ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE

DRAFT FOR PUBLIC COMMENT

SEPTEMBER, 2014

TABLE OF CONTENTS

List of Figures

List of Tables

CAUTIONARY NOTE

This publication is not intended for regulatory use. It is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that energy sector organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, this publication uses the words "adopt", "use", and "implement" interchangeably. These words are not intended to imply compliance or mandatory requirements.

ACKNOWLEDGMENT

The Department of Energy (DOE) acknowledges the dedication and technical expertise of all the organizations and individuals who participated in the development of the Energy Sector Framework Implementation Guidance. This document is based on inputs from members of framework guidance development workgroups under the Electricity Subsector Coordinating Council (ESCC) and Oil & Natural Gas Subsector Coordinating Council (ONG SCC). The DOE also acknowledges inputs provided by members of the government partners working group, representing different public sector organizations, as well as comments provided by other public and private stakeholders during the public comment period.

1. INTRODUCTION

The National Institute of Standards and Technology (NIST) released the voluntary Cybersecurity Framework (Framework) in February 2014 to provide a common language organizations can use to assess and manage cybersecurity risk. Developed in response to Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity" of February 2013, the Framework recommends risk management processes that enable organizations to inform and prioritize decisions regarding cybersecurity based on business needs, without additional regulatory requirements. It enables organizations—regardless of sector, size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. Each sector and individual organization can use the Framework in a tailored manner to address its cybersecurity objectives.

Energy sector organizations have a strong track record of working together to develop cybersecurity standards, tools, and processes that ensure uninterrupted service. The U.S. Department of Energy (DOE), as the Energy Sector-Specific Agency (SSA), worked with the Energy Sector Coordinating Councils and other SSAs to develop this Framework Implementation Guidance specifically for energy sector owners and operators. It is tailored to the energy sector's risk environment and existing cybersecurity and risk management tools and processes that organizations can use to implement the Framework. This Framework Implementation Guidance is designed to assist energy sector organizations to:

- Characterize their current and target cybersecurity posture.
- Identify gaps in their existing cybersecurity risk management programs, using the Framework as a guide, and identify areas where current practices may exceed the Framework.
- Recognize that existing sector tools, standards, and guidelines may support Framework implementation.
- Effectively demonstrate and communicate their risk management approach and use of the Framework to both internal and external stakeholders.

Section 2 provides key Framework terminology and concepts for its application, and Section 3 identifies example resources that may support Framework use. Section 4 outlines a general approach to Framework implementation, followed in Section 5 by an example of a tool-specific approach to implementing the Framework. The tool selected for this example is the DOE- and industry-developed Cybersecurity Capability Maturity Model (C2M2; DOE 2014a).

Energy sector organizations, particularly those that are using the Framework to establish a new security risk management program are invited to contact DOE via email at cyber.framework@hq.doe.gov with any questions or requests for direct assistance.

2. Preparing for Framework Implementation

This section helps in preparation for Cybersecurity Framework implementation by presenting key Framework terminology, concepts, and benefits.

2.1 Framework Guidance Terminology

The three main elements of the Cybersecurity Framework (NIST 2014) are the **Core**, the Framework **Implementation Tiers (Tiers)**, and the **Profile**. These terms are frequently used in this Framework guidance document and defined below.

The ***Core*** is a set of "cybersecurity activities, desired outcomes, and applicable informative references that are common across critical infrastructure sectors," which are organized under five Functions: Identify, Protect, Detect, Respond, and Recover. Each **Function** is divided into Categories, Subcategories, and informative references. The **Categories** are cybersecurity outcomes that are closely tied to programmatic needs and particular activities. The **Subcategories** are specific outcomes of technical and/or management activities that support achievement of each Category. Informative references are specific cross-sector standards, guidelines, and best practices that illustrate a method to achieve the outcomes associated with each Subcategory.

Tiers describe an organization's approach to "cybersecurity risk and the processes in place to manage that risk," ranging from Tier 1 (Partial) to Tier 4 (Adaptive). Each Tier demonstrates an increasing degree of rigor and sophistication of cybersecurity risk management and integration with overall organizational needs. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Tiers are associated with the overall robustness of an organization's risk management process and are *not* tied to Functions, Categories, or Subcategories. An organization may align its application of the Tiers with its desired scope for using the Framework (e.g., if an organization is using the Framework for a specific business function only, the Tiers could be used to describe the overall robustness of risk management processes at that business function level).

Profiles align the Framework core elements with business requirements, risk tolerance, and organizational resources. The Profile can be used to identify opportunities for improving cybersecurity posture by comparing a Current Profile to a Target Profile. Profiles provide a roadmap to reduce cybersecurity risk consistent with business practices.

This document also frequently refers to the term ***organization***, which describes a functional entity of any size that uses the same cybersecurity risk management program within its different components and may individually use the Framework. This may describe one corporation, or one business unit within a multi-unit corporation. As each company may develop and implement its risk management programs at different levels, this guidance is designed for any organization, be it the enterprise or a business unit within the enterprise.

2.2 Framework Guidance Concepts

This document provides guidance to organizations at all different levels of maturity in their cybersecurity and risk management programs.

For organizations that do not have a cybersecurity risk management program, this implementation guidance will assist organizations in directly implementing the Framework or selecting an alternative approach (such as a widely used set of standards or security and risk management tools) that effectively implements the Framework by its use.

For organizations that have an existing cybersecurity risk management program, this document will assist them in reviewing their existing program, identifying any cybersecurity and risk management gaps, and aligning their existing program to the key Framework elements. Aligning current approaches to the Framework can help demonstrate implementation and support the organization in communicating its cybersecurity risk profile and management approach with internal organizations and external stakeholders.

To use the Framework, an organization does not have to directly match every element in their organization's cybersecurity program with the Framework elements. However, organizations who wish to demonstrate their alignment with the Framework are recommended to review and document the alignment of their program and practices with the objectives of the Framework's Core Functions, Tiers, and Profiles.

The Framework includes considerations to address **privacy and civil liberties issues** during implementation. In certain sectors and organizations, these issues might be directly applicable to the reliable delivery of critical services. In other sectors and organizations, these issues may not be relevant because of the nature of the information the organizations handle and the degree to which it is aggregated. This Framework guidance document does not directly address privacy and civil liberties issues. However, organizations are encouraged to review and consider using the Framework's privacy and civil liberties guidance (NIST 2014, p. 15) in alignment with other privacy guidelines and state and federal laws.

2.3 Framework Implementation Process and Benefits

The Framework and this guidance are designed to be flexible enough to be used both by energy sector organizations with mature cybersecurity and risk management programs and by those with less-developed programs. Each organization will choose if, how, and where it will use the Framework based on its own operating environment. Choosing to implement the Framework does not imply that an existing cybersecurity and risk management approach is ineffective or needs to be replaced. Rather, it means that the organization wishes to take advantage of the benefits that the Framework offers.

Implementing the Framework provides the mechanism for an organization to:

1. Describe their current cybersecurity posture in terms of **Functions**, **Category** and **Subcategory Outcomes,** and **Implementation Tiers** for appropriate stakeholders.
2. Describe the **Current and Target Profiles** for their cybersecurity programs.
3. Assess progress toward the desired **Target Profiles**.

4. **Identify and prioritize opportunities for improvement** within the context of a continuous and repeatable process.
5. **Communicate the Current and Target Profiles** and other risk management information to internal and external cybersecurity risk stakeholders.

Organizations with less-developed cybersecurity risk management programs can use the framework to define and establish a program that successfully addresses cybersecurity risk commensurate with the organization's business and critical infrastructure security objectives.

A key benefit of Framework implementation is to strengthen an organization's risk management approach and communicate its use of particular cybersecurity practices to internal and external stakeholders. The implementation approach detailed in Section 4 guides organizations to map their existing cybersecurity and risk management approaches (e.g., standards, tools, methods, and guidelines) to the Framework's Core and Implementation Tiers. The mapping may:

- **Identify gaps between the outcomes achieved by the organization's approach and the outcomes defined in the Framework Core and the organization's desired Implementation Tier**. The organization may take steps to address these gaps, or may ultimately determine that these differences are not significant or material to managing its cybersecurity risks. However, the organization may need to describe and document these differences to facilitate communications about the organization's use of the Framework.
- **Identify areas where the organization's approach is more comprehensive than the Framework Core and desired Implementation Tier.** Due to specific organizational or critical infrastructure risks, an organization may deploy cybersecurity approaches that achieve outcomes that go above and beyond the outcomes described by the Framework's Core Categories and Subcategories or Implementation Tiers. Those organizations may also need to identify and document those differences to facilitate risk communication with internal and external stakeholders. When appropriate, energy sector organizations should consider sharing their risk management approach with DOE and NIST to help strengthen and expand the Framework.

Ideally, the Framework would be incorporated as part of an ongoing cybersecurity and risk management process improvement program.

3. Sector Framework Guidance Resources

This section presents an overview of some of the existing cybersecurity tools and processes currently in use by the energy sector that may support Framework implementation.

3.1 Sample Energy Sector Security and Risk Management Approaches

Several cybersecurity risk management tools, processes, standards, and guidelines already widely used by energy sector organizations may align well with Framework security and risk management approaches and help demonstrate how an organization is already applying Framework concepts. While this Framework guidance document only supplies a mapping of one tool—the Cybersecurity Capability Maturity Model (C2M2)—to the Framework, other in-use approaches will likely support an organization in mapping its program to the Framework. An example set of readily available tools and processes used across the energy sector is described in Table 1. Other tools and processes are in active use, or in development, which may provide similar cybersecurity risk management capabilities.

Table 1: Example Cybersecurity Tools and Processes

Name	Summary	Additional Information
Cybersecurity Capability Maturity Model (C2M2), both electricity and oil and natural gas sector-specific versions	Used to assess an organization's cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity.	http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2
Cyber Resilience Review (CRR)	Evaluates an organization's operational resilience and cybersecurity practices across ten domains.	https://www.us-cert.gov/ccubedvp/self-service-crr
Cyber Security Evaluation Tool (CSET)	Guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards.	http://ics-cert.us-cert.gov/Assessments
Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline	Enables organizations to apply effective and efficient risk management processes and tailor them to meet their organizational requirements.	http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012

3.2 Sample Subsector-Specific Security and Risk Management Approaches

The electricity and oil and natural gas subsectors each have tailored standards or cybersecurity approaches that many organizations may use voluntarily or by requirement, in addition to the cross-sector informative references identified in the Framework Core. Some of these, like the C2M2 (included in Table 1), have customized versions for different subsectors. This section presents examples of tools and processes that are applicable only to specific subsectors.

Table 2. Examples of Electricity Subsector Tool and Processes

Name	Summary	Additional Information
Critical Infrastructure Protection (CIP) Standards	The North American Electric Reliability Corporation (NERC) CIP Standards provide a set of regulatory cybersecurity requirements to assist in securing the energy system assets that operate and maintain the bulk electric grid.	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security	These National Institute of Standards and Technology (NIST) guidelines present an analytical framework to develop effective cybersecurity strategies tailored to their particular smart grid-related characteristics, risks, and vulnerabilities.	http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

Table 3. Examples of Oil and Natural Gas Subsector Tools and Processes

Name	Summary	Additional Information
Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	This Interstate Natural Gas Association of America (INGAA) guideline assists operators of natural gas pipelines in managing their control systems cyber security requirements. It sets forth and details the unique risk and impact-based differences between the natural gas pipeline industry and the hazardous liquid pipeline and liquefied natural gas operators.	http://www.ingaa.org/
API OS0001 – Security Guidance	This American Petroleum Institute (API) document provides guidance on security for	http://www.api.org/publications-standards-and-

Name	Summary	Additional Information
for the Petroleum Industry, Second Edition	worldwide offshore oil and natural gas operations.	statistics
Chemical Facilities Anti-Terrorism Standards	These risk-based performance standards (RBPS) from the Department of Homeland Security (DHS) provide guidance on physical and cybersecurity for organizations handling chemicals of interest. RBPS 8 specifically requires facilities regulated by CFATS to address cybersecurity in their facility security plan.	http://www.dhs.gov/chemical-facility-anti-terrorism-standards

3.3 MAPPING TO THE FRAMEWORK

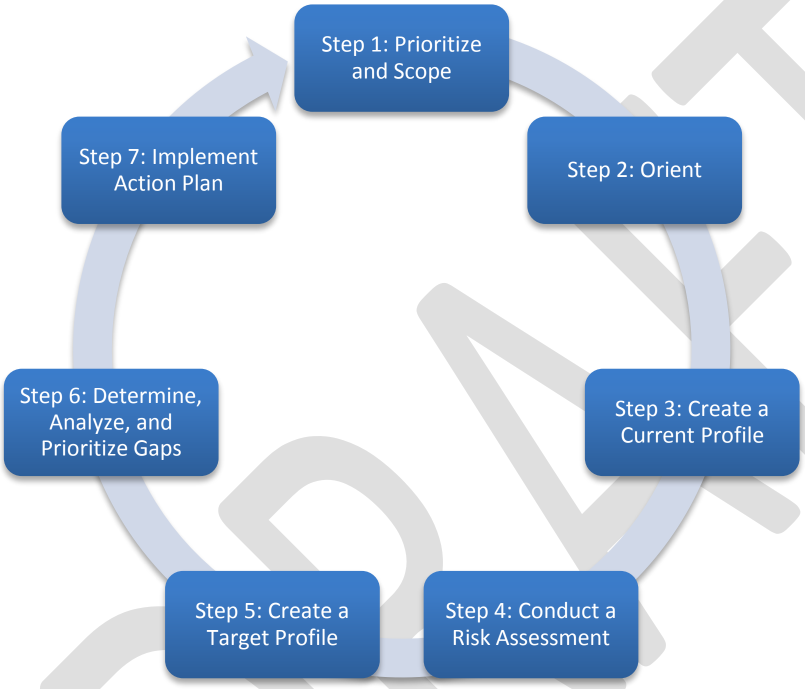
Section 5 details a Framework implementation approach using the C2M2, and a mapping of the C2M2 to the Framework is provided in Appendix A. Vendors and standards developers may also have separately developed mappings of other tools and processes to the Framework. Organizations may use any such mappings along with this guidance to support use of the Framework. For more information on available mappings, please contact the developer of the practice, tool, or standard, or the appropriate Subsector Coordinating Council.

Organizations can map their current cybersecurity approach to the Framework elements, using tool-specific mappings as a guide where possible. Mapping not only supports an organization's ability to identify potential gaps that may need to be addressed, but it can also highlight where the Framework does not adequately describe the organization's cybersecurity approach. A clear mapping provides a translation between the organization's current practices and the Framework taxonomy, supporting communication to external stakeholders. See "Step 3: Create a Current Profile" in Section 4 for guidance about using mappings with the Framework.

4. Approach to Framework Implementation

This section presents a standard approach for using the Framework (Figure 1) that is aligned with the seven-step process outlined in the Framework document (NIST 2014; section 3.2). This approach can be used along with any cybersecurity standard, energy-sector-specific tool, or commercial tool for managing cybersecurity risk—such as those described in Section 3 of this document—to facilitate Framework implementation. (As an example, Section 5 of this guidance document explains how Cybersecurity Capability Maturity Model [C2M2] implementation fits within this approach.)

Figure 1: Framework Implementation Approach


Step 1: Prioritize and Scope
Step 2: Orient
Step 3: Create a Current Profile
Step 4: Conduct a Risk Assessment
Step 5: Create a Target Profile
Step 6: Determine, Analyze, and Prioritize Gaps
Step 7: Implement Action Plan

Each step is introduced by a table describing the step's inputs, activities, and outputs. Additional explanation is provided below each table. A summary table of the inputs, activities, and outputs for each step is included in Appendix B.

Many energy sector organizations already have comprehensive risk management programs that allow for framing risk (i.e., establish the context for risk-based decisions), assessing risk, addressing identified risk, and monitoring risk on an ongoing basis. Many also use effective communications and an iterative feedback loop for continuous improvement (see the *Electricity Subsector Cybersecurity Risk Management Process Guideline* [RMP; DOE 2012b] for a possible risk management approach). For these organizations, the activities described in these seven steps are most likely already performed, and implementing the Framework is largely a matter of describing and aligning or "translating" elements of their current approach to the Framework Core and Implementation Tiers.

Step 1: Prioritize and Scope

Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Threat information	1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cybersecurity capabilities	1. Framework usage scope

A risk management process typically includes a strategy addressing how to frame, assess, respond to, and monitor risk. This strategy may be developed at the company/entity level for all of the company's organizations, or individual strategies may be developed at the organizational level. Regardless, the applicable strategy explicitly and transparently describes the identified organizational risks that the organization routinely uses to inform investment and operational decisions. This strategy should recognize each organization's contribution to the national security of critical energy infrastructure, and includes both organization-specific and sector-wide objectives and priorities for risk management (see the *Electricity Subsector Cybersecurity Risk Management Process Guideline* [RMP; DOE 2012b] for a possible approach).

In this step, the organization decides how and where it wants to use the Framework (its Framework usage scope)—whether in a subset of its operations, in multiple subsets of its operations, or for the entire organization. This decision should be based on the organization's risk management strategy, organizational and critical infrastructure objectives and priorities, availability of resources, its current risk environment, and other internal and external factors. Current threat information (e.g., information from important vendors, communications from the Electricity and Oil and Natural Gas Information Sharing and Analysis Centers [ISACs], or other threat advisories) may also help inform scoping decisions.

It is recommended that organizations using the Framework for the first time identify a small subset of operations for initial Framework application to gain familiarity and experience with the Framework. After this pilot activity, the organization can consider applying the Framework to a broader subset of operations or to additional parts of the organization as appropriate.

Step 2: Orient

Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and informative references (e.g., cybersecurity and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (i.e., regulatory, company, organizational) 3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines 4. Evaluation approach

The organization identifies the systems, assets, requirements, and cybersecurity and risk management approaches that are in scope. This includes standards and practices the organization already uses, and could include additional standards and practices that the organization believes would help achieve its critical infrastructure and business objectives for cybersecurity risk management. The organization's risk management program will often already have identified and documented much of this information or the program can help identify individual outputs. A good general rule is to initially focus on critical systems and assets and then expand the focus to less critical systems and assets as resources permit.

The organization should also determine the evaluation approach it will use to identify its current cybersecurity and risk management states. Organizations can use any of a number of evaluation methods to identify their current cybersecurity approach and create a Current Profile. For example, these include self-evaluations, where an organization may leverage its own resources and expertise, or facilitated approaches, where the evaluation is performed by a third party.

Step 3: Create a Current Profile

Inputs	Activities	Outputs
1. Evaluation approach 2. In-scope systems and assets 3. In-scope regulatory requirements 4. In-scope cybersecurity and risk management standards, tools, methods, and guidelines	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile 2. Current Implementation Tier

The organization creates a Current Profile and identifies its current Implementation Tier by mapping its existing cybersecurity and risk management practices to specific descriptions in the Framework document (NIST 2014). It is important to understand that the purpose of identifying a Current Profile is not simply to create a map between organizational practices and Category and Subcategory outcomes, but also to understand the degree to which those practices *achieve the outcomes* outlined by the Framework.

To identify the Current Profile, the organization uses the evaluation approach identified in Step 2 to map its existing cybersecurity approach and outcomes to the Category and Subcategory outcomes in Appendix A of the Framework document (called the Framework Core). Organizations may already perform these evaluations as part of risk assessment or have defined processes that can be leveraged to identify their current state. For example, many organizations perform regular evaluations of their cybersecurity programs through internal audits or similar activities. The outputs of those activities may describe which practices are performed for in-scope systems and assets and can be used for this step.

The current Implementation Tier describes the degree of rigor and sophistication of the in-scope cybersecurity risk management program. To identify the Implementation Tier, the organization maps its current approach to the Implementation Tier descriptions in the Framework document (NIST 2014). Implementation Tiers do not apply to the individual Functions and Categories and Subcategories outcomes in the Framework Core; the organization identifies an Implementation Tier for the in-scope cybersecurity and risk management program as a whole. Organizations may already be using tools and processes or complying with industry standards that closely align with the Framework. Some industry and standards organizations have begun to publish their own guidance to map existing standards and tools to the Framework elements to facilitate implementation. (Section 5 of this guidance, for example, maps the C2M2 to the Framework).

Table 4 provides an example of how a mapping can be used to create a Current Profile for a specific Subcategory outcome (see Section PR.AC-3 of the Framework document [NIST 2014]) for three organizations using three different approaches. A similar table could be built for Implementation Tiers, keeping in mind that Tiers are focused at broader program level risk management. Note that the examples in these tables are intended to be illustrative of the mapping concept and are unlikely to address any specific organization's particular approach. The level of specificity and granularity required for a Profile to be useful will be unique to each organization.

Table 4: Connecting Organizational Approach to Framework

Organization 1
Internal Controls Approach

Function	Category	Subcategory	Profiles
			Current
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-3:** Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged

			• Immediate disabling of VPN account upon employee termination

Organization 2
Standards Based Approach

Function	Category	Subcategory	Profiles
			Current
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-3:** Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)

Organization 3
Exception Approach

Function	Category	Subcategory	Profiles
			Current
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-3:** Remote access is managed	• Not Applicable - No remote access available for in-scope assets and systems

While the Framework provides broad coverage of the cybersecurity and risk management domains, it is not all-inclusive, and the organization may have deployed standards, tools, methods, and guidelines that achieve outcomes not defined by or referenced in the Framework. The Current Profile should identify these practices as well. When appropriate, organizations should consider sharing these practices with NIST to help strengthen and expand the Framework.

Step 4: Conduct a Risk Assessment

Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy 3. Organization-defined risk assessment approach 4. In-scope regulatory requirements 5. In-scope cybersecurity and risk management standards, tools, methods, and guidelines	1. Perform risk assessment for in-scope portion of the organization	1. Risk assessment reports

Organizations perform cybersecurity risk assessments to identify and evaluate cybersecurity risks and determine which are outside of current tolerances. The outputs of cybersecurity risk assessment activities assist the organization in developing its Target Profile and identifying a Target Implementation Tier, which occurs in Step 5. (See the *Electricity Subsector Cybersecurity Risk Management Process Guideline* [DOE 2012b] and *Integrating Electricity Subsector Failure Scenarios into a Risk Assessment*

Methodology [DOE 2013] for possible guidance on performing a cybersecurity risk assessment.) For organizations that have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist.

Step 5: Create a Target Profile

Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Organizational objectives 4. Risk management strategy 5. Risk assessment reports	1. Organization identifies goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives	1. Target Profile 2. Target Tier

In creating a Target Profile, the organization should consider:

- Current risk management practices
- Current threat environment
- Legal and regulatory requirements
- Business and mission objectives
- Organizational constraints

The Target Profile identifies the desired Category and Subcategory outcomes and associated cybersecurity and risk management standards, tools, methods, and guidelines that will mitigate cybersecurity risks, commensurate with the risk to organizational and critical infrastructure security objectives. As noted in Step 3, the Framework provides broad coverage of the cybersecurity and risk management domains, but is not all-inclusive. The organization may need to deploy standards, tools, methods, and guidelines that achieve outcomes not defined by the Framework. The Target Profile should also identify these practices.

Table 5 provides an example of a Target Profile for a specific Subcategory outcome (PR.AC-3) for three organizations using three different approaches. The ***bold and italicized*** text in the Target Profile highlights where the organization has identified additional practices it desires to use to successfully achieve an outcome based on its current risk environment and business and critical infrastructure objectives. Organization 1 has determined that its current practices for managing remote access are not adequate for addressing its unique risk environment, and identifies additional practices that are required. Organization 2 comes to the same conclusion and identifies additional standards that it wants to roll out across the in-scope organization. Organization 3 shows an organization whose Current Profile is the same as the Target Profile for this Subcategory outcome. This will be the case when the standards, tools, methods, and guidelines currently deployed by the organization meet its cybersecurity and risk management requirements. While not included in an example, an organization may determine that a current practice is no longer necessary or is inadequate and it might be omitted from the Target Profile.

In developing a Target Profile, organizations may take a broad approach—considering more effective and efficient risk management approaches across the entire in-scope organizations—rather than examining individual Categories and Subcategories.

In addition to the Target Profile, the organization selects a Target Implementation Tier that applies to the in-scope risk management process. The organization examines each Tier and selects its target (the "desired" state), using the same list of considerations above for the Target Profile. Once a Target Implementation Tier is selected, the organization identifies the cybersecurity practices and risk management activities necessary to achieve that target—considering their ability to meet organizational goals, feasibility to implement, and their ability to reduce cybersecurity risks to acceptable levels for critical assets and resources (i.e., those most important to achieving the organization's business and critical infrastructure objectives).

Using its collection of cybersecurity and risk management standards, tools, methods, and guidelines, the organization documents these desired outcomes in the Target Profile and Target Implementation Tier.

Table 5: Creating a Target Profile

Organization 1
Internal Controls Approach

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-3:** Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • ***Supervisor signature required before VPN account issued*** • ***Bi-annual review of authorized VPN account list***

Organization 2
Standards Based Approach

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-3:** Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • ***NIST SP 800-53 Rev 4 AC-17 (3)*** • ***NIST SP 800-53 Rev 4 AC-17 (4)*** • NIST SP 800-53 Rev 4 AC-19 • ***NIST SP 800-53 Rev 4 AC-19 (5)*** • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • ***NIST SP 800-53 Rev 4 AC-20 (2)***

Organization 3
Exception Approach

Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	**Access Control**	**PR.AC-3:** Remote	• Not Applicable - No remote access available for in-scope assets and systems	• Not Applicable - No remote access available to in-scope assets and systems

🟪	**(PR.AC)**	access is managed		

Bold and italicized text highlights the differences between the current and target approaches.

Step 6: Determine, Analyze, and Prioritize Gaps

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

The organization evaluates its Current Profile and Implementation Tier against its Target Profile and Target Implementation Tier and identifies any gaps. It is important to include inputs from all appropriate organizational stakeholders to ensure that business and critical infrastructure objectives are considered in the prioritization process.

A gap exists when there is a desired Category or Subcategory outcome in the Target Profile or program characteristic in the Target Implementation Tier that is not currently achieved by the organization's existing cybersecurity and risk management approach, as well as when current practices do not achieve the outcome to the degree of satisfaction required by the organization's risk management strategy. The ***bold and italicized*** text in Table 6 provides some very simple examples where organizations may identify additional practices or standards to achieve outcomes to the degree required by the organization's risk tolerances.

As noted, the identified Framework Category and Subcategory outcomes may not address all of the organization's cybersecurity risks. However, the Target Profile should include all applicable cybersecurity practices, tools, standards, and guidelines that will be used by the organization to address cybersecurity risk commensurate with the risk to organizational and critical infrastructure objectives, even if those go beyond the outcomes identified in the Framework.

Table 6: Identifying Implementation Gaps

Organization 1
Internal Controls Approach

Function	Category	Subcategory	Profiles		
			Current	**Target**	**Gaps**
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-3:** Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • Supervisor signature required before VPN account issued • Bi-annual review of authorized VPN account list	• ***Supervisor signature required before VPN account issued*** • ***Bi-annual review of authorized VPN account list***

Organization 2
Standards Based Approach

Function	Category	Subcategory	Profiles		
			Current	**Target**	**Gaps**
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-3:** Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-17 (3) • NIST SP 800-53 Rev 4 AC-17 (4) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-19 (5) • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • NIST SP 800-53 Rev 4 AC-20 (2)	• ***NIST SP 800-53 Rev 4 AC-17 (3)*** • ***NIST SP 800-53 Rev 4 AC-17 (4)*** • ***NIST SP 800-53 Rev 4 AC-19 (5)*** • ***NIST SP 800-53 Rev 4 AC-20 (2)***

Organization 3
Exception Approach

Function	Category	Subcategory	Profiles		
			Current	Target	Gaps
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-3:** Remote access is managed	• Not Applicable - No remote access available for in-scope assets and systems	• Not Applicable - No remote access available for in-scope assets and systems	• ***None***

Bold and italicized text indicates gaps between the Current and Target Profiles.

After identifying both types of gaps (Profile and Tier), the organization determines the potential consequences of failing to address those gaps. A mitigation priority should then be assigned to all identified gaps. Prioritization should consider current risk management practices, the current threat environment, legal and regulatory requirements, business and mission objectives, and any organizational constraints deemed relevant.

Once each gap is assigned a mitigation priority, the organization identifies potential mitigation activities and performs a cost-benefit analysis (CBA) on those potential actions. Where applicable, a CBA should consider the cost of possible regulatory fines or sanctions. The organization develops a plan of prioritized mitigation actions—based on available resources, business needs, and current risk environment—to move from the current state to the target state. If the organization is at its target state, it would seek to maintain its security posture as the risk landscape changes.

Step 7: Implement Action Plan

Inputs	Activities	Outputs
1. Prioritized implementation plan	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks, metrics, and performance indicators 4. Report progress	1. Project tracking data 2. New security measures implemented

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

4.1 Summary of Seven-Step Approach

This implementation approach can help organizations to use the Framework to establish a strong cybersecurity program or to validate the effectiveness of an existing program. It enables organizations to map their existing program to the Framework, identify improvements, and communicate results. It can incorporate and align with processes and tools the organization is already using or plans to use.

This approach, as Figure 1 showed, is intended to be a continuous process, repeated according to organization-defined criteria (such as a specific period of time or a specific type of event) to address the evolving risk environment. Implementation of this approach should include a plan to communicate progress to appropriate stakeholders, such as senior management. Ideally this process would be integrated into an organization’s risk management program.

5. Cybersecurity Capability Maturity Model (C2M2) Approach to Framework Implementation

The Cybersecurity Capability Maturity Model (C2M2) was developed by the Department of Energy (DOE) and contributors from industry and other government agencies to help critical infrastructure organizations evaluate and potentially improve their cybersecurity practices. As this section demonstrates, using the C2M2 also provides a means for any energy sector organization to implement the Framework.

The C2M2 includes a self-evaluation toolkit that guides each organization to identify its cybersecurity and risk management practices, map them to specific levels of maturity within the model, set target maturity levels, and identify gaps and potential practices that allow the organization to mature over time. The C2M2 covers *all* of the practices of the Framework Core and Tiers, and the C2M2 and its supporting toolkit guide an organization to identify its Current Profile and to establish a Target Profile.

This section outlines the benefits of using the tool-specific (vs. general) approach to the Framework, briefly describes the C2M2 in further detail, and demonstrates how it can support the Framework in seven steps. A complete, detailed mapping of the C2M2 to the Framework is provided in Appendix A.

5.1 Benefits of the C2M2 Approach to Framework Implementation

In addition to providing an industry-developed, step-by-step process that aligns well with that of the Framework, the C2M2 offers the following benefits to energy sector owners and operators interested in demonstrating their implementation of the Framework:

- ***A common goal***: The purpose of both the Framework and the C2M2 is to help critical infrastructure organizations evaluate and potentially improve their cybersecurity capabilities.
- ***Widespread use***: The C2M2 has already been adopted by many energy sector entities, which enables organizations to voluntarily share knowledge and best practices using common terminology.
- ***Supports benchmarking across the sector***: Broad use of the model by each subsector could support benchmarking of the sector's cybersecurity capabilities.
- ***Tailored sector-specific risk mitigation***: The C2M2 has two variants that have each been specifically tailored to address concerns of either the Electricity Subsector or the Oil and Natural Gas Subsector, using sector-specific analysis of cyber risk mitigation, including descriptive guidance specific to energy sector control systems.
- ***Descriptive guidance for the Framework***: The C2M2 provides descriptive rather than prescriptive guidance at a high level of abstraction. This helps organizations of all types,

structures, and sizes to map C2M2 practices to Framework Subcategories. Also, the recommended process for using the C2M2 parallels the Framework approach of setting a target, identifying gaps, and addressing gaps.

- ***Complete coverage of Framework practices***: The included mapping of C2M2 practices to Subcategories and Tiers shows that the C2M2 adequately addresses all the objectives of the Framework.
- ***Progressive maturity levels***: The C2M2 uses maturity indicator levels that can help an organization track measurable, incremental progression in the maturity of cybersecurity practices.
- ***Self-evaluation toolkit***: The C2M2 toolkit enables step-by-step self-evaluations using the C2M2, with macro-based scoring and reporting of results. These resources help make periodic re-evaluation and measuring progress against goals more feasible.

5.2 C2M2 Overview

The C2M2 is organized around ten *domains* that cover the range of cybersecurity and risk management practices used in the energy sector:

Table 7. C2M2 Domains and Abbreviations

Domain	Abbreviation
Asset, Change, and Configuration Management	ACM
Cybersecurity Program Management	CPM
Supply Chain and External Dependencies Management	EDM
Identity and Access Management	IAM
Event and Incident Response, Continuity of Operations	IR
Information Sharing and Communications	ISC
Risk Management	RM
Situational Awareness	SA
Threat and Vulnerability Management	TVM
Workforce Management	WM

Using the C2M2 toolkit, organizations self-evaluate their current practices within each domain. Each domain is divided into a number of objectives that support the domain. (For example, the Risk Management domain comprises three objectives: Establish Cybersecurity Risk Management Strategy, Manage Cybersecurity Risk, and Management Activities.) *Objectives* are each made up of one or more *practices* that demonstrate the organization is effectively meeting the objective, commensurate with their specific level of risk.

Each domain has one consistent objective—Management Activities—which describes the activities the organization performs to *institutionalize* the domain-specific practices throughout the organization. Institutionalization refers to the extent to which a practice or activity is ingrained into the way an organization operates.

Achieving and Demonstrating Maturity

Each domain in the C2M2 includes four maturity indicator levels (MIL), labeled as MIL0 (Not Performed) through MIL3 (Managed). Organizations progressively advance in maturity level by improving: 1) the completeness, thoroughness, or level of development of the practices in a given domain, and 2) how ingrained or institutionalized the practices are in the organization's operations and way of conducting business. Organizations achieve a MIL when they perform both the domain-specific cybersecurity objectives and practices and the Management Activities of that MIL. Organizations can establish a target MIL for each domain to guide their cybersecurity improvement.

Tiers vs. Maturity Indicator Levels (MILs)

As shown in Table 12 of Appendix A, there is some correspondence between Framework Tier characteristics and C2M2 practices of various domains and MILs. But Tiers and MILs have a different structure and purpose. Tiers "describe the degree to which an organization's cybersecurity risk management practices… [are] risk and threat aware, repeatable, and adaptive" (NIST 2014, p. 5). Tiers therefore describe the practices as a whole. C2M2 MILs independently describe the individual maturity of each domain; each domain has a set of MIL3 practices and a set of MIL2 practices, and most domains have a set of MIL1 practices. An organization could be at MIL3 in the Identity and Access Management domain, for example, and at MIL1 in the Situational Awareness domain. Organizations using the C2M2 can use the mapping in Table 12 to identify their Framework Tier and also use the MILs for domain-specific metrics.

Subsector-Specific C2M2 Variants

There are currently three variants of the C2M2. The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2; DOE 2012a) and Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2; DOE 2014b) contain guidance and examples pertinent to those subsectors. The more general Cybersecurity Capability Maturity Model (C2M2; DOE 2014a) can be used by organizations regardless of their sector.

5.3 Leveraging the C2M2 to Support Framework Implementation

This section explains how using the C2M2 addresses each of the steps in the Framework implementation approach described in Section 4. Details specific to the C2M2 are shown in ***bold and italicized***. Several of the steps refer to the *Cybersecurity Capability Maturity Model Facilitator Guide* (DOE 2014c), which can be downloaded from the DOE website, and elements of the C2M2 toolkit, which is available by request.[1]

A C2M2 self-evaluation is an integral activity in using the C2M2 to achieve the goals of the Framework. *The C2M2 Facilitator Guide* contains detailed instructions for conducting a C2M2 self-evaluation workshop and for understanding and benefitting from its results. An evaluation survey and scoring and reporting mechanisms used in the self-evaluation are provided in the C2M2 toolkit.

Step 1: Prioritize and Scope

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

Organizations begin a C2M2 self-evaluation by determining the scope—the subset of the operations of the organization that will be evaluated. Section 2.6 of the *C2M2 Facilitator Guide* provides guidance for scoping.

In the C2M2, each organizational subset that will be evaluated is referred to as a *function*. The ES-C2M2 and ONG-C2M2 each have some predefined subsector-specific functions and scoping guidance. However, the C2M2 is flexible enough to be used for whatever scope an organization chooses for Framework implementation, including systems or technology areas that cross organizational boundaries. A C2M2 *function* could be the same as *organization* as defined in Section 2.1.

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

Step 2: Orient

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

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

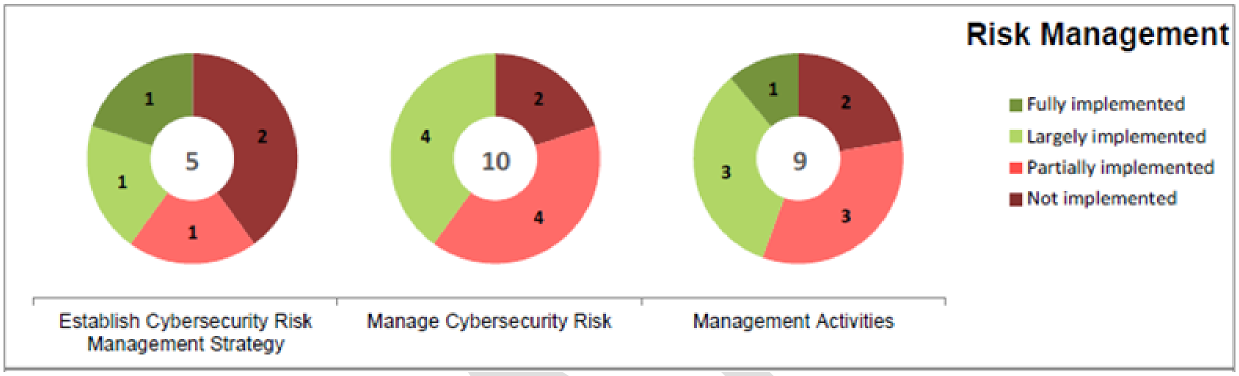
Step 3: Create a Current Profile

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

The C2M2 is typically applied through a facilitated, one-day workshop that includes key individuals representing all in-scope assets and functions. The C2M2 self-evaluation workshop results in a Scoring Report that can serve as a Current Profile. Through open dialog and consensus, survey workshop participants answer questions in the evaluation survey about practices in each domain. Responses are chosen from a four-point scale: Not Implemented, Partially Implemented, Largely Implemented, or Fully Implemented. Using the toolkit, the C2M2 Evaluation Scoring Report is generated from the survey results. The report presents results in two views: the Objective view, which shows practice question responses by each domain and its objectives, and the Domain view, which shows responses by all domains and MILs. Figure 2 gives an example of results for the Risk Management domain in the Objective view, and Figure 3 gives an example of results in the Domain view.

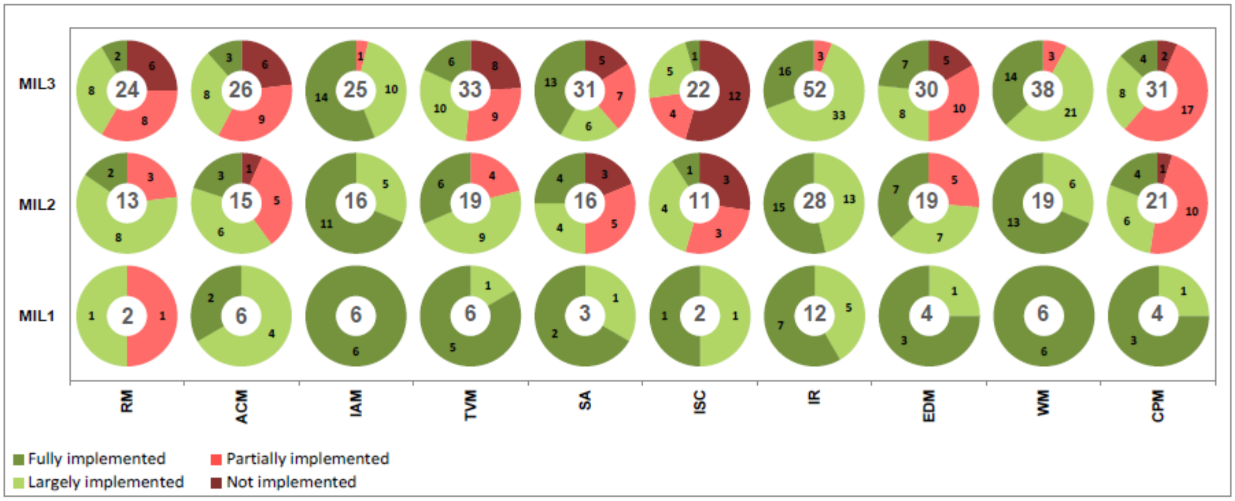
Red sectors in a doughnut chart show a count of the number of questions that received survey responses of “Not Implemented” (dark red) or “Partially Implemented” (light red). The green sectors show the number of questions that received responses of “Largely Implemented” (light green) or “Fully Implemented”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

Figure 2: Objective View Example



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

Figure 3: Domain View Example



In the Domain view, the number in the center of the doughnut indicates the cumulative number of questions that must be answered “Largely Implemented” or “Fully Implemented” to achieve that MIL for that domain. For the full list of domain names and abbreviations, see Table 7.

Step 4: Conduct a Risk Assessment

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

The C2M2 recommends that organizations use the model as part of a continuous enterprise risk management process that includes risk assessments (C2M2 2014, p. 4). Results of the risk assessment are used as input in all of the rest of the C2M2 implementation steps. Both the C2M2 and the Framework identify risk assessment as an important practice. Organizations can also look to the *Electricity Subsector Cybersecurity Risk Management Process Guideline* for additional guidance for this activity (DOE 2012b).

Step 5: Create a Target Profile

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

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

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

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

With either method, an organization can use the mapping of C2M2 practices to the Framework Core Subcategories (in Table 11 in Appendix A) and the mapping of C2M2 practices to the Tier characteristics (in Table 12 in Appendix A) to compare its Target Profile to the Framework and possibly make adjustments to its Target Profile.

For example, Company A has decided to include only MIL1 Threat and Vulnerability Management (TVM) practices in its Target Profile. Company A then highlights all its selected practices on Table 11. This reveals that no MIL1 C2M2 practices address the Framework Subcategory ID.RA-4, as shown in Table 8. Company A decides that based on its current risk management strategy, the ID.RA-4 practice (identifying potential business impacts and likelihoods of cybersecurity risks) is a priority, so it adds the MIL2 practices TVM-1d and TVM-1f to its Target Profile.

Table 8. Example C2M2 Mapping

Function	Category	Subcategory	C2M2 Practices		
			MIL1	MIL2	MIL3
IDENTIFY (ID)	**Risk Assessment (RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-4:** Potential business impacts and likelihoods are identified		TVM-1d TVM-1f	TVM-1i

Mapping of Tier Characteristics to C2M2 Practices

Framework Implementation Tiers are associated with the overall robustness of an organization’s risk management process and are not directly tied with individual Functions, Categories, or Subcategories. At face value, it may seem difficult to map Framework Tiers to C2M2 domains or practices. However, using the C2M2 practices organized by maturity level, and using the C2M2 Risk Management domain in particular, organizations can map Tier characteristics to similar C2M2 practices, as shown in Table 12 in Appendix A. Table 9 shows one mapping example from Framework Implementation Tier 3:

Table 9. C2M2 Mapping Example from Framework Implementation Tier 3

Tier Category	Characteristic	C2M2 Domain	C2M2 Practice
Risk Management Process	The organization's risk management practices are formally approved and expressed as policy.	Risk Management	Risk management activities are guided by documented policies or other organizational directives.

The C2M2 and the Table 12 mapping thus can help organizations gauge their progress against the Framework's recommended cybersecurity risk management capabilities as described in Implementation Tiers.

For example, after defining a tentative Target Profile, Company B highlights its C2M2 practices in Table 12. Company B can then see that it can achieve Implementation Tier 2, "Risk Informed," by adding two C2M2 Risk Management practices to its Target Profile: RM-3a, "Documented practices are followed for risk management activities," and RM-3b, "Stakeholders for risk management activities are identified and involved." Company B decides that, while this goal is worthwhile, its Target Profile achieves the objectives of its current risk management strategy, and so it chooses not to add the two practices to the Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps

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

The C2M2 Self-Evaluation Scoring Report enables organizations to identify gaps between the Current Profile and the Target Profile. Section 4.3.2 of the *C2M2 Facilitator Guide* [DOE 2014c] provides guidance on how to plan and prioritize the actions needed to address gaps and achieve the Target Profile. Prioritization should consider how gaps affect organizational objectives and the relative criticality of those objectives; the cost of implementing the target practices; and the availability of resources to implement the practices.

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

Step 7: Implement Action Plan

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

6. Alignment with Other Sectors

DOE and the private sector stakeholders recognize that many organizations operate in multiple critical infrastructure sectors and as a result need alignment between the guidance developed by overlapping Sector-Specific Agencies and associated cybersecurity approaches.

DOE is actively engaged with government partners from different sectors to ensure diligence with regard to cross-sector overlaps. As different sectors increase their implementation of the Framework, this guidance may be updated or supplemented to harmonize framework use across different sectors.

7. References

(DOE 2014a) U.S. Department of Energy. *Cybersecurity Capability Maturity Model*. DOE, February 2014. http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity-capability-maturity-model-c2m2

(DOE 2014b) U.S. Department of Energy. *Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model*. DOE, February 2014. http://energy.gov/oe/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-ong-c2m2

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

(DOE 2013) U.S. Department of Energy. *Integrating Electricity Subsector Failures Scenarios into a Risk Assessment Methodology*. DOE, December 2013. http://energy.gov/oe/downloads/integrating-electricity-subsector-failure-scenarios-risk-assessment-methodology

(DOE 2012a) U.S. Department of Energy. *Electricity Subsector Cybersecurity Capability Maturity Model*. DOE, May 2012. http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

(DOE 2012b) U.S. Department of Energy. *Electricity Subsector Cybersecurity Risk Management Process Guideline*. DOE, May 2012. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

(NIST 2014) National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Security*. NIST, February 2014. http://www.nist.gov/cyberframework/index.cfm

APPENDIX A: MAPPING OF C2M2 TO THE FRAMEWORK

As discussed in Section 5 of this guidance, energy sector organizations using the C2M2 may want to map their C2M2 practices to the Framework Core and Implementation Tiers to guide their decisions about Target Profiles or to demonstrate their implementation of the Framework. The following two-part mapping—with Table 11 for the Framework Core and the C2M2 practices and Table 12 for the Implementation Tiers and the C2M2 practices—provides extensive detail for organizations to use to map their practices, or to simply learn more about how the C2M2 practices meet the intent of the Framework.

The mappings in Table 11 and Table 12 collectively present a comprehensive view of how the C2M2 complements the Framework. It is possible that an organization that performs C2M2 practices mapped to a specific framework outcome may determine that some C2M2 practices do not satisfy the outcome to a degree required by that organization. Organizations utilizing this mapping should therefore review it and ensure that it aligns with their needs.

C2M2 practices are denoted by the domain abbreviation, a hyphen, the objective number, and the practice letter. For example, “ACM-1a” denotes practice A in Objective 1 of the Asset, Change, and Configuration Management domain. The domain abbreviations are listed in Table 10.

Table 10: **C2M2 Domains and Abbreviations**

Domain	Abbreviation
Asset, Change, and Configuration Management	ACM
Cybersecurity Program Management	CPM
Supply Chain and External Dependencies Management	EDM
Identity and Access Management	IAM
Event and Incident Response, Continuity of Operations	IR
Information Sharing and Communications	ISC
Risk Management	RM
Situational Awareness	SA
Threat and Vulnerability Management	TVM
Workforce Management	WM

Table 11: C2M2 Practices Mapped to the Framework Core

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	**MIL 2**	**MIL3**
IDENTIFY (ID)	**Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	ACM-1a	ACM-1c	ACM-1e ACM-1f
		ID.AM-2: Software platforms and applications within the organization are inventoried	ACM-1b	ACM-1c	ACM-1e ACM-1f
		ID.AM-3: Organizational communication and data flows are mapped		RM-2g	ACM-1e
		ID.AM-4: External information systems are catalogued	EDM-1a	EDM-1c EDM-1e	EDM-1g RM-1c
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	ACM-1a ACM-1b	ACM-1c ACM-1d	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	WM-1a WM-1b	WM-1c	

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
IDENTIFY (ID)	**Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	EDM-1b	EDM-1d	EDM-1f EDM-1g RM-1c
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	EDM-1b	EDM-1d CPM-1c	EDM-1f EDM-1g RM-1c
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated		RM-3b	RM-1c
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	ACM-1a ACM-1b EDM-1a	ACM-1c ACM-1d EDM-1c EDM-1e	ACM-1e ACM-1f RM-1c EDM-1g
		ID.BE-5: Resilience requirements to support delivery of critical services are established	IR-4ª IR-4b IR-4c	IR-4e	
	Governance (GV): The policies, procedures, and processes to manage and monitor	**ID.GV-1:** Organizational information security policy is established	RM-1a	CPM-2g	CPM-5d RM-3e

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
	the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	WM-1a WM-1b	WM-1c WM-5b ISC-2b	WM-1f WM-1g
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed			CPM-2k IR-3n RM-3f ACM-4f IAM-3f TVM-3f SA-4f ISC-2f IR-5f EDM-3f WM-5f
		ID.GV-4: Governance and risk management processes address cybersecurity risks	RM-2a RM-2b	RM-3b	RM-2h RM-3e RM-1c RM-1e
IDENTIFY (ID)	**Risk Assessment (RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	TVM-2a TVM-2b TVM-2c	TVM-2d TVM-2e TVM-2f	RM-1c RM-2j TVM-2i TVM-2j TVM-2k TVM-2l TVM-2m
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	TVM-1a TVM-1b TVM-2a TVM-2b		

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
		ID.RA-3: Threats, both internal and external, are identified and documented	TVM-1a TVM-1b	TVM-1d TVM-1e TVM-1f	RM-1c RM-2j TVM-1j TVM-1i
		ID.RA-4: Potential business impacts and likelihoods are identified		TVM-1d TVM-1f	TVM-1i
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk			RM-1c RM-2j TVM-1i TVM-2l TVM-2m
		ID.RA-6: Risk responses are identified and prioritized		RM-2e	RM-1c RM-2j TVM-1i TVM-2l IR-3m IR-4d IR-4e
	Risk Management Strategy (RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	RM-2a RM-2b	RM-1a RM-1b RM-2c RM-2d RM-2e RM-2f RM-2g RM-3a RM-3b RM-3c RM-3d	RM-1c RM-1d RM-1e RM-2h RM-2i RM-2j RM-3e RM-3f RM-3g RM-3h RM-3i
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed			RM-1c RM-1e

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
IDENTIFY (ID)		**ID.RM-3**: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis		RM-1b	RM-1c
PROTECT (PR)	**Access Control (AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	IAM-1a IAM-1b IAM-1c	IAM-1d IAM-1e IAM-1f	RM-1c IAM-1g
		PR.AC-2: Physical access to assets is managed and protected	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g
		PR.AC-3: Remote access is managed	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties		IAM-2d	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	CPM-3a	CPM-3b CPM-3c	CPM-3d

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
PROTECT (PR)	**Awareness and Training (AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	WM-3a	WM-3b WM-3c WM-3d	WM-3e WM-3f WM-3g WM-3h WM-3i
		PR.AT-2: Privileged users understand roles & responsibilities	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
		PR.AT-4: Senior executives understand roles & responsibilities	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	WM-1a WM-1b	WM-1c WM-1d	WM-1e WM-1f WM-1g
	Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	ACM-1b TVM-1c TVM-2c	CPM-3b	ACM-1e TVM-2i TVM-2n
		PR.DS-2: Data-in-transit is protected	ACM-1b TVM-1c TVM-2c	CPM-3b	ACM-1e TVM-2i TVM-2n

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
PROTECT (PR)		**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition	ACM-1a ACM-1b ACM-2a ACM-2b ACM-3a ACM-3b	ACM-1c ACM-1d ACM-2c ACM-3c ACM-3d ACM-4a ACM-4b ACM-4c ACM-4d	ACM-1e ACM-1f ACM-2d ACM-2e ACM-3e ACM-3f ACM-4e ACM-4f ACM-4g ACM-4h ACM-4i
		PR.DS-4: Adequate capacity to ensure availability is maintained	TVM-1c TVM-2c	CPM-3b	TVM-2i TVM-2n
		PR.DS-5: Protections against data leaks are implemented	TVM-1c TVM-2c	CPM-3b	TVM-2i TVM-2n
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity		ACM-3d	
		PR.DS-7: The development and testing environment(s) are separate from the production environment		ACM-3c	ACM-3e

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	**MIL 2**	**MIL3**
PROTECT (PR)	**Information Protection Processes and Procedures (IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	ACM-2a ACM-2b	ACM-2c	ACM-2d ACM-2e
		PR.IP-2: A System Development Life Cycle to manage systems is implemented		ACM-3d	
		PR.IP-3: Configuration change control processes are in place	ACM-3a ACM-3b	ACM-3c ACM-3d	ACM-3e ACM-3f
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	IR-4a IR-4b IR-4c	IR-4f	IR-4g IR-4j
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	RM-2b IAM-2a		RM-3f IAM-3f
		PR.IP-6: Data is destroyed according to policy		ACM-3d	
		PR.IP-7: Protection processes are continuously improved		TVM-1h	CPM-1g

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	ISC 1a ISC-1b	ISC-1c ISC-1d ISC-1e ISC-1f ISC-1g ISC-2b	ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	IR-4c	IR-3e IR-3f IR-4d IR-4f IR-5a IR-5b IR-5c IR-5d RM-1a RM-1b TVM-1d	IR-3k IR-3m IR-4i IR-4j IR-5e IR-5f IR-5g IR-5h IR-5i RM-1c
		PR.IP-10: Response and recovery plans are tested		IR-3e IR-4f	IR-3k IR-4i IR-4j
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	WM-2a WM-2b	WM-2c WM-2d	WM-2e WM-2f WM-2g WM-2h
PROTECT (PR)		**PR.IP-12:** A vulnerability management plan is developed and implemented		TVM-2d TVM-2e	TVM-3e TVM-3f
	Maintenance (MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	IAM-2a	ACM-1c	ACM-3f

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
	procedures.	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	SA-1a IR-1c IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g IAM-2h IAM-2i
	Protective Technology (PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	SA-1a SA-2a	SA-1b SA-1c SA-2e SA-4a	SA-1d SA-1e SA-3d SA-4e
		PR.PT-2: Removable media is protected and its use restricted according to policy	IAM-2a IAM-2b TVM-1c	IAM-2c	IAM-2e IAM-3f TVM-1i
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g IAM-2h IAM-2i
		PR.PT-4: Communications and control networks are protected	CPM-3a	CPM-3b CPM-3c	CPM-3d
DETECT (DE)	**Anomalies and Events (AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	SA-2b	SA-2e	

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
		DE.AE-2: Detected events are analyzed to understand attack targets and methods			IR-2i IR-3h
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors		IR-1e	IR-1f IR-2i
		DE.AE-4: Impact of events is determined	IR-2b	IR-2d	IR-2g
		DE.AE-5: Incident alert thresholds are established		IR-2d TVM-1d SA-2d	IR-2g RM-2j
	Security Continuous Monitoring (CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	SA-2a SA-2b	SA-2e SA-2f	SA-2g SA-2i
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	SA-2a SA-2b		SA-2i
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	SA-2a SA-2b		SA-2i
		DE.CM-4: Malicious code is detected	SA-2a SA-2b	SA-2e CPM-4a	SA-2i
		DE.CM-5: Unauthorized mobile code is detected	SA-2a SA-2b	SA-2e	SA-2h SA-2i
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	EDM-2a SA-2a SA-2b		EDM-2j EDM-2l EDM-2n

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
DETECT (DE)		**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	SA-2a SA-2b	SA-2e SA-2f	SA-2g SA-2i
		DE.CM-8: Vulnerability scans are performed		TVM-2e	TVM-2i
	Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	IR-1a IR-3a WM-1a WM-1b	WM-1d	WM-1f WM-2h
		DE.DP-2: Detection activities comply with all applicable requirements		IR-1d	IR-1g IR-5f RM-1c RM-2j
		DE.DP-3: Detection processes are tested		IR-3e	IR-3j
		DE.DP-4: Event detection information is communicated to appropriate parties	IR-1b IR-3c ISC-1a	ISC-1c ISC-1d	IR-3n ISC-1h
		DE.DP-5: Detection processes are continuously improved		IR-3h	IR-3k
RESPOND (RS)	**Response Planning (RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event		IR-3d	

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
RESPOND (RS)	**Communications (CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	IR-3a		IR-5a IR-5b
		RS.CO-2: Events are reported consistent with established criteria	IR-1a IR-1b		
		RS.CO-3: Information is shared consistent with response plans	ISC-1a ISC-1b	IR-3d ISC-1c ISC-1d	
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans		IR-3d IR-5b	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	ISC-1a ISC-1b IR-3c	ISC-1c ISC-1d ISC-1e ISC-1f	ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l
	Analysis (AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated		IR-1e SA-3a	IR-1f IR-1h
		RS.AN-2: The impact of the incident is understood	IR-2d IR-2g	IR-2d TVM-1d	IR-2g RM-2j
		RS.AN-3: Forensics are performed		IR-3d	IR-3i
		RS.AN-4: Incidents are categorized consistent with response plans	IR-2a	IR-1d IR-1e IR-2d TVM-1d	IR-2g RM-1c
	Mitigation (MI): Activities are performed to prevent expansion of an event, mitigate its	**RS.MI-1:** Incidents are contained	IR-3b		
		RS.MI-2: Incidents are mitigated	IR-3b		

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
	effects, and eradicate the incident.	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	TVM-2c	TVM-2f TVM-2g	RM-2j TVM-2m TVM-2n
	Improvements (IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned			IR-3h
		RS.IM-2: Response strategies are updated	IR-3e		IR-3k
RECOVER (RC)	**Recovery Planning (RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	IR-3b		IR-3o IR-4k
	Improvements (IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned			IR-3h IR-4i IR-3k
		RC.IM-2: Recovery strategies are updated			IR-3h IR-3k
	Communications (CO): Restoration activities are coordinated with internal and external	**RC.CO-1:** Public relations are managed		TVM-1d IR-4d	RM-1c
		RC.CO-2: Reputation after an event is repaired		IR-4d	

Function	Category	Subcategory	C2M2 Practices		
			MIL 1	MIL 2	MIL3
	parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams		IR-3d	IR-5e

Table 12. C2M2 Practices Mapped to NIST Framework Tiers

Table 12 maps the Framework Implementation Tiers and the C2M2 practices. This mapping is cumulative, i.e., the practices mapped to a Tier 1 Category are required for Tier 2 as well. This means an organization striving for Tier 3 should consider practices listed under Tier 1, 2, and 3 headings in Table 12. Moreover, the framework describes some Tier Categories as the absence and/or ad hoc performance of a risk management practice. In such cases, the C2M2 practice mapped for ad hoc performance is marked with an asterisk. By design, the C2M2 recognizes MIL 1 practices as initial security and risk management activities that organizations may perform in an ad hoc manner.

It is possible that an organization that performs C2M2 practices mapped to a specific Framework Tier may determine that some C2M2 practices do not satisfy the Tier characteristics to a degree required by that organization. Organizations utilizing this mapping should therefore review it and ensure that it aligns with their needs.

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
Tier 1: Partial	Risk Management Process	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.	RM-2a* RM-2b*		
		Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	RM-2a* RM-2b*		
	Integrated Risk Management Program	There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a* RM-2b*		
		The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.	RM-2a* RM-2b*		
		The organization may not have processes that enable cybersecurity information to be shared within the organization.	RM-2a* RM-2b*		

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
	External Participation	An organization may not have the processes in place to participate in coordination or collaboration with other entities.	RM-2a* RM-2b*		

*As described in the Framework, these Tier characteristics correspond to the specified C2M2 practices performed in an ad hoc manner.

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
Tier 2: **Risk Informed**	Risk Management Process	Risk management practices are approved by management but may not be established as organizational-wide policy.		RM-3a* RM-3b*	
		Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.			RM-1c
	Integrated Risk Management Program	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a RM-2b		
		Risk informed, management -approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.	CPM-2a CPM-2b	RM-3a RM-3b RM-3c	RM-1c
		Cybersecurity information is shared within the organization on an informational basis.	ISC-1a		
	External Participation	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.	EDM-1a EDM-1b	ISC-1c	

*As described in the Framework, these Tier characteristics correspond to the specified C2M2 practices performed in an ad hoc manner.

Framework Implementation Tier	**Tier Category**	**Characteristics**	**C2M2 Reference**		
			MIL 1	MIL 2	MIL3
Tier 3: Repeatable	Risk Management Process	The organization's risk management practices are formally approved and expressed as policy.			RM-3e
		Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.			RM-1d CPM-1g
	Integrated Risk Management Program	There is an organization-wide approach to manage cybersecurity risk.	CPM-1a	RM-1a RM-1b	
		Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.			RM-3e RM-3g CPM-2i CPM-3d
		Personnel possess the knowledge and skills to perform their appointed roles and responsibilities		WM-3b WM-3c WM-3d	RM-3i ACM-4i IAM-3i TVM-3i SA-4i ISC-2i IR-5i EDM-3i WM-5i CPM-5f

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
	External Participation	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.	EDM-2a	ISC-1d	

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
Tier 4: Adaptive	Risk Management Process	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.		RM-2j TVM-1j TVM-2m	RM-1d
		Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.			RM-1g CPM-1g
	Integrated Risk Management Program	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.		TVM-1d	RM-2h RM-3e IAM-1g TVM-1i TVM-2j TVM-2l IR-3m IR-4h EDM-1g EDM-2k
		Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.			SA-3d SA-3e

Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
Tier 4: Adaptive	External Participation	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.			ISC-1h ISC-1i ISC-1j ISC-1k ISC-1l

APPENDIX B: SUMMARY OF FRAMEWORK USE STEPS

Table 13. Summary of Framework Use Steps

Step 1: Prioritize and Scope		
Inputs	**Activities**	**Outputs**
1. Risk management strategy 2. Organizational objectives and priorities 3. Threat information	1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cybersecurity capabilities	1. Framework usage scope
Step 2: Orient		
Inputs	**Activities**	**Outputs**
1. Framework usage scope 2. Risk management strategy	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and informative references (e.g., cybersecurity and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (i.e., regulatory, company, organizational) 3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines 4. Evaluation approach
Step 3: Create a Current Profile		
Inputs	**Activities**	**Outputs**
1. Evaluation approach 2. In-scope systems and assets 3. In-scope regulatory requirements 4. In-scope cybersecurity and risk management standards, tools, methods, and guidelines	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile 2. Current Implementation Tier
Step 4: Conduct a Risk Assessment		
Inputs	**Activities**	**Outputs**
1. Framework usage scope 2. Risk management strategy	1. Perform risk assessment for in-scope portion of the organization	1. Risk assessment reports

3. Organization-defined risk assessment approach 4. In-scope regulatory requirements 5. In-scope cybersecurity and risk management standards, tools, methods, and guidelines		
Step 5: Create a Target Profile		
Inputs	**Activities**	**Outputs**
1. Current Profile 2. Current Tier 3. Organizational objectives 4. Risk management strategy 5. Risk assessment reports	1. Organization identifies goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives	1. Target Profile 2. Target Tier
Step 6: Determine, Analyze, and Prioritize Gaps		
Inputs	**Activities**	**Outputs**
1. Current Profile 2. Current Tier 3. Target Profile 4. Target Tier 5. Organizational objectives 6. Impact to critical infrastructure 7. Gaps and potential consequences 8. Organizational constraints 9. Risk management strategy 10. Risk assessment reports	1. Analyze gaps between current state and Target Profile in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) on actions 6. Prioritize actions (CBA and consequences) 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan
Step 7: Implement Action Plan		
Inputs	**Activities**	**Outputs**
1. Prioritized implementation plan	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks, metrics, and performance indicators 4. Report progress	1. Project tracking data 2. New security measures implemented