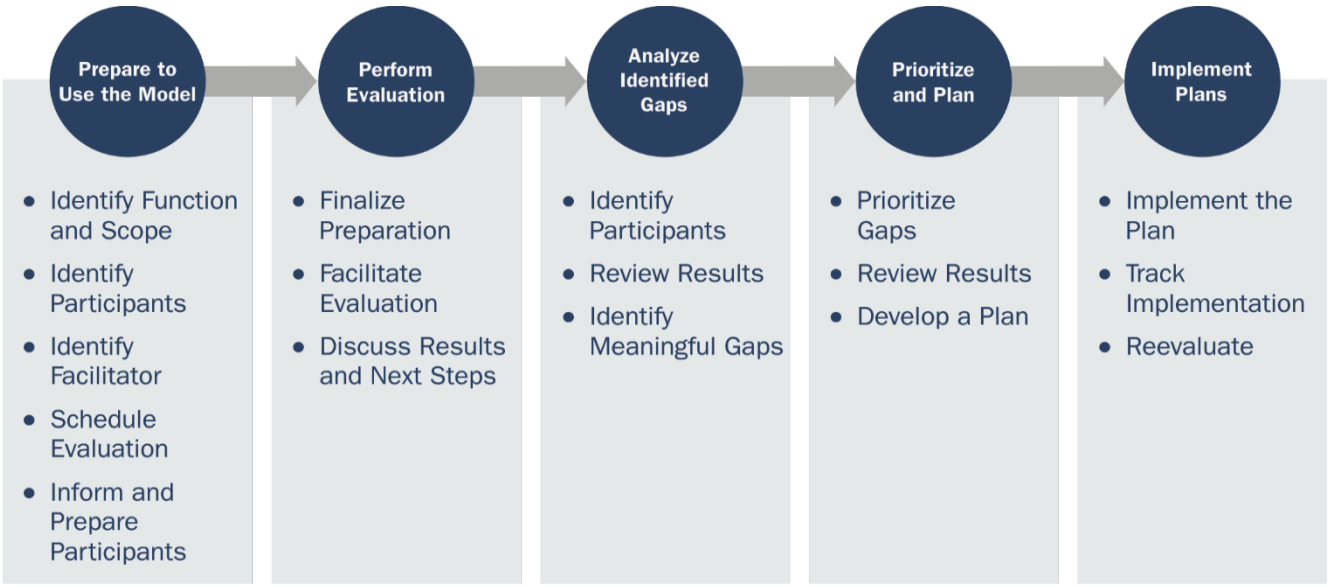
1. Establish Cybersecurity Risk Management Strategy and Program	
MIL1	a) The organization has a strategy for cybersecurity risk management, which may be developed and managed in an ad hoc manner.
MIL2	b) There is a documented cybersecurity risk management strategy. c) The cybersecurity risk management strategy is maintained to support the organization's cybersecurity program strategy (CPM-1b) and enterprise architecture d) The strategy provides an approach for risk prioritization, including consideration of effect. e) Information from RM activities is communicated to relevant stakeholders. f) Governance for the cyber risk management program is established and maintained
MIL3	g) There is a documented cybersecurity risk management strategy. h) The cybersecurity risk management strategy is maintained to support the organization's cybersecurity program strategy and enterprise architecture i) The strategy provides an approach for risk prioritization, including consideration of effect. j) Information from RM activities is communicated to relevant stakeholders. k) Governance for the cyber risk management program is established and maintained

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

5. 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* provides additional details, suggested approaches, and templates to complete each of these steps.

FIGURE 3.—Recommended Process for Implementing the Dams-C2M2



5.1 Prepare to Use the Model

A design goal of the model was to enable organizations to complete a self-evaluation for a single function in less than one day 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.

Identify Function and Scope: Selecting the function—the subset of operations performed by the organization to which the C2M2 is being applied—is a key early step in implementing the model. The function is an important process, system, or operation the organization intends to evaluate for cybersecurity maturity. The scope limits the focus of the evaluation to logical boundaries for defining what is and is not included in the evaluation of the function.

Example: Identify Function and Scope

Anywhere USA Hydro has decided to conduct a C2M2 evaluation for a portion of its operations. To limit the focus to a specific operational area, they will apply the C2M2 to evaluate their control center operations (i.e., ***function***) at the Alpha Dam (i.e., ***scope***).

Setting the evaluation scope is essential for an organization to effectively use the C2M2 because the scope defines the context in which to evaluate cybersecurity maturity and ensures consistency throughout the implementation process.

Identify Personnel: Selecting the appropriate personnel to participate in the evaluation is another important early C2M2 implementation step. Broad representation across the parts of the organization involved in the function to be evaluated yields the best results and enables internal information sharing about the cybersecurity practices. Participants may include operational personnel, management stakeholders, and any others who could provide useful information about the organization's performance of cybersecurity practices.

Identify Facilitator: Though the C2M2 is intended to guide an organization in a self-evaluation of its cybersecurity maturity, a facilitator can be useful in guiding the participants through the implementation of the model. The facilitator must have the knowledge and skill to be able to intervene in discussions as needed in a way that adds to the group's creativity rather than lessening it. The major delineation between approaches to identifying a C2M2 facilitator is the selection of a professional within or outside the organization.

Schedule the Evaluation: Scheduling the evaluation includes selecting when to run the evaluation and for what duration. The evaluation may take place prior to an upcoming budget cycle (i.e., to identify and justify needed investments); prior to implementing technology or policy changes; in preparation for a site visit, assessment, or inspection by a federal, state, or local agency; or to coincide with another event (e.g., training). While the evaluation was designed to be completed in an average of two days, the actual duration depends on a number of factors, including the number of participants and their knowledge of the C2M2, the complexity of the function being evaluated, the facilitator's effectiveness, and whether homework was assigned and completed.

Inform and Prepare Participants: Prior to performing the evaluation, it is prudent that all participants become familiar with the C2M2 model and implementation process, especially if the evaluation will bring together people from different parts of the organization and with diverse roles. Planning calls and read-ahead materials (possibly including homework) are effective mechanisms to communicate with participants about the evaluation and their role, as well as answer questions about the model and/or implementation process.

5.2 Perform an Evaluation

Following the detailed planning and preparation, the sponsor, facilitator, and participants gather to conduct the evaluation in a workshop setting. The evaluation entails the participants' assessing cybersecurity maturity across ten cybersecurity domains (logical groupings of cybersecurity practices) and the discussion of results and next steps.

Finalize Preparation: Before the evaluation is conducted, the facilitator and any support staff ensure that the meeting space is adequately configured and provisioned for a productive evaluation, including preparing equipment, seating, and other logistical tools and aides.

Facilitate the Evaluation: Conducting the evaluation broadly involves opening with a welcoming statement and an overview of the C2M2 model, followed by progressing through the model to evaluate the maturity of cybersecurity practices for the function. The facilitator guides the participants through the model and discussion, and a member of the evaluation team records decisions and discussion points.

Discuss Preliminary Results and Next Steps: Following the selection of MILs across the ten domains and their recording in appropriate documentation (e.g., worksheets, spreadsheets, reports) the participants discuss the results of that effort and next steps leading from the evaluation. The facilitator summarizes the

selected MILs, successes, and gaps and leads a discussion to confirm the organization's cybersecurity maturity profiles. Participants review the current profile (i.e., actual MILs) and the capability profile (i.e., target MILs) and prepare for the examination of those profiles to identify, analyze, prioritize, and mitigate gaps.

5.3 Analyze Identified Gaps

The completion of the C2M2 evaluation and the establishment of maturity profiles (current and capability) allow the organization to analyze its 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 provide the basis for determining which are meaningful and, of those, which should be prioritized.

Identify Participants: After the participants have completed the C2M2 evaluation, a separate group of personnel (referred to as the post-evaluation group) coordinates the results of the evaluation and collaborates on identifying gaps between the organization's current and capability profiles. This group is generally smaller than the group of evaluation participants and includes key decision-makers relating to the objectives and practices of the function that was evaluated.

Review Results: Once the post-evaluation group has been selected to continue through the steps of the model, the evaluation results review can take place. The group might prefer to convene in a workshop setting immediately following the evaluation or may wish to conduct this step over time through multiple meetings. Reviewing the documents used to record results from the evaluation will allow the post-evaluation group to become familiar with the decisions and supporting discussion from the evaluation.

Identify Meaningful Gaps: The current and capability profiles provide the fundamental basis for the identification and analysis of gaps. Specifically, the gaps exist where the actual MIL falls short of the target MIL. Selecting meaningful gaps from the full list of gaps is a practical step in narrowing the organization's focus on those gaps to prioritize for mitigation. An organization may focus on gaps with high-level, strategic relevance, or focus on more technical issues relating to the objectives and practices of the gaps. Regardless of the analysis method, the resulting list of meaningful gaps is documented in a Gap Mitigation Plan for use in progressing through the next steps in the C2M2.

5.4 Prioritize and Plan

Organizations prioritize the gaps between their current and capability profiles in order to plan targeted mitigation actions to address those gaps. Limited time and resources require intelligent choices about which actions to pursue first to ensure deployment of a mature, robust cybersecurity management strategy. Prioritization that aligns with business objectives and understanding of risk informs the choices about actions. Planning actions improves the likelihood of effective implementation of new practices. Documentation, rationale, and ownership of projects can help build consensus and support for closing priority gaps.

Prioritize Gaps: Identifying the meaningful gaps isolates significant issues an organization faces. Prioritizing these gaps helps an organization to make informed decisions about where and when to apply limited resources to mature cybersecurity capabilities. Organizations may choose to apply existing internal strategic planning processes to prioritize gaps, or they can select different prioritization criteria, such as level of importance, timeframe, cost-benefit analysis, or a combination of these criteria.

Review Results: Reviewing the prioritization results in a Gap Mitigation Plan allows the organization to organize, sort, select, or highlight specific gaps or groups of gaps that are higher or lower in priority. This step may include sorting or rearranging the list of gaps into ordered categories. The ultimate aim is to select those for further development in the C2M2. At this point in the prioritization process, it may be

useful for the organization to also review the list or groupings of gaps and priority categories to ensure that the results are congruent with the organization's expectations for the C2M2.

Develop a Plan: The development of a Gap Mitigation Plan can be useful for articulating and addressing the prioritized gaps and, ultimately, for managing the maturation of the organization's cybersecurity capabilities. The organization may choose to incorporate the process of developing a Gap Mitigation Plan into its established strategic planning process. The primary components to consider include brainstorming and confirming mitigation actions that would address the selected gaps, determining key information needed to implement the actions (e.g., milestones, staff assignments, and resources), and designating an owner of the plan to track progress.

5.5 Implement Plans

Organizations can implement the Gap Mitigation Plan developed to address the gaps identified and planned for in previous steps of the C2M2. Plan implementation improves the organization's cybersecurity capabilities and helps drive the evaluated function toward achieving the capability profile (i.e., target MILs). Tracking implementation of the Gap Mitigation Plan is an important step to ensure that the desired outcomes can be met on time and on budget. Periodic reevaluation is useful in allocating limited remaining resources and reviewing overall progress to keep the organization focused and on track.

Implement the Plan: The implementation of the Gap Mitigation Plan may proceed through an established strategic planning process. Key factors to consider when implementing the plan include allocating adequate and appropriate resources, communicating the desired milestones and outcomes to assigned staff, and managing the implementation process (e.g., setting schedules, establishing reporting formats, and communicating with both implementing staff and interested supervisory roles such as senior management or the board of directors).

Track Implementation: Tracking implementation of mitigation actions helps to ensure that progress is made towards the desired capability profile and allows an organization to course-correct before major issues arise. Well-defined milestones can be helpful in checking that implementation of mitigation actions remains on schedule and on budget. Frequent communication with implementing staff to gather status reports or review actions undertaken and regular reporting to senior management on overall progress may also be helpful in identifying and addressing barriers.

Reevaluate: Defining and conducting routine reviews to reevaluate gap mitigation implementation status is a common project management practice for maintaining effectiveness of the mitigation actions and helping to keep the organization's efforts on track, on schedule, and on budget. The reevaluation of the Gap Mitigation Plan or the current and capability profiles allows the organization to adjust its gap mitigation priorities, resource allocations, and metrics to align with current conditions. Accordingly, reevaluations should also be considered in response to major changes in the business or risk environments to continue on the path of matching the organization's current profile to its desired state of cybersecurity maturity.

6. Model Domains

6.1 Asset Identification, Change, and Configuration Management

Purpose: Manage the organization's OT and IT 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 IT and OT Asset Inventory
2. Manage IT and OT Asset Configuration
3. Manage Changes to IT and OT Assets
4. Management Activities

Owners and operators review their organization's assets to identify and inventory assets that are important to the delivery of the function. 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 assets and ensuring that assets are configured according to the baseline. Most commonly, this practice applies to ensuring that similar assets are configured in the same way. However, in cases where assets are either unique or must have individual configurations, managing asset configuration involves controlling the configuration baseline of the asset when it is deployed for operation and ensuring that the asset remains configured according to the baseline.

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

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.

Objectives and Practices	
1. Manage IT and OT Asset Inventory	
MIL1	a) There is an inventory of IT and OT assets[1] that are important to the delivery of the function; management of the inventory may be ad hoc. b) The inventory includes information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data).
MIL2	c) Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, operating system and firmware versions, criticality of the asset,[2] service dependencies, service level agreements, and conformance of assets to relevant industry standards). d) The information asset inventory includes attributes that support cybersecurity activities (e.g., backup locations and frequencies, storage locations, cybersecurity requirements). e) Inventoried IT and OT assets are prioritized based on their importance to the delivery of the function.
MIL3	f) There is an inventory for all connected[3] IT and OT assets related to the delivery of the function. g) The asset inventory is current, as defined by the organization. h) The asset inventory is used to identify cyber risks, such as asset end of life or end of support and single points of failure. i) Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life.
2. Manage IT and OT 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.
MIL2	c) The design of configuration baselines includes cybersecurity objectives. d) Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARC-1e).
MIL3	e) Configuration of assets is monitored for consistency with baselines throughout the assets' life cycle. f) Configuration baselines are reviewed and updated at an organization-defined frequency, such as system changes and changes to the cybersecurity architecture.

[1] 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 processes of OT assets.

[2] 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.

[3] 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 processes.

Objectives and Practices	
3. Manage Changes to IT and OT Assets	
MIL1	a) Changes to inventoried assets are evaluated and approved before being implemented. b) Changes to inventoried assets are logged.
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).
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 (e.g., availability, integrity, confidentiality).
4. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for ACM activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support ACM activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for ACM activities. d) Personnel performing ACM activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of ACM activities are assigned to personnel. f) The effectiveness of ACM activities is evaluated and tracked.

6.2 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 impact organizational operations (e.g., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Threats to IT, OT, and communication infrastructure assets vary and may include advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, malware, and ransomware.

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

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 considers the vulnerability's local impact (i.e., 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, replacing outdated equipment, or through other risk management activities (e.g., those found in the Risk Management and Cybersecurity Program Management domains).

Responding to threats and sharing threat information 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 the function. A threat profile for the function includes the characterization of likely intent, capability, and target of threats to the function. The function's threat profile can be used to guide the identification of specific threats, the risk analysis process described in the Risk Management domain, and the building of the operational and cyber status described in the Situational Awareness domain.

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 cyberattack 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 trusted sources (e.g., Information Sharing and Analysis Centers [ISACs], CISA's Known Exploited Vulnerabilities Catalog, CISA's alerts and advisories websites) 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. Anywhere USA Hydro also uses the MITRE ATT&CK framework to inform the CVSS score by relating potential cyber threat actor TTPs to vulnerabilities.

Objectives and Practices	
1. Reduce Cybersecurity Vulnerabilities	
MIL1	a) Information sources to support cybersecurity vulnerability discovery are identified (e.g., ISACs, CISA's Known Exploited Vulnerabilities Catalog, CISA's alerts and advisories websites, InfraGard, industry associations, vendors, federal briefings, internal assessments). b) Cybersecurity vulnerability information is gathered and interpreted for the function. c) Cybersecurity vulnerability assessments are performed. d) Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches).
MIL2	e) Cybersecurity vulnerability information sources that address all assets important to the function are monitored (ACM-1f). f) Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools). g) 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). h) Cybersecurity vulnerabilities are addressed according to the assigned priority. i) Operational impact to the function is evaluated prior to deploying patches. j) Information on any discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders.
MIL3	k) Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency. l) Cybersecurity vulnerability assessments are informed by the organization's risk criteria (RM-1g). m) Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function. n) Identified vulnerabilities that pose ongoing risk to the function are referred to the risk management program (RM-2) for response. o) Vulnerability monitoring activities include review and confirmation of actions taken in response to cybersecurity vulnerabilities where appropriate.

Objectives and Practices	
2. Respond to Threats and Share Threat Information	
MIL1	a) Information sources to support threat management activities are identified (e.g., ISACs, CISA's Known Exploited Vulnerabilities Catalog, CISA's alerts and advisories websites, InfraGard, industry associations, vendors, federal briefings, internal assessments). 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).
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) Threat information is exchanged with stakeholders (e.g., government, connected organizations, vendors, sector organizations, regulators, ISACs, internal entities) based on risk to critical infrastructure. h) Threats are addressed according to the assigned priority.
MIL3	i) The threat profile for the function is validated at an organization-defined frequency. j) Analysis and prioritization of threats are informed by the organization's risk criteria (RM-1g). k) Threat monitoring and response activities leverage and trigger predefined states of operation (SA-3g). l) Threat information is added to the risk register (RM-2m). m) Threats that pose ongoing risk to the function are referred to the risk management program for action (RM-2).
3. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for TVM activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support TVM activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for TVM activities. d) Personnel performing TVM activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of TVM activities are assigned to personnel. f) The effectiveness of TVM activities is evaluated and tracked.

6.3 Risk Management

Purpose: Establish, operate, and maintain a 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 relates to the loss of confidentiality, integrity, or availability of information, data, or information or control systems and reflects the potential adverse impacts to organizational operations (e.g., mission, functions, image, and reputation) and assets, individuals, other organizations, and the nation. 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 and Program
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 organization's 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 aligns with existing enterprise risk management concepts and documentation (e.g., strategy, program, activities) 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 (i.e., accepting, avoiding, mitigating, transferring), communicating, 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 (e.g., Situational Awareness, Event and Incident Response, Continuity of Operations, and Cybersecurity Architecture) refer to the risk register and illustrate how the practices in the model are strengthened as they connect through a cybersecurity risk

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 such as 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, such as 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. Because its network diagram includes elements such as 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.

management program. Information generated through activities in the Threat and Vulnerability Management and Third-Party Risk Management domains is used to update cyber risks and identify new risks.

Objectives and Practices	
1. Establish Cybersecurity Risk Management Strategy and Program	
MIL1	a) The organization has a strategy for cybersecurity risk management, which may be developed and managed in an ad hoc manner.
MIL2	b) There is a documented cybersecurity risk management strategy. c) The cybersecurity risk management strategy is maintained to support the cybersecurity program strategy (CPM-1b) and enterprise architecture. d) The strategy provides an approach for risk prioritization, including consideration of effect. e) Information from RM activities is communicated to relevant stakeholders. f) Governance for the cybersecurity risk management program is established and maintained.
MIL3	g) Organizational cybersecurity risk criteria (i.e., 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. h) The cybersecurity risk management strategy is periodically updated to reflect the current threat environment. i) An organization-specific risk taxonomy is documented and is used in risk management activities. j) A cybersecurity risk management program is established and maintained to implement and perform risk management activities in alignment with the organization's mission and objectives. k) The cybersecurity risk management strategy and program activities are coordinated with the organization's enterprise-wide risk management strategy and program.

Objectives and Practices	
2. Manage Cybersecurity Risk	
MIL1	a) Cybersecurity risks are identified. b) Identified risks are mitigated, accepted, tolerated, or transferred.
MIL2	c) Risk assessments are performed to identify risks in accordance with the cybersecurity risk management strategy. d) Identified risks are documented. e) Identified risks are analyzed to prioritize response activities in accordance with the cybersecurity risk management strategy. f) Identified risks are monitored in accordance with the cybersecurity risk management strategy. g) Risk analysis is informed by network (e.g., IT and/or OT) architecture. h) Stakeholders from appropriate operations and business areas participate in the identification, analysis, and mitigation of cyber risks.
MIL3	i) The risk management program defines and operates risk management policies and procedures that implement the cybersecurity risk management strategy. j) A current cybersecurity architecture is used to inform risk analysis. k) Cybersecurity risk identification considers risks that may arise from or affect critical infrastructure or other interconnected organizations. l) Information from ACM, TVM, TPM, and ARC activities is used to update cybersecurity risks and identify new risks. m) A risk register (i.e., a structured repository of identified risks) is used to support RM activities. n) Cybersecurity risks and risk categories are retired when they no longer require tracking or response.
3. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for RM activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support RM activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for RM activities. d) Personnel performing RM activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of RM activities are assigned to personnel. f) The effectiveness of RM activities is evaluated and tracked.

6.4 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 (i.e., 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 (i.e., removing available identities when they are no longer required) of identities to entities. Entities may include individuals internal or external to the organization as well as devices, systems, or processes that require access to assets. In some cases, organizations may need to use shared identities. Management of shared identities may require compensatory measures to ensure an appropriate level of security. Maintenance of identities includes traceability, (i.e., 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, their 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.

Objectives and Practices	
1. Establish and Maintain Identities	
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.
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 organization-defined time thresholds when no longer required. g) Stronger or multifactor credentials are required for access that poses higher risk to the function (e.g., privileged accounts, service accounts, shared accounts, and remote access).
MIL3	h) Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1g).
2. Control Access	
MIL1	a) Access requirements, including those for remote access, are determined. b) 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. c) Access is granted to identities based on requirements. d) Access is revoked when no longer required.
MIL2	e) Access requirements incorporate least privilege and separation of duties principles. f) Access requests are reviewed and approved by the asset owner. g) Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring.
MIL3	h) Access privileges are reviewed and updated to ensure validity, at an organization-defined frequency. i) Access to assets is granted by the asset owner based on risk to the function. j) Anomalous access attempts are monitored as indicators of cybersecurity events.
3. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for IAM activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support IAM activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for IAM activities. d) Personnel performing IAM activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of IAM activities are assigned to personnel. f) The effectiveness of IAM activities is evaluated and tracked.

6.5 Situational Awareness

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

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 common operating picture (COP) for the function, it can align predefined cybersecurity states of operation (e.g., normal, alert, and hazard) to changes in the operating environment. The ability to shift from one predefined state to another can enable faster and more effective response to cybersecurity events or changes in the threat environment.

The Situational Awareness (SA) domain has four objectives:

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

Logging is 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.

Monitoring data collected in logs and through other means enables the organization to analyze and understand the function's cybersecurity state. Effectively communicating the cybersecurity state 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 (e.g., organizational e-mail or messaging, internal websites or applications) 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. In addition, the personnel monitor a number of resources that provide reliable cybersecurity information, including their vendors, E-ISAC, and CISA's alerts and advisories.

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.

Objectives and Practices	
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) IT and OT environments are monitored for anomalous behavior that may indicate a cybersecurity event.
MIL2	c) Monitoring 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 (EIR-1d). e) Indicators of anomalous activity have been defined and are monitored across the IT and OT environments. f) Monitoring activities are aligned with the function's threat profile (TVM-2d).
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 IT and OT environments to identify anomalous activity. j) Risk register (RM-2m) content is used to identify indicators of anomalous activity. k) Alarms and alerts are evaluated and updated periodically, at an organization-defined frequency.

3. Establish and Maintain a Common Operating Picture	
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 cybersecurity state of the function (e.g., a COP, which may or may not include visualization or be presented graphically). c) Information from across the organization is available to enhance the COP.
MIL3	d) Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders. e) Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the COP. f) Relevant information from outside the organization is collected to enhance the COP. g) Predefined states of operation are defined and invoked (e.g., with manual or automated process) based on the COP.
4. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for SA activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support SA activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for SA activities. d) Personnel performing SA activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of SA activities are assigned to personnel. f) The effectiveness of SA activities is evaluated and tracked.

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

Purpose: Establish and maintain plans, procedures, and technologies to detect, analyze, respond to, and recover from 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 (e.g., 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 Cybersecurity Events and Incidents
4. Plan for Continuity of Operations
5. Management Activities

Detecting cybersecurity events includes designating a forum for reporting events and establishing criteria for event prioritization. These criteria 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. Cybersecurity events may originate with or impact third parties necessitating coordination in response planning, execution, and communications.

Escalating cybersecurity events involves applying the criteria discussed in the Detect Cybersecurity Events objective 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 establish and maintain a process to limit the effects of cybersecurity events to organizational operations (e.g., mission, functions, image, or reputation) and assets. The process describes how the organization manages all phases of the event or incident life cycle (e.g., triage, handling, communication, coordination, and closure). Conducting lessons-learned reviews as a part of cybersecurity event and incident response and continuity of operations helps the organization eliminate the exploited vulnerability that led to the event or incident.

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.

Planning for continuity involves the necessary activities to sustain organizational operations 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. Ensuring that continuity plans address potential cybersecurity incidents requires consideration of known cybersecurity threats and identified categories of cybersecurity risk. Continuity plans include cybersecurity incident scenarios and are tested and adjusted to ensure they remain realistic and practicable.

Objectives and Practices	
1. Detect Cybersecurity Events	
MIL1	a) There is a point of contact (e.g., a person or role) to whom cybersecurity events are reported. b) Detected cybersecurity events are reported. c) Cybersecurity events are logged and tracked (SA-1c).
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.
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-2m) and function's threat profile (TVM-2d) to help detect known threats and monitor for identified risks. h) The COP for the function is monitored to support the identification of cybersecurity events (SA-3b).
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.
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) Escalated cybersecurity events and incidents are declared based on the appropriate criteria. g) There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure. h) Cybersecurity stakeholders (e.g., government, connected organizations, vendors, sector organizations, regulators, and internal entities) are identified and notified of escalated events and incidents based on situational awareness reporting requirements (SA-3d).
MIL3	i) Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization's risk register (RM-2m) and function's threat profile (TVM-2d). j) Escalated cybersecurity events and declared cybersecurity incidents inform the COP (SA-3b) for the function. k) Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features.

Objectives and Practices	
3. Respond to Cybersecurity Events and Incidents	
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, ISACs, FBI's CyWatch, CISA Incident Reporting).
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.
MIL3	h) Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken. i) Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., tabletop, 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, as appropriate (e.g., vendors, law enforcement, and other government or external entities). l) Cybersecurity event and incident response plans are aligned with the organization's risk criteria (RM-1g) and function's threat profile (TVM-2d). 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.

Objectives and Practices	
4. Plan for Continuity of Operations	
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) Data backups are available and tested. d) IT and OT assets requiring spares are identified. e) Continuity plans are developed to sustain and restore operation of the function.
MIL2	f) Business impact analyses inform the development of continuity plans. g) Data backups are logically or physically separated from source data. h) Spares for selected IT and OT assets are available. i) Recovery time objectives (RTO) and recovery point objectives (RPO) for the function are incorporated into continuity plans. j) Continuity plans address IT, OT, and communication infrastructure assets important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets. k) Continuity plans are evaluated and exercised. l) Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel.
MIL3	m) Business impact analyses are periodically reviewed and updated. n) RTO and RPO are aligned with the organization's risk criteria (RM-1g). o) The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly. p) Continuity plans are periodically reviewed and updated. q) Restored assets are configured appropriately and inventory information is updated following execution of continuity plans.
5. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for EIR activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support EIR activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for EIR activities. d) Personnel performing EIR activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of EIR activities are assigned to personnel. f) The effectiveness of EIR activities is evaluated and tracked.

6.7 Third-Party Risk 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 dependencies among infrastructure and third parties (e.g., 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.

Third-party risk management typically focuses on supplier and customer dependencies and associated relationships with such third parties. 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. Organization's requests for proposal often provide suppliers of high-technology systems, devices, and services only rough specifications, which may lack adequate requirements for security and quality assurance. The autonomy organizations often provide to their individual business units further increases the risk, unless procurement activities are constrained by plan or policy to include cybersecurity requirements.

The Third-Party Risk Management (TPM) domain has three objectives:

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

Example: Third-Party Risk 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. In addition, Anywhere USA Hydro conducted a review of the vendor's practices (e.g., 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 (i.e., to help detect counterfeits), verifying digital signatures for associated software and firmware, and checking initial configuration settings for conformance.

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

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 are reviewed and approved for cybersecurity risk mitigation, such as contract language that establishes vendor responsibilities for meeting or exceeding specified cybersecurity standards or guidelines. Service level agreements can specify monitoring and audit processes to verify that vendors and service providers meet cybersecurity and other performance measures.

Objectives and Practices	
1. Identify and Prioritize 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). c) Other third parties that have access to, control of, or custody of any IT, OT, or communication infrastructure assets important to the delivery of the function are identified.
MIL2	d) Supplier dependencies are identified according to established criteria. e) Customer dependencies are identified according to established criteria. f) Single-source and other essential dependencies are identified. g) Dependencies are prioritized according to established criteria (e.g., importance to the delivery of the function, effect of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts).
MIL3	h) Dependency identification and prioritization are based on the organization's risk criteria (RM-1g). i) Prioritization of dependencies is periodically reviewed and updated.
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.

Objectives and Practices	
MIL2	c) Identified cybersecurity dependency risks are entered into the risk register (RM-2m). 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 cybersecurity requirements.
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-1g). 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).
3. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for TPM activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support TPM activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for TPM activities. d) Personnel performing TPM activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of TPM activities are assigned to personnel. f) The effectiveness of TPM activities is evaluated and tracked.

6.8 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 organizations increasingly adopt advanced digital technology, it may be challenging to enhance the skill sets of their existing workforce and to hire personnel with the appropriate level of cybersecurity experience, education, and training. The Dams Sector's 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. Develop Cybersecurity Workforce
3. Implement Workforce Controls
4. Increase Cybersecurity Awareness
5. Management Activities

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

Developing a cybersecurity workforce includes training and recruiting to address identified skill gaps. For example, hiring practices ensure that recruiters and interviewers are aware of cybersecurity workforce needs. Also, security awareness training for newly recruited personnel and contractors can reduce their vulnerability to social engineering and other threats.

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.

Implementing workforce controls 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.

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 an organization'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 shares 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 be less likely to adhere to security processes and procedures.

Objectives and Practices	
1. Assign Cybersecurity Responsibilities	
MIL1	a) Cybersecurity responsibilities for the function are identified. b) Cybersecurity responsibilities are assigned to specific people.
MIL2	c) Cybersecurity responsibilities are assigned to specific roles, including external service providers. d) Cybersecurity responsibilities are documented (e.g., in position descriptions).
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.
2. Develop Cybersecurity Workforce	
MIL1	a) Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities. b) Cybersecurity knowledge, skill, and ability gaps are identified.
MIL2	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).
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.

Objectives and Practices	
3. Implement Workforce Controls	
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.
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. e) Personnel are informed of their responsibilities for protection and acceptable use of IT, OT, and communication infrastructure assets.
MIL3	f) Risk designations are assigned to all positions that have access to the assets required for delivery of the function. g) Vetting is performed for all positions (e.g., employees, vendors, and contractors) at a level commensurate with position risk designation. h) Succession planning is performed for personnel based on risk designation. i) A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures.
4. Increase Cybersecurity Awareness	
MIL1	a) Cybersecurity awareness activities are conducted.
MIL2	b) Objectives for cybersecurity awareness activities are established and maintained. c) Cybersecurity awareness content is based on the function's threat profile (TVM-2d).
MIL3	d) Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3g). e) The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate.
5. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for WM activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support WM activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for WM activities. d) Personnel performing WM activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of WM activities are assigned to personnel. f) The effectiveness of WM activities is evaluated and tracked.

6.9 Cybersecurity Architecture

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

A cybersecurity architecture helps an organization plan for how security is to be engineered in a way that transcends point solutions for individual assets such as identity management or access control. It enables reasoning about the security of critical applications and data in terms of known architectural controls to, for example, detect, resist, react to, and recover from attacks. The cybersecurity architecture serves as a reference to guide how cybersecurity is to be implemented to meet the objectives of the cybersecurity program strategy.

The Cybersecurity Architecture (ARC) domain has six objectives:

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

Establishing a cybersecurity architecture involves identifying cybersecurity requirements for the organization's assets and designing appropriate controls to protect them. This includes developing a strategy for the cybersecurity architecture and a program to implement the strategy. The cybersecurity architecture is governed such that those responsible for the cybersecurity architecture are included in planning and decision-making processes when changes to the organization, IT systems, or OT systems are being considered. In this way, changes to the organization can be reviewed to address security concerns and align with the organization's cyber risk tolerance.

Effective cybersecurity architecture includes multiple elements required for its implementation. For example, network protections include segmentation, choice of hosting solutions, cryptographic controls, and audit trails, which can be combined with availability controls such as monitoring, rollback, and

Example: Cybersecurity Architecture

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

The cybersecurity architecture permits reasoning about the capabilities of prospective vendor solutions in the context of Anywhere USA Hydro's cybersecurity program. It provides a comprehensive picture of how system components and their interactions will handle responsibilities such as application and data security. It facilitates the creation of integrated end-to-end scenarios by which the quality of a proposed vendor solution may be evaluated.

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

redundancy. OT and IT asset security includes cybersecurity controls with increased rigor for high-priority assets, enforcing the principles of least privilege and least functionality (i.e., to limit access, services, and infrastructure, as appropriate), and device and firmware configuration controls. 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. Data security includes protections and controls for data in transit or at rest per defined categories from the Asset Identification, Change, and Configuration Management domain, such as provisions for cryptographic data and key management, data encryption, and prevention of unauthorized software, firmware, and data changes.

Objectives and Practices	
1. Establish and Maintain Cybersecurity Architecture Strategy and Program	
MIL1	a) The organization has a strategy for cybersecurity architecture.
MIL2	b) A strategy for cybersecurity architecture is established and maintained to support the organization's cybersecurity program strategy (CPM-1b) and enterprise architecture. c) A documented cybersecurity architecture strategy includes IT and OT systems and networks and aligns with system and asset categorization and prioritization. d) Governance for cybersecurity architecture (e.g., an architecture review board) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process. e) The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets. f) Cybersecurity controls are selected and implemented to meet cybersecurity requirements.
MIL3	g) The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program. h) Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated at an organization-defined frequency. i) The cybersecurity architecture is guided by the organization's risk analysis information (RM-2e) and function's threat profile (TVM-2d). j) The cybersecurity architecture addresses predefined states of operation (SA-3g).
2. Implement Network Protections as an Element of the Cybersecurity Architecture	
MIL1	a) The organization's IT systems are separated from OT systems through segmentation, either through physical or logical means.
MIL2	b) Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements (ACM-1a, ACM-2a). c) Network protections incorporate the principles of least privilege and least functionality. d) Network protections are defined and enforced for selected asset types according to asset risk and priority (e.g., internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices). e) Network protections include monitoring, analysis, and control of network traffic for selected security zones (e.g., firewalls, whitelisting, intrusion detection and prevention systems). f) Web traffic and email are monitored, analyzed, and controlled (e.g., malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking).

Objectives and Practices	
MIL3	g) All assets are segmented into distinct security zones based on cybersecurity requirements. h) Isolated networks are implemented such that assets are logically or physically segmented into security zones with independent authentication, as appropriate. i) OT systems are operationally independent from IT systems so that OT operations are unimpeded by an outage of IT systems. j) Network connections are protected commensurate with risk to the organization (e.g., secure connections for remote administration). k) Device connections to the network are controlled to ensure that only authorized devices can connect (e.g., network access control [NAC]). l) The cybersecurity architecture enables the isolation of compromised assets.
3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture	
MIL1	a) Cybersecurity controls are implemented for assets important to the delivery of the function.
MIL2	b) More rigorous cybersecurity controls are implemented for higher priority assets (ACM-1e). c) The principle of least privilege (e.g., limiting administrative access for users and service accounts) is enforced. d) The principle of least functionality (e.g., limiting services, limiting applications, limiting ports, limiting connected devices) is enforced. e) Secure configurations are implemented as part of the asset deployment process where feasible. f) Security applications are required as an element of device configuration where feasible (e.g., endpoint detection and response, host-based firewalls). g) The use of removeable media is controlled (e.g., limiting the use of USB devices, managing external hard drives). h) Cybersecurity controls, including physical access controls, are implemented for all assets used for the delivery of the function (ACM-1f) either at the asset level or as compensating controls where asset-level controls are not feasible.
MIL3	i) Configuration of and changes to firmware are controlled throughout the asset life cycle. j) Controls are implemented to prevent the execution of unauthorized code.
4. Implement Software Security as an Element of the Cybersecurity Architecture	
MIL1	No practice at MIL1.
MIL2	a) Software developed in-house for deployment on higher priority assets (ACM-1e) is developed using secure software development practices. b) The selection of procured software for deployment on higher priority assets (ACM-1e) includes consideration of the vendor's secure software development practices. c) Secure software configurations are required as part of the software deployment process.

Objectives and Practices	
MIL3	d) All software developed in-house is developed using secure software development practices. e) The selection of all procured software includes consideration of the vendor's secure software development practices. f) The architecture review process evaluates the security of new and revised applications prior to deployment. g) The authenticity of all software and firmware is validated prior to deployment. h) Security testing (e.g., static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications at an organization-defined frequency.
5. Implement Data Security as an Element of the Cybersecurity Architecture	
MIL1	a) Sensitive data is protected at rest.
MIL2	b) All data at rest is protected for selected data categories (ACM-1d). c) All data in transit is protected for selected data categories (ACM-1d). d) Cryptographic controls are implemented for data at rest and data in transit for selected data categories (ACM-1d). e) Key management infrastructure (i.e., key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls. f) Controls to restrict the exfiltration of data (e.g., data loss prevention tools) are implemented.
MIL3	g) The cybersecurity architecture includes protections (e.g., full disk encryption) for data that is stored on assets that may be lost or stolen. h) The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data.
6. Management Activities	
MIL1	No practice at MIL1.
MIL2	a) Documented procedures are established, followed, and maintained for ARC activities. b) Adequate resources (e.g., people, funding, and tools) are provided to support ARC activities.
MIL3	c) Up-to-date policies or other organizational directives define requirements for ARC activities. d) Personnel performing ARC activities have the skills and knowledge needed to perform their assigned responsibilities. e) Responsibility, accountability, and authority for the performance of ARC activities are assigned to personnel. f) The effectiveness of ARC activities is evaluated and tracked.

6.10 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 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 three objectives:

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

The cybersecurity program strategy is established as the foundation for the program. In its simplest form, the program strategy includes 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 complex 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 (e.g., 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.

Objectives and Practices	
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 identifies standards and guidelines intended to be followed by the program. g) The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (e.g., NERC CIP, NIST guidelines, ISO, CMMC Framework). h) The cybersecurity program strategy is approved by senior management.
MIL3	i) The cybersecurity program strategy—including policies and standards—is updated to reflect business changes, changes in the operating environment and changes in the function's threat profile (TVM-2d).
2. Sponsor Cybersecurity Program	
MIL1	a) Resources (e.g., 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 (e.g., 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. i) Stakeholders for cybersecurity program management activities are identified and involved.
MIL3	j) The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy. k) The cybersecurity program is independently reviewed (i.e., by reviewers who are not in the program) to ensure conformance with cybersecurity policies and procedures. l) The cybersecurity program addresses and enables the achievement of regulatory compliance, as appropriate. m) The cybersecurity program monitors and/or participates in the development and implementation of select cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies.

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

Appendix A. Acronyms

ACM	Asset Identification, Change, and Configuration Management	**IAM**	Identity and Access Management
APT	Advanced Persistent Threat	**ICS**	Industrial Control Systems
ARC	Cybersecurity Architecture	**IT**	Information Technology
C2M2	Cybersecurity Capability Maturity Model	**MIL**	Maturity Indicator Level
CISA	Cybersecurity and Infrastructure Security Agency	**NAC**	Network Access Control
COP	Common Operating Picture	**NIST**	National Institute of Standards and Technology
CPM	Cybersecurity Program Management	**OT**	Operational Technology
CVSS	Common Vulnerability Scoring System	**PPD-21**	Presidential Policy Directive 21
Dams-C2M2	Dams Sector Cybersecurity Capability Maturity Model	**RM**	Risk Management
DDoS	Distributed Denial of Service	**RPO**	Recovery Point Objectives
DHS	U.S. Department of Homeland Security	**RTO**	Recovery Time Objectives
DOE	U.S. Department of Energy	**SA**	Situational Awareness
EIR	Event and Incident Response, Continuity of Operations, and Service Restoration	**SCADA**	Supervisory Control and Data Acquisition
EO 13636	Executive Order 13636	**SCC**	Sector Coordinating Council
GCC	Government Coordinating Council	**TTP**	Tactics, Techniques, and Procedures
ISAC	Information Sharing & Analysis Center	**TVM**	Threat and Vulnerability Management
FERC	Federal Energy Regulatory Commission	**VoIP**	Voice Over Internet Protocol
FIRST	Forum of Incident Response and Security Teams	**VPN**	Virtual Private Network
HSIN-CI	Homeland Security Information Network – Critical Infrastructure	**TPM**	Third-Party Risk Management
HVAC	Heating, Ventilation, and Air Conditioning	**WM**	Workforce Management

Appendix B. Source Documents

Sector Documents

Dams Sector Cybersecurity Framework Implementation Guidance, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2020. cisa.gov/dams-sector-publications (accessed June 2022).

Dams Sector Cybersecurity Program Guidance, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2016. Please contact DamsSector@cisa.dhs.gov to access the document.

Dams Sector Roadmap to Secure Control Systems, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2015. Please contact DamsSector@cisa.dhs.gov to access the document.

Dams Sector-Specific Plan: An Annex to the NIPP 2013, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2015, cisa.gov/dams-sector-publications (accessed June 2022).

Dams Sector Security Awareness Handbook, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2022. Please contact DamsSector@cisa.dhs.gov to access the document.

Dams Sector Security Guidelines, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2015. Please contact DamsSector@cisa.dhs.gov to access the document.

Dams Sector Surveillance and Suspicious Activities Indicators Guide, Washington, D.C.: Cybersecurity and Infrastructure Security Agency, 2021. Please contact DamsSector@cisa.dhs.gov to access the document.

Federal Agency Guidelines

Critical Infrastructure Protection Reliability Standards, Washington, D.C.: North American Electric Reliability Corporation, 2016, nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed June 2022).

Cybersecurity Capability Maturity Model (C2M2), Version 2.1, Washington, D.C.: U.S. Department of Energy, 2022, energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf (accessed July 2022).

Electricity Subsector Cybersecurity Risk Management Process, Washington, D.C.: U.S. Department of Energy, 2012, energy.gov/oe/articles/doe-releases-electricity-subsector-cybersecurity-risk-management-process-rmp-guideline (accessed June 2022).

FERC Security Program for Hydropower Projects: Revision 3A, Washington, D.C.: Federal Energy Regulatory Commission, Division of Dam Safety and Inspections, 2016, ferc.gov/dam-safety-and-inspections/security-program-hydropower-projects-revision-3 (accessed June 2022).

FERC Security Program for Hydropower Projects FAQ, Washington, D.C.: Federal Energy Regulatory Commission, Division of Dam Safety and Inspections, 2020, ferc.gov/sites/default/files/2020-04/faq.pdf (accessed June 2022).

Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1, Gaithersburg, MD: National Institute of Standards and Technology, 2018, nist.gov/cyberframework/framework (accessed June 2022).

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, Washington, D.C.: The White House, 2021. whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (accessed June 2022).

Pipeline Security Guidelines, Washington, D.C.: Transportation Security Administration, 2011, tsa.gov/sites/default/files/pipeline_security_guidelines.pdf (accessed June 2022).

NIST Computer Security Special Publications:

Assessing Security and Privacy Controls in Information Systems and Organizations (NIST 800-53A), Gaithersburg, MD: National Institute of Standards and Technology, 2022, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf (accessed June 2022).

Computer Security Incident Handling Guide (NIST 800-61), Gaithersburg, MD: National Institute of Standards and Technology, 2012, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (accessed June 2022).

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, (NIST 800-161), Gaithersburg, MD: National Institute of Standards and Technology, 2022, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf (accessed June 2022).

Guide for Cybersecurity Event Recovery (NIST 800-184), Gaithersburg, MD: National Institute of Standards and Technology, 2016, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf (accessed June 2022).

Guide for Security-Focused Configuration Management of Information Systems (NIST 800-128), Gaithersburg, MD: National Institute of Standards and Technology, 2019, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf (accessed June 2022).

Guide to Industrial Control Systems (ICS) Security (NIST 800-82), Gaithersburg, MD: National Institute of Standards and Technology, 2015, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (accessed June 2022).

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (NIST 800-84), Gaithersburg, MD: National Institute of Standards and Technology, 2006, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf (accessed June 2022).

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, (NIST 800-37), Gaithersburg, MD: National Institute of Standards and Technology, 2018, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (accessed June 2022).

Secure Software Development Framework Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, (NIST 800-218), Gaithersburg, MD: National Institute of Standards and Technology, 2022, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf (accessed June 2022).

Security and Privacy Controls for Information Systems and Organizations (NIST 800-53), Gaithersburg, MD: National Institute of Standards and Technology, 2020, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed June 2022).

Appendix C. Dams-C2M2 Reference Mapping

This appendix offers a general mapping of the domains and objectives of the Dams-C2M2 to relevant cybersecurity guidance documents. Owners and operators can use this general mapping to relate their existing or planned cybersecurity practices to the different sections of the Dams-C2M2. Note that the majority of objectives for management activities do not show associated mapping due to the specificity of those activities to the internal operations of the organization.

Relevant documents included in the following mapping include:

- **Dams Sector Documents**
  - **Crisis Management Handbook (CMH)**, 2021, CISA
  - **Cybersecurity Program Guidance (DCG)**, 2016, CISA
  - **Protective Measures Handbook (PMH)**, 2017, CISA
  - **Security Awareness Handbook (SAH)**, [revision pending], CISA
- **Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)**, 2018, NIST
- **NIST SP-800 Series**
  - **SP-800-37**, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018, NIST
  - **SP-800-53**, Security and Privacy Controls for Information Systems and Organizations, 2020, NIST
  - **SP-800-53A**, Assessing Security and Privacy Controls in Information Systems and Organizations, 2022, NIST
  - **SP-800-61**, Computer Security Incident Handling Guide, 2012, NIST
  - **SP-800-63-3**, Digital Identity Guidelines, 2020, NIST
  - **SP-800-82**, Guide to Industrial Control Systems (ICS) Security, 2015, NIST
  - **SP-800-84**, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, 2006, NIST
  - **SP-800-161**, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 2022, NIST
  - **SP-800-184**, Guide for Cybersecurity Event Recovery, 2016, NIST
  - **SP-800-218**, Secure Software Development Framework Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, 2022, NIST

The following tables and alignment do not represent a complete listing of relevant documents, nor are all sections of the listed documents included in the mapping.

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
1. Asset Identification, Change, and Configuration Management				
ACM-1	Manage IT and OT Asset Inventory	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 PR.IP-6	SP-800-37 3.1, 3.2 SP-800-53 3.3, 3.4, 3.5 SP-800-53A 4.3, 4.4, 4.5 SP-800-82 4.5, 6.1	**DCG** Cyber Asset Identification (p.3–4), Cyber Asset Criticality (p.4), Criticality Determination (p.5), Criticality Determination Guidance Documents (p.6) **PMH** Cybersecurity (p.32)
ACM-2	Manage IT and OT Asset Configuration	PR.IP-1 PR.IP-4 PR.IP-5 PR.MA-1 PR.MA-2 PR.PT-3 DE.AE-1	SP-800-37 3.1, 3.2 SP-800-53 3.5, 3.9 SP-800-53A 4.5, 4.9 SP-800-82 4.5, 6.1	**DCG** Cyber Asset Identification (p.3), Cyber Asset Criticality (p.4), Cybersecurity Functions: Baselining (p.13–14) **PMH** Cybersecurity (p.32)
ACM-3	Manage Changes to IT and OT Assets	PR.IP-2 PR.IP-3	SP-800-37 3.7 SP-800-53 3.5, 3.9 SP-800-53A 4.5, 4.9 SP-800-82 4.5, 6.1	**DCG** Security Measures (p.14)
ACM-4	Management Activities			
2. Threat and Vulnerability Management				
TVM-1	Reduce Cybersecurity Vulnerabilities	PR.IP-12 ID.RA-1 ID.RA-2 ID.RA-4 PR.DS-1 PR.DS-2 PR.DS-5 PR.DS-6 DE.CM-8 RS.AN-5 RS.MI-3	SP-800-37 3.1, 3.3, 3.5 SP-800-53 3.16 SP-800-53A 4.16 SP-800-82 3.3, 4.5, 6.1 SP-800-84 4.2, 5.2	**DCG** Cybersecurity Risk Assessment (p.7–8), Assessment Tools and Methodologies (p.8–9), Risk Management Strategies (p.12–13), Cybersecurity Awareness (p.16–17) **PMH** Cyber Attack (p.26–27), Cybersecurity (p.32) **SAH** Cyber Threat (p.12-13), Cyberattacks (p.17–19), Site-Specific Vulnerabilities (p.24–26)

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
TVM-2	Respond to Threats and Share Threat Information	PR.IP-8 ID.RA-3 RS.CO-3 RS.AN-5 RS.MI-3	SP-800-37 3.5 SP-800-53 3.8 SP-800-53A 4.8 SP-800-82 3.3, 4.5, 6.1	**DCG** Cybersecurity Risk Assessment (p.7–8), Assessment Tools and Methodologies (p.8–9), Cybersecurity Information Sharing (p.9), Risk Management Strategies (p.12–13) **PMH** Cyber Attack (p.26–27), Cybersecurity (p.32) **SAH** Cyber Threat (p.12-13), Cyberattacks (p.17–19)
TVM-3	Management Activities	PR.IP-7 PR.IP-8		
3. Risk Management				
RM-1	Establish Cybersecurity Risk Management Strategy and Program	ID.GV-1 ID.GV-4 ID.RM-1 ID.RM-2	SP-800-37 3.1 SP-800-53 3.12, 3.13 SP-800-53A 4.12, 4.13 SP-800-82 3.1	**DCG** Risk Management Plan (p.11–12), Risk Management Strategies (p.12–13), Risk Management Guidelines and Frameworks (p.18)
RM-2	Manage Cybersecurity Risk	ID.RA-1 ID.RA-4 ID-RA-5 ID.RA-6 PR.DS-1 PR.DS-2	SP-800-37 3.1, 3.3, 3.5, 3.6 SP-800-53 3.4, 3.16 SP-800-53A 4.4, 4.16 SP-800-82 3.3, 4.5, 6.1	**DCG** Risk Management Plan (p.11–12), Risk Management Strategies (p.12–13), Risk Management Guidelines and Frameworks (p.18) **PMH** Cybersecurity (p.32)
RM-3	Management Activities	PR.IP-7 PR.IP-8		
4. Identity and Access Management				
IAM-1	Establish and Maintain Identities	PR.AC-1 PR.AC-6	SP-800-53 3.1, 3.7 SP-800-53A 4.1, 4.7 SP-800-63-3 4.2, 4.3 SP-800-82 5.15	**DCG** Information System Security Controls (p.14–15)

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
IAM-2	Control Access	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-6 PR.AC-7 DE.CM-3	SP-800-37 2.5, 3.1, 3.7 SP-800-53 3.1 SP-800-53A 4.1 SP-800-63-3 4.2, 4.3 SP-800-82 5.15	**DCG** Information System Security Controls (p.14–15) **PMH** Cybersecurity (p.32)
IAM-3	Management Activities	PR.IP-7 PR.IP-8		
5. Situational Awareness				
SA-1	Perform Logging	PR.MA-1 PR.MA-2 PR.PT-1	SP-800-53 3.3 SP-800-53A 4.3 SP-800-82 5.16	
SA-2	Perform Monitoring	PR.PT-1 DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-6 DE.CM-7	SP-800-37 3.1, 3.7 SP-800-53 3.4 SP-800-53A 4.4 SP-800-82 5.16	
SA-3	Establish and Maintain a Common Operating Picture		SP-800-53 3.2 SP-800-53A 4.2	
SA-4	Management Activities			
6. Event and Incident Response, Continuity of Operations, and Service Restoration				
EIR-1	Detect Cybersecurity Events	DE.AE-2 DE.AE3 DE.CM-4 DE.CM-5 DE.DP-2	SP-800-53 3.8 SP-800-53A 4.8 SP-800-61 3.2 SP-800-82 5.17, 6.2	**CMH** Cyber Incident Response Plan (p.15) **DCG** Incident Response (p.19–20) **SAH** Cyberattacks (p.17–19), Cyber [event] (p.30–31)
EIR-2	Escalate Cybersecurity Events and Declare Incidents	DE.AE-2 DE.AE-4 DE.AE-5 RS.AN-1 RS.AN-4	SP-800-61 2.1, 3.2 SP-800-82 3.3, 5.17	**CMH** Cyber Incident Response Plan (p.15) **DCG** Incident Response (p.19–20)

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
EIR-3	Respond to Cybersecurity Events and Incidents	DE.AE-2 DE.AE-4 DE.DP-4 RS.RP-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.AN-1 RS.AN-2 RS-AN-3 RS.MI-1 RS.MI-1 RC.RP-1	SP-800-37 3.4 SP-800-53 3.8 SP-800-53A 4.8 SP-800-61 3.3 SP-800-82 5.17, 6.2	**CMH** Cyber Incident Response Plan (p.15), Recovery Plans (p.25-28) **DCG** Incident Response (p.19–20)
EIR-4	Plan for Continuity of Operations	ID.SC-5 PR.IP-9 PR.IP-10 PR.IP-10 RC.RP-1 RC.IM-1 RC.IM-2 RC.CO-2	SP-800-53 3.6 SP-800-53A 4.6 SP-800-61 2.3 SP-800-82 4.1, 4.2, 6.2 SP-800-184 2.1–2.6, 3.1–3.3	**CMH** Continuity Plans (p.29–32) **DCG** Continuity of Operations (p.20), Disaster Recovery (p.20)
EIR-5	Management Activities	PR.IP-7 PR.IP-8 DE.DP-1 DE.DP-4 DE.DP-5 RS.RP-1 RS.CO-1 RC.CO-3	SP-800-184 3.1–3.3	

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
7. Third-Party Risk Management				
TPM-1	Identify and Prioritize Dependencies	ID.AM-6 ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5 ID.RM-3 ID.SC-1 ID.SC-2 PR.PT-5	SP-800-37 2.8 SP-800-53 3.20 SP-800-53A 4.20 SP-800-82 2.2, 6.2 SP-800-161 2.3, 3.1	**DCG** Vendor Security (p.15–16) **SAH** Supply Chain (p.17–18), Dependency and Interdependency Vulnerabilities (p.27–28)
TPM-2	Manage Dependency Risk	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5 PR.AT-3 PR.DS-4 PR.PT-5 DE.CM-6 RS.CO-5	SP-800-37 2.8 SP-800-53 3.20 SP-800-53A 4.20 SP-800-82 2.2, 6.2 SP-800-161 2.3, 3.1, 3.4	**DCG** Vendor Security (p.15–16) **SAH** Supply Chain (p.17–18)
TPM-3	Management Activities	PR.IP-8		
8. Workforce Management				
WM-1	Assign Cybersecurity Responsibilities	ID.AM-6 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1	SP-800-37 3.1, 3.7 SP-800-53 3.1, 3.2 SP-800-53A 4.1, 4.2 SP-800-63-3 4.1, 4.2, 4.3 SP-800-82 4.2 SP-800-84 2.1, 2.2	**DCG** Information System Security Controls (p.14–15)
WM-2	Develop Cybersecurity Workforce	PR.AT-1	SP-800-53A SP-800-82 4.2, 6.2 SP-800-84 2.1, 2.2, 3.1	**DCG** Information System Security Controls (p.14–15) **PMH** Cybersecurity (p.32)

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
WM-3	Implement Workforce Controls	PR.IP-11 PR.AT-1	SP-800-53 3.1 SP-800-53A 4.1 SP-800-63-3 4.2, 4.3 SP-800-82 6.2 SP-800-84 3.1, 6.3	**DCG** Information System Security Controls (p.14–15) **PMH** Cybersecurity (p.32)
WM-4	Increase Cybersecurity Awareness	PR.IP-8 PR.AT-1	SP-800-53 3.2 SP-800-53A 4.2 SP-800-82 6.2 SP-800-84 3.1	**CMH** Exercises (p.33–37) **DCG** Information System Security Controls (p.14–15), Cybersecurity Awareness (p.16–17) **PMH** Cybersecurity (p.32)
WM-5	Management Activities	PR.IP-8		
9. Cybersecurity Architecture				
ARC-1	Establish and Maintain Cybersecurity Architecture Strategy and Program	PR.AC-1	SP-800-82 4.3, 4.5 SP-800-218 2.1	
ARC-2	Implement Network Protections as an Element of the Cybersecurity Architecture	PR.AC-5 PR.DS-7 PR.PT-4	SP-800-82 5.1–5.17	
ARC-3	Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture	PR.DS-3 PR.DS-6 PR.DS-8 PR.PT-2	SP-800-82 2.4, 4.5	
ARC-4	Implement Software Security as an Element of the Cybersecurity Architecture	PR.DS-6	SP-800-82 2.4 SP-800-218 2.1–2.4	
ARC-5	Implement Data Security as an Element of the Cybersecurity Architecture	PR.DS-1 PR.DS-2 PR.DS-5 PR.DS-6	SP-800-82 5.10	
ARC-6	Management Activities	PR.IP-8		

Notation	Objective	Relevant Reference Documents		
		NIST CSF	NIST SP-800	Dams Sector Documents
10. Cybersecurity Program Management				
CPM-1	Establish Cybersecurity Program Strategy	ID.GV-1 ID.GV-3 ID.GV-4 ID.RM-1 ID.RM-2	SP-800-37 3.1 SP-800-53 3.12, 3.13 SP-800-53A 4.12, 4.13 SP-800-82 4.3, 6.2	**DCG** Primary Elements of a Cybersecurity Program (p.1)
CPM-2	Sponsor Cybersecurity Program	PR.AT.4	SP-800-82 4.1	
CPM-3	Management Activities			