ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0

31 May 2012

TABLE OF CONTENTS

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was developed in support of a White House initiative led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), and in collaboration with industry, private-sector, and public-sector experts. The model was developed collaboratively with an industry advisory group through a series of working sessions and revised based on feedback from industry experts and pilot evaluations. The advisory group for the initiative included representatives from industry associations, utilities, and government. Additionally, more than 40 subject matter experts (SMEs) from industry participated in development of the model.

The following documents served as foundational references for the model development team:

- *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, DOE
- *Cross-Sector Roadmap for Cybersecurity of Control Systems*, DHS Industrial Control Systems Joint Working Group (ICSJWG)
- *Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*, DOE
- *The CERT® Resilience Management Model (CERT®-RMM)*, Software Engineering Institute
- *NERC Cyber Risk Preparedness Assessment (CRPA): Improving the Cyber Security Posture of the North American Bulk Power System*, North American Electric Reliability Corporation (NERC)
- *NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security*, National Institute of Standards and Technology (NIST)
- *Cyber Attack Task Force (CATF) Final Report*, North American Electric Reliability Corporation (NERC)

The NERC Critical Infrastructure Protection (CIP) cybersecurity standards provide specific requirements that apply to the bulk power system, and were used as a reference by the model development team. While it is anticipated that entities subject to compliance with NERC CIP standards would use this model, compliance requirements are not altered in any way by this model. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

The DOE wishes to acknowledge and thank the senior leaders from the White House, DOE, DHS, and utility executives for their support, along with the members of the advisory group, model development team, subject matter expert teams, and pilot utilities who participated in the development of this model.

Initiative Lead

Samara Moore
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Model Architect

David W. White
Carnegie Mellon University Software Engineering Institute - CERT Program

Advisory Group

Mike Assante
National Board of Information Security Examiners (NBISE)

David Batz
Edison Electric Institute (EEI)

Gary Bell
Southern California Edison (SCE)

Jim Brenton
Electric Reliability Council of Texas (ERCOT)

Seth Bromberger
National Electric Sector Cybersecurity Organization (NESCO)

Larry Buttress
Bonneville Power Administration (BPA)

Kevin Dillon
Department of Homeland Security (DHS)

Rhonda Dunfee
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Mark Engels
Dominion Resources Services

Lisa Kaiser
Department of Homeland Security (DHS)

Akhlesh Kaushiva
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Henry Kenchington
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Carlos Kizzee
Department of Homeland Security (DHS)

David Kuipers
Idaho National Laboratory (INL)

Barry Lawson
National Rural Electric Cooperative Association (NRECA)

Annabelle Lee
Electric Power Research Institute (EPRI), representing NESCOR

Suzanne Lemieux
BCS Incorporated (Contract support of DOE-OE)

Craig Miller
National Rural Electric Cooperative Association (NRECA)

Nathan Mitchell
American Public Power Association (APPA)

Samara Moore
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Tim Roxey
North American Electric Reliability Corporation, Electricity Sector Information Sharing and Analysis Center (NERC ES-ISAC)

James W. Sample
Pacific Gas & Electric Company (PG&E)

Sean Sherman
Arctic Slope Regional Corporation (Contract support of DOE-OE)

Gal Shpantzer
National Electric Sector Cybersecurity Organization (NESCO)

Paul Skare
Pacific Northwest National Laboratory (PNNL)

James Stevens
Carnegie Mellon University Software Engineering Institute - CERT Program

Kevin Stogran
American Electric Power (AEP)

Marianne Swanson
National Institute of Standards and Technology (NIST)

David W. White
Carnegie Mellon University Software Engineering Institute - CERT Program

Model Development Team

Matthew Butkovic
Carnegie Mellon University Software Engineering Institute - CERT Program

John Fry
ICF International (Contract Support of DOE-OE)

Matthew Light
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Howard Lipson, PhD
Carnegie Mellon University Software Engineering Institute - CERT Program

Samuel A. Merrell
Carnegie Mellon University Software Engineering Institute - CERT Program

Samara Moore
Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)

Fowad Muneer
ICF International (Contract Support of DOE-OE)

Paul Ruggiero
Carnegie Mellon University Software Engineering Institute - CERT Program

Anthony David Scott
Accenture (Contract Support of DOE-OE)

Sean Sherman
Arctic Slope Regional Corporation (Contract support of DOE-OE)

Paul Skare
Pacific Northwest National Laboratory (PNNL)

James Stevens
Carnegie Mellon University Software Engineering Institute - CERT Program

Barbara Tyson, PhD
Carnegie Mellon University Software Engineering Institute - CERT Program

David W. White
Carnegie Mellon University Software Engineering Institute - CERT Program

Initiative Working Session Facilitation Team

Jack Eisenhauer
Nexight Group (Contract Support of DOE-OE)

Lindsay Kishter
Nexight Group (Contract Support of DOE-OE)

Subject Matter Expert Team

Andy Bochman
IBM

Rich Caralli
Carnegie Mellon University Software Engineering Institute - CERT Program

Dr. Les Cardwell
Central Lincoln PUD

Douglas M. DePeppe
Information Security & Center for Information Age Transformation

Tim Dierking
Aclara

Ed Goff
Progress Energy Service Company

Baiba Grazdina
Duke Energy

Neil Greenfield
American Electric Power (AEP)

Casey Groves
Department of Defense (DOD)

David Hallquist
Vermont Electric Cooperative

Donny Helm
Oncor

Darren Reece Highfill
UtiliSec

Fred Hintermister
North American Electric Reliability Corporation, Electricity Sector Information Sharing and Analysis Center (NERC ES-ISAC)

Dennis Holstein
Opus Consulting Group

Charles Hunt
SGIP - CSWG

William Keagle
Baltimore Gas and Electric (BGE)

Justin Kelly
Federal Energy Regulatory Commission (FERC)

Heath Knakmuhs
UL LLC

Barry Kuehnle
Federal Energy Regulatory Commission (FERC)

Alex Kunz
Sempra Energy

Steven Latham
South Plains Electric Coop

Jeff Lowder
Society of Information Risk Analysts

Trevor MacCrae

Clifford Maraschino
Southern California Edison (SCE)

Ken Modeste
UL Communications

Paul Mohler
Law Offices of Paul Mohler

Donald Morris
Centerpoint Energy

Bruce Oliver
Sacramento Municipal Utility District (SMUD)

Ward Pyles

Austin Rappeport
Federal Energy Regulatory Commission (FERC)

Evelyn Remaley Hasch
Department of Defense (DOD)

Scott Saunders
Sacramento Municipal Utility District (SMUD)

Daniel Taft
Consolidated Edison (ConEd)

Dr. David H. Tobey
National Board of Information Security Examiners

Ben Tomhave
Lock Path

Victoria Yan Pillitteri
Booz Allen Hamilton

Daniel Yagudayev
Consolidated Edison (ConEd)

CAUTIONARY NOTE
Intended Scope and Use of This Publication

The guidance provided in this publication is intended to address *only* the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology (i.e., energy delivery systems) and/or with the environments in which they operate. The guidance is *not* intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that electricity subsector organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulation, policies, programmatic initiatives, or mission and business requirements. Additionally, this guidance is not part of any regulatory framework and is not intended for regulatory use. Rather, the guidance in this publication is intended to complement a comprehensive enterprise cybersecurity program.

1. INTRODUCTION

This document describes the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The goal of this model is to support ongoing development and measurement of cybersecurity capabilities within the electricity subsector through the following four objectives:

- Strengthen cybersecurity capabilities in the electricity subsector.
- Enable utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities.
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities.
- Enable utilities to prioritize actions and investments to improve cybersecurity.

The model was developed to apply to all electric utilities, regardless of ownership structure, size, or function. Broad use of the model is expected to support benchmarking for the subsector's cybersecurity capabilities.

Section 2 of this document presents background information on the model and its development. Section 3 gives an overview of the U.S. electricity subsector. Section 4 contains the model itself. It begins by describing the model's development and architecture, and then it presents the model's objectives and practices, organized into 10 domains. Section 5 recommends an approach for using the model. Appendix A lists the references used for the glossary definitions, the domains, and the document in general. Appendix B gives an annotated bibliography that describes the key resources for each domain of the model. Appendix C is a glossary that defines many of the terms used in this document. Appendix D defines the acronyms used in this document. Appendix E describes related initiatives.

2. BACKGROUND

The model was developed in support of the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, a White House initiative led by the Department of Energy (DOE) in partnership with the Department of Homeland Security (DHS) and in collaboration with representatives of asset owners and operators within the electricity subsector. The initiative used the National Infrastructure Protection Plan framework as a public-private partnership mechanism to support the development of the model.

The initiative leveraged and built upon existing efforts, models, and cybersecurity best practices and is aligned with strategies contained in the White House's 2010 *Cyberspace Policy Review,* the DOE's *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, the *Energy Sector-Specific Plan*, and the Industrial Control Systems Joint Working Group's *Cross-Sector Roadmap for Cybersecurity of Control Systems*.

A team of representatives from the public and private sectors developed the model in collaboration with experts from the Carnegie Mellon Software Engineering Institute (SEI).

3. ABOUT THE ELECTRICITY SUBSECTOR

The electricity portion of the energy sector includes the generation, transmission, distribution, and marketing of electricity. The use of electricity is ubiquitous, spanning all sectors of the U.S. economy. The electric power subsector accounts for 40 percent of all energy consumed in the United States. Electricity system facilities are dispersed throughout the North American continent. Although most assets are privately owned, no single organization represents the interests of the entire subsector. An energy delivery system abstract topology of the electric grid showing the power system (primary equipment) against the energy delivery system is shown in Figure 1. This architecture was developed with cooperation between the National Institute of Standards and Technology (NIST) Smart Grid Interoperability Panel (SGIP) GridWise Architecture Council (GWAC); the European Union (EU) M/490 Reference Architecture Working Group (RAWG); and the International Electrotechnical Commission (IEC) Technical Committee 57, Working Group 19.

The Federal Government will continue to facilitate the development of rigorous, open standards and guidelines for cybersecurity through public private cooperation.

— A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future, pg. 5

Goal 2: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resilience.

— Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010, pg. 2

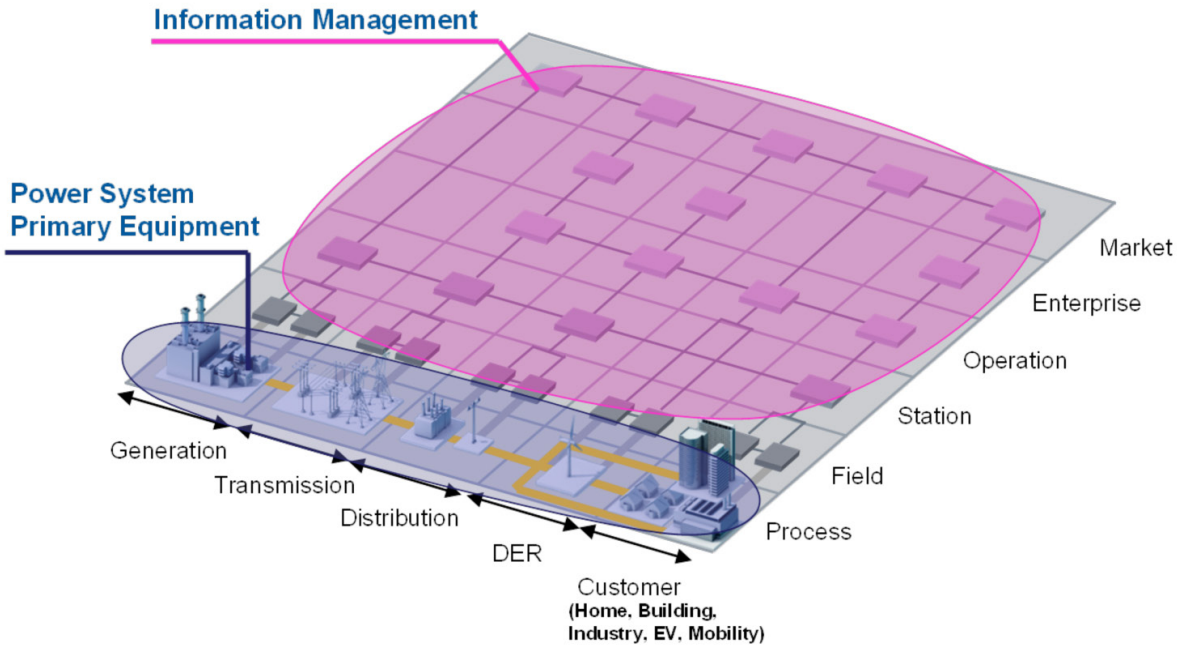


Figure 1: Electric Grid Energy Delivery System Abstract Topology

Throughout the model, "function" is used to describe the set of activities performed by the utility to which the model is being applied. For the purpose of applying this model to the electricity subsector, the advisory group focused on four high-level functions performed by electric utilities: generation, transmission, distribution, and markets. However, the model can be applied to other functions or subfunctions performed by the organization. An alternate depiction of the relationship of the functions is provided in Figure 2.

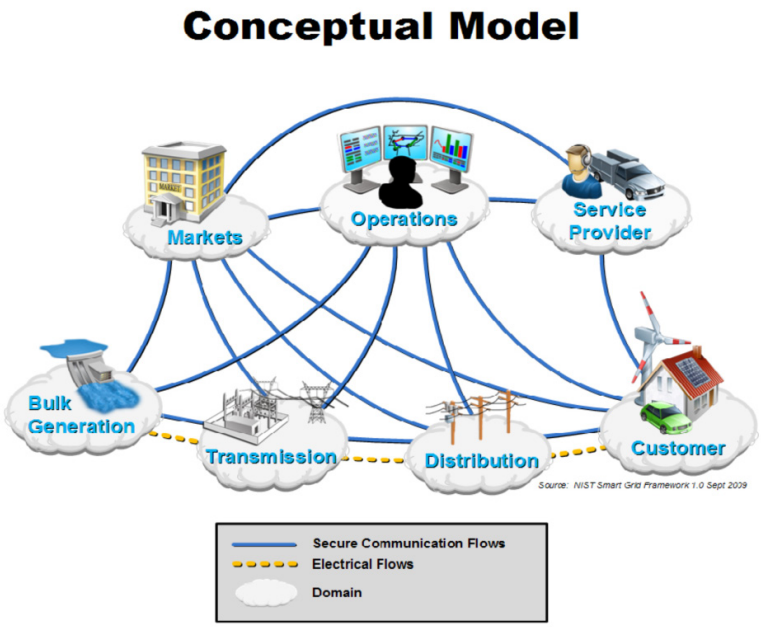


Figure 2: NIST Smart Grid Conceptual Model [NIST Framework]

4. THE MODEL

4.1 Model Development Approach

This initial version of the model was developed from January through May 2012. The following themes characterize the overall approach to the development effort:

- **Public-private partnership**
  Numerous government, industry, and academic organizations participated in the development of the model, bringing a broad range of knowledge, skills, and experience to the team. The model was developed collaboratively with an industry advisory group through a series of working sessions, and it was revised based on feedback from more than 40 industry experts and 17 pilot evaluations at utilities.
- **Leveraging of related works and initiatives**
  The model builds upon and ties together a number of existing cybersecurity resources and initiatives and was informed by a review of cyber threats to the subsector. Leveraging related works shortened the development schedule and helped to ensure that the model would be relevant and beneficial to the subsector.
- **Descriptive, not prescriptive**
  The model was developed to provide descriptive, not prescriptive, guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be at a high level of abstraction so that they can be interpreted for utilities of various structures, functions, and sizes.
- **Pilot to test, validate, and improve**
  The draft model was piloted at 17 utilities to validate that it would provide valuable feedback as a basis for evaluation and to collect feedback for improvement.
- **Fast-paced development**
  The development effort focused on quickly developing a model that would provide value to the subsector and be available as soon as possible. As this initial version is used, feedback will be collected to improve future versions of the model.

Future versions of the model are planned and will include enhancements such as the following items:

- **Additional MILs**
  One or more additional maturity indicator levels (MILs; additional MILs currently reserved as MILX) will be populated with practices that reflect more advanced approaches and more mature institutionalization than are reflected in MIL3 in this version of the model.
- **Performance metrics and measurement**
  Guidance on developing a cybersecurity performance metrics and measurement program will be added to the model.
- **Additional informative materials**
  Informative material will be added to the domains to provide additional guidance and examples for how an organization can implement the domain practices.

4.2 Model Architecture

The model is organized into 10 domains and 4 maturity indicator levels (MILs). Figure 3 presents the basic structure of the model as a matrix, with domains as columns and MILs as rows.

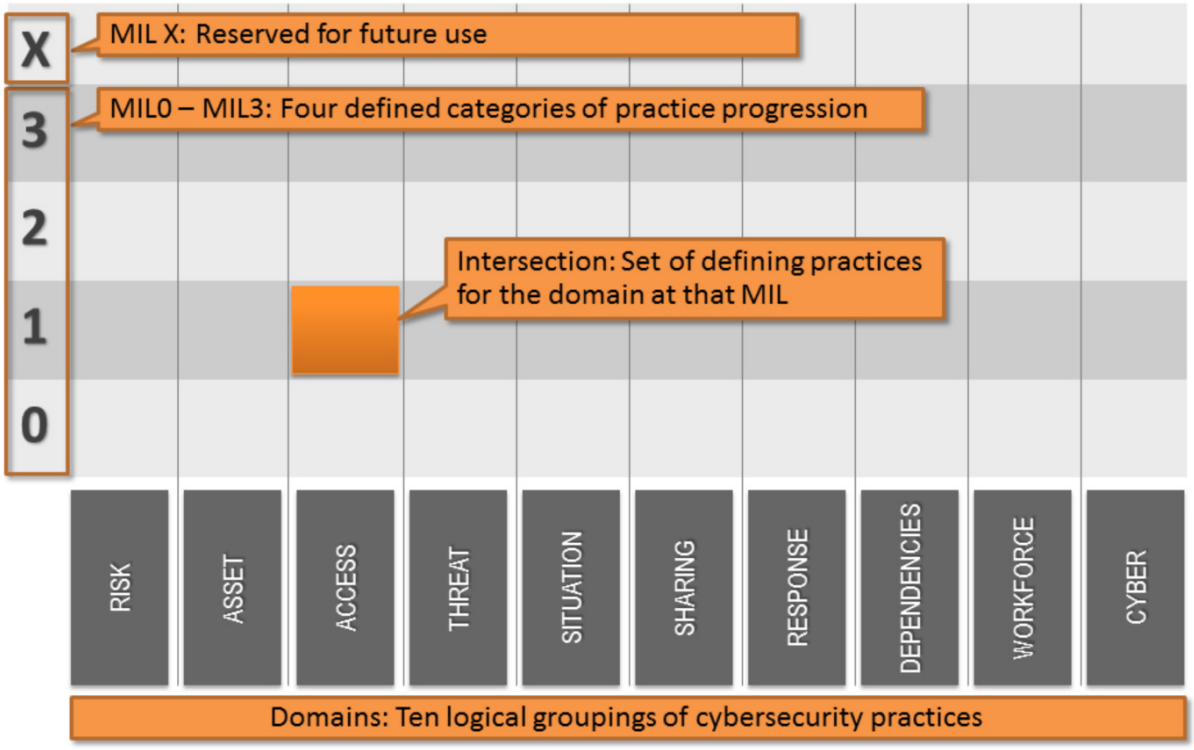


Figure 3: Structure of Model

Each domain is a logical grouping of cybersecurity practices. A domain's practices are organized by MIL to define the progression of capability maturity for the domain. As shown in Figure 3, the intersection of each domain and MIL contains a set of practices that define the domain for that MIL.

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

4.2.1 Domains

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

Each domain has a full name, such as "Risk Management," and a short name in all caps, such as "RISK." For each domain, the model provides a purpose statement, which is a high-level summary of the practices in the domain. Introductory notes follow, which give context for the domain and introduce its practices.

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

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

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. Figure 4 summarizes the elements of each domain.

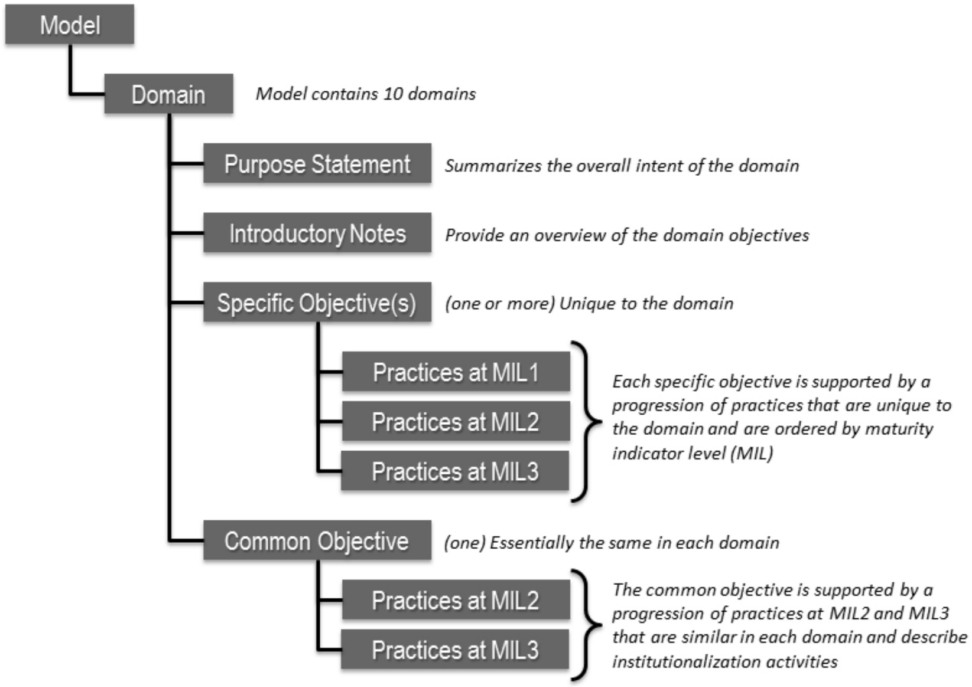


Figure 4: Model and Domain Elements

The 10 domains are listed below in the order in which they appear in the model. The list provides a brief description and the objectives for each domain.

Risk Management (RISK)

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

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

Asset, Change, and Configuration Management (ASSET)

Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives. ASSET comprises four objectives:

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

Identity and Access Management (ACCESS)

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

1. Establish and Maintain Identities
2. Control Access
3. Manage ACCESS Activities

Threat and Vulnerability Management (THREAT)

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

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

Situational Awareness (SITUATION)

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

1. Perform Logging
2. Monitor the Function
3. Establish and Maintain a Common Operating Picture
4. Manage SITUATION Activities

Information Sharing and Communications (SHARING)

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

1. Share Cybersecurity Information
2. Manage SHARING Activities

Event and Incident Response, Continuity of Operations (RESPONSE)

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

1. Detect Cybersecurity Events
2. Escalate Cybersecurity Events
3. Respond to Escalated Cybersecurity Events
4. Plan for Continuity
5. Manage RESPONSE Activities

Supply Chain and External Dependencies Management (DEPENDENCIES)

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

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

Workforce Management (WORKFORCE)

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

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

Cybersecurity Program Management (CYBER)

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

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

The model's domains are drawn from or informed by numerous reference sources, including the following:

- Threat data (e.g., DOE and DHS threat briefings, NERC *Cyber Attack Task Force Final Report*)
- Sector standards and guidance (e.g., ICSJWG *Cross-Sector Roadmap, NISTIR 7628, International Society for Automation (ISA) 99*, NESCOR failure scenarios and analyses, DHS Cyber Resilience Review, *NERC Cyber Risk Preparedness Assessment* [CRPA])
- Related maturity models (e.g., *CERT®-Resilience Management Model (CERT®-RMM),* NESCO's *Security Logging in the Utility Sector: Roadmap to Improved Maturity)*

4.2.2 Maturity Indicator Levels

The model defines four MILs, MIL0 through MIL3, that apply across all the domains, and it holds a fifth MIL, MILX, in reserve for use in future versions of the model. Each of the four defined MILs is further designated by a name, for example, "MIL3: Managed."

MIL0 through MIL3 define the maturity progression in the model. Each MIL describes the approach and institutionalization of the practices in a domain at that MIL. Three aspects of the MILs are important for understanding and correctly applying the model:

- **The maturity indicator levels apply independently to each domain.** As a result, an organization using the model may receive different MIL ratings for different domains. For example, an organization could be functioning at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
- **The MILs are cumulative within each domain; to earn a MIL in a given domain, an organization must perform all of the practices in that level and its predecessor level(s).** For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
- **Striving to achieve the highest MIL in all domains may not be optimal for all organizations.** Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy. It is recommended that organizations familiarize themselves with the practices in the model and then determine target levels of MIL achievement per domain. Gap analysis activities and improvement efforts should then focus on achieving those target levels.

The MILs define a dual progression of maturity: an institutionalization progression and an approach progression, as explained in the following sections.

4.2.2.1 Institutionalization Progression

Institutionalization describes the extent to which a practice or activity is ingrained into an organization's operations. The more deeply ingrained an activity, the more likely it is that the organization will continue to perform the activity over time.

The progression of institutionalization is described at the highest level by a set of common practices that that can be performed to institutionalize the domain-specific practices. The progression of the practices within a domain objective corresponds to the progression of the common practices, though not necessarily practice-to-practice. Table 1 shows an example mapping of the common practices to the practices in the second objective of the RISK domain:

Table 1: Mapping of Common Practices to Domain-Specific Practices, Example: RISK domain

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

The common practices are listed and summarized in the description of each MIL in the sections below.

MIL0: Incomplete

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

MIL1: Initiated

In each domain, MIL1 contains a set of initial practices. To achieve MIL1, these initial activities may be performed in an ad hoc manner, but they must be performed. If an organization were to start with no capability in managing cybersecurity, it should focus initially on implementing the MIL1 practices.

MIL1 is characterized by a single common practice:

1. **Initial practices are performed but may be ad hoc.** In the context of this model, *ad hoc* (i.e., an ad-hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training.

   Depending on who performs the practice, when it is performed, and the context of the problem being addressed, the methods, tools, and techniques used; the priority given a particular instance of the practice; and the quality of the outcome may vary significantly. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, at this maturity level, lessons learned are typically not captured at the organizational level, so approaches and outcomes are difficult to repeat or improve across the organization.

MIL2: Performed

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

1. **Practices are documented.** The practices in the domain are being performed according to a documented plan. The focus here should be on planning to ensure that the practices are intentionally designed (or selected) to serve the organization.
2. **Stakeholders of the practice are identified and involved.** Stakeholders of practices are identified and involved in the performance of the practices. This could include stakeholders from within the function, from across the organization, or from outside the organization, depending on how the organization has implemented or approached the performance of the practice.

3. **Adequate resources are provided to support the process (people, funding, and tools).** Adequate resources are provided in the form of people, funding, and tools to ensure that the practices can be performed as intended. For the purpose of evaluating the performance of this practice, the test for adequacy is to determine whether any desired practices have not been implemented due to a shortage of resources. If all desired practices have been implemented as intended by the organization, then adequate resources have been provided.
4. **Standards and/or guidelines have been identified to guide the implementation of the practices.** The organization has identified some standards and/or guidelines to inform the implementation of practices in the domain. These may simply be the reference sources the organization consulted when developing the plan for performing the practices.

Overall, the practices at MIL2 are more complete than at MIL1 and are no longer performed irregularly or ad hoc in their implementation. As a result, the organization's performance of the practices is more stable. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time.

MIL3: Managed

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

1. **Activities are guided by policies (or other organizational directives) and governance.** Managed activities in a domain receive guidance from the organization in the form of organizational direction, as in policies and governance. Policies are an extension of the planning activities that are in place at MIL2.
2. **Activities are periodically reviewed to ensure they conform to policy.** The domain practices are periodically reviewed to ensure that they conform to policy. In other words, the policies are followed to ensure that the practices continue to be performed.
3. **Responsibility and authority for performing the practice is clearly assigned to personnel.** Personnel are assigned responsibility and authority for performing the domain activities.
4. **Personnel performing the practice have adequate skills and knowledge.** The personnel assigned to perform the activities have adequate domain-specific skills and knowledge to perform their assignments.

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

MILX: Reserved for future use

MILX is a placeholder for use in future model versions.

4.2.2.2 Approach Progression

The progression of the approach to cybersecurity in the model is described by the specific practices in a domain. "Approach" describes the completeness, thoroughness, or level of development of an activity in a domain. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the core activities in the domain. At MIL1, where only the initial set of practices for a domain is expected, an organization is also expected to be performing additional practices at higher MILs.

Table 2 provides an example of the progression of approach in the CYBER domain. At MIL1, a cybersecurity program strategy exists in any form. MIL2 adds more requirements to the strategy, including the need for defined objectives, alignment with the overall organization's strategy, and approval of senior management. Finally, in addition to requiring performance of all MIL1 and MIL2 practices, MIL3 requires that the strategy is being updated to reflect business changes, changes in the operating environment, and changes to the threat profile (developed in the THREAT domain).

Table 2: Example Progression of Specific Characteristics in the CYBER Domain

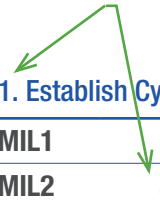
1. Establish Cybersecurity Program Strategy		
MIL1	a.	The organization has a cybersecurity program strategy
MIL2	b.	The cybersecurity program strategy defines objectives for the organization's cybersecurity activities
	c.	The cybersecurity program strategy and priorities are documented and aligned with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

4.2.2.3 Practice Reference Notation

A number of practices within the domains are connected to other model practices. When this occurs for a practice, the model references its connecting practice using a notation that begins with the capitalized short domain name, a hyphen, the objective number (in the order in which it appears in the domain), and the practice letter. Figure 5 shows an example from the RISK domain: the domain's first practice, "There is a documented cybersecurity risk management strategy," would be referenced elsewhere in the model using the notation "RISK-1a." Users of the model may find this practice reference notation helpful when using the model.

Example: RISK-1a

Domain name-Objective number practice letter



1. Establish Cybersecurity Risk Management Strategy

MIL1		*No practice at MIL1*
MIL2	a.	There is a documented cybersecurity risk management strategy
	b.	The strategy provides an approach for risk prioritization, including consideration of impact
MIL3	c.	Organizational risk criteria (tolerance for risk, risk response approaches) are defined
	d.	The risk management strategy is periodically updated to reflect the current threat environment
	e.	An organization-specific risk taxonomy is documented and is used in risk management activities

Figure 5: Referencing an Individual Practice, Example: RISK-1a

4.3 Model Domains

This section presents the model domains. Each domain begins on a new page and is presented according to the outline in Figure 4.

4.3.1 Risk Management (RISK)

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

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

The Risk Management (RISK) domain comprises three objectives:

1. Establish Cybersecurity Risk Management Strategy
2. Manage Cybersecurity Risk
3. Manage RISK Activities *(common objective)*

A cybersecurity risk management strategy is a high-level strategy that provides direction for analyzing and prioritizing cybersecurity risk and defines risk tolerance. The cybersecurity risk management strategy includes a risk assessment methodology, risk monitoring strategy, and cybersecurity governance program. This includes defining the enterprise risk criteria (e.g., impact thresholds, risk response approaches) that guide the cybersecurity program discussed in the CYBER domain later in this model. The cybersecurity risk management strategy should align with the enterprise risk management strategy to ensure that cybersecurity risk is managed in a manner that is consistent with the organization's mission and business objectives.

Managing cybersecurity risk involves framing, identifying and assessing, responding to (accepting, avoiding, mitigating, transferring), and monitoring risks in a manner that aligns with the needs of the organization. Key to performing these activities is a common understanding of the cybersecurity risk management strategy discussed above. With defined risk criteria, organizations can consistently respond to and monitor identified risks. A risk register—a list of identified risks and associated attributes—facilitates this process. Other domains in this model, including RESPONSE, THREAT, and SITUATION, refer to the risk register and illustrate how the practices in the model are strengthened as they connect through a cybersecurity risk management program. The DOE Risk Management Process Guidelines document provides a flexible risk management process for framing (risk strategy), assessing, responding to, and monitoring risk across all levels of an organization.

EXAMPLE: RISK MANAGEMENT

Anywhere Power has developed an enterprise risk management strategy that identifies their risk tolerance and strategy for assessing, responding, and monitoring cybersecurity risks. The Board of Directors reviews this strategy annually to ensure that it remains aligned with the strategic objectives of the organization.

The risk management program of Anywhere Power defines the organization's policies and procedures that implement its risk management strategy. Within this program, risk tolerances, including compliance risk and risk to the delivery of power, are identified and documented. When Anywhere Power performs its risk assessments, they use a risk assessment methodology that integrates the enterprise risk tolerances to ensure that risks are evaluated consistently and are responded to in a manner that aligns with the organization's objectives. Identified risks are recorded in a risk register to ensure that they are monitored and responded to in a timely manner and to identify trends. Anywhere Power uses historical risk management information as input when evaluating the effectiveness of its system of cybersecurity controls.

Domain-Specific Objectives and Practices

1. Establish Cybersecurity Risk Management Strategy

MIL1		*No practice at MIL1*
MIL2	a.	There is a documented cybersecurity risk management strategy
	b.	The strategy provides an approach for risk prioritization, including consideration of impact
MIL3	c.	Organizational risk criteria (tolerance for risk, risk response approaches) are defined
	d.	The risk management strategy is periodically updated to reflect the current threat environment
	e.	An organization-specific risk taxonomy is documented and is used in risk management activities

2. Manage Cybersecurity Risk

MIL1	a.	Cybersecurity risks are identified
	b.	Identified risks are mitigated, accepted, tolerated, or transferred
MIL2	c.	Risk assessments are performed to identify risks in accordance with the risk management strategy
	d.	Identified risks are documented
	e.	Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy
	f.	Identified risks are monitored in accordance with the risk management strategy
	g.	A network (IT and/or OT) architecture is used to support risk analysis
MIL3	h.	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy
	i.	A current cybersecurity architecture is used to support risk analysis
	j.	A risk register (a structured repository of identified risks) is used to support risk management activities

Common Objective and Practices

3. Manage RISK Activities

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

4.3.2 Asset, Change, and Configuration Management (ASSET)

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

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

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

1. Manage Asset Inventory
2. Manage Asset Configuration
3. Manage Changes to Assets
4. Manage ASSET Activities *(common objective)*

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

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

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

EXAMPLE: ASSET, CHANGE, AND CONFIGURATION MANAGEMENT

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

Anywhere Power uses this information for cybersecurity risk management activities, including identifying which systems may be affected by software vulnerabilities, prioritizing cybersecurity incident response, and planning disaster recovery.

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

Domain-Specific Objectives and Practices

1. Manage Asset Inventory

MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, historian, state estimations)
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, Service Level Agreements and conformance of assets to relevant industry standards)
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function
MIL3	e.	The asset inventory is current (as defined by the organization) for assets of defined categories
	f.	There is an inventory for all connected OT and IT assets related to the delivery of the function

2. Manage Asset Configuration

MIL1	a.	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
	b.	Configuration baselines are used to configure assets at deployment
MIL2	c.	The design of configuration baselines includes cybersecurity objectives
MIL3	d.	Configuration of assets are monitored for consistency with baselines throughout the assets' lifecycle
	e.	Configuration baselines are routinely reviewed and updated

3. Manage Changes to Assets

MIL1	a.	Changes to inventoried assets are evaluated before being implemented
	b.	Changes to inventoried assets are logged
MIL2	c.	Changes to assets are tested prior to being deployed, whenever possible
	d.	Change management practices address the full lifecycle of assets (i.e., acquisition, deployment, operation, retirement)
MIL3	e.	Changes to assets are tested for cybersecurity impact prior to being deployed
	f.	Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)

Common Objective and Practices

4. Manage ASSET Activities

MIL1		*No practice at MIL1*
MIL2	a.	Documented practices are followed for asset inventory, configuration, and change management activities
	b.	Stakeholders for asset inventory, configuration, and change management activities are identified and involved
	c.	Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change management activities
	d.	Standards and/or guidelines have been identified to inform asset inventory, configuration, and change management activities
MIL3	e.	Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives
	f.	Policies include compliance requirements for specified standards and/or guidelines
	g.	Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy
	h.	Responsibility and authority for the performance of asset inventory, configuration, and change management activities is assigned to personnel
	i.	Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities

4.3.3 Identity and Access Management (ACCESS)

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

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

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

1. Establish and Maintain Identities
2. Control Access
3. Manage ACCESS Activities *(common objective)*

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

Controlling access includes determining access requirements, granting access to assets based on those requirements, and revoking access when it is no longer required. Access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters. For example, the access requirements for a vendor might allow access only to a specific asset, during a specified maintenance interval, and when using multifactor authentication. At higher maturity indicator levels, more scrutiny is applied to the access being granted. Access is granted only after considering risk to the function, and regular reviews of access are conducted.

EXAMPLE: IDENTITY AND ACCESS MANAGEMENT

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

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

Anywhere Power updates its identity management processes to include coordination with the organization's HR processes to help ensure that whenever a user changes roles or leaves the organization, their access will be reviewed and updated appropriately. It also institutes a quarterly review to ensure that access granted to the utility's assets aligns with access requirements.

Domain-Specific Objectives and Practices

1. Establish and Maintain Identities

MIL1	a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities) b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys) c. Identities are deprovisioned when no longer required
MIL2	d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access) e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity f. Identities are deprovisioned within organizationally-defined time thresholds when no longer required
MIL3	g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RISK-1c)

2. Control Access

MIL1	a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters) b. Access is granted to identities based on requirements c. Access is revoked when no longer required

MIL2	d. Access requirements incorporate least privilege and separation of duties principles e. Access requests are reviewed and approved by the asset owner f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
MIL3	g. Access privileges are reviewed and updated to ensure validity, at an organizationally-defined interval h. Access to assets is granted by the asset owner based on risk to the function i. Anomalous access attempts are monitored as indicators of cybersecurity events

Common Objective and Practices

3. Manage ACCESS Activities

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

4.3.4 Threat and Vulnerability Management (THREAT)

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

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

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

The Threat and Vulnerability Management domain comprises three objectives:

1. Identify and Respond to Threats
2. Reduce Cybersecurity Vulnerabilities
3. Manage THREAT Activities *(common objective)*

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

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

EXAMPLE: THREAT AND VULNERABILITY MANAGEMENT

Anywhere Power has examined the types of threats that it normally responds to, including malicious software, denial-of-service attacks, and activist cyber-attack groups. This information has been used to develop Anywhere Power's documented threat profile.

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

When reducing cybersecurity vulnerabilities, Anywhere Power uses the NIST Common Vulnerability Scoring System (CVSS) to better identify the potential impacts of known software vulnerabilities. This allows the organization to prioritize reduction activities according to the importance of the vulnerabilities.

Domain-Specific Objectives and Practices

1. Identify and Respond to Threats

MIL1	a.	Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings)
	b.	Cybersecurity threat information is gathered and interpreted for the function
	c.	Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status)
MIL2	d.	A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function
	e.	Threat information sources that address all components of the threat profile are prioritized and monitored
	f.	Identified threats are analyzed and prioritized
	g.	Threats are addressed according to the assigned priority
MIL3	h.	The threat profile for the function is validated at an organization-defined frequency
	i.	Analysis and prioritization of threats are informed by the function's (or organization's) risk criteria (RISK-1c)
	j.	Threat information is added to the risk register (RISK-2j)

2. Reduce Cybersecurity Vulnerabilities

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

Common Objective and Practices

3. Manage THREAT Activities

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

4.3.5 Situational Awareness (SITUATION)

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

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

The Situational Awareness domain comprises four objectives:

1. Perform Logging
2. Monitor the Function
3. Establish and Maintain a Common Operating Picture
4. Manage SITUATION Activities *(common objective)*

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

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

EXAMPLE: SITUATIONAL AWARENESS

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

Anywhere Power consolidates current cybersecurity information from these sources, as well as its own data on cybersecurity incidents, to develop an understanding of its current state of operations. The organization summarizes its current state of operations using a color-coded scale, which is posted on the wall of the control room as well as on the corporate intranet site: green is "normal," yellow is "alerted," and red is "state of emergency."

As the function moves through the state-of-operations scale described above, personnel modify their behavior according to a plan. For example, when the current state is "yellow," personnel increase logging and log monitoring. When the condition is "red," they change firewall rule sets, delay nonessential change requests, and activate the cybersecurity incident response team.

Domain-Specific Objectives and Practices

1. Perform Logging

MIL1	a.	Logging is occurring for assets important to the function where possible
MIL2	b.	Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])
	c.	Log data are being aggregated within the function
MIL3	d.	Logging requirements are based on the risk to the function
	e.	Log data support other business and security processes (e.g., incident response, asset management)

2. Monitor the Function

MIL1	a.	Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)
	b.	Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event
MIL2	c.	Monitoring and analysis requirements have been defined for the function and address timely review of event data
	d.	Alarms and alerts are configured to aid the identification of cybersecurity events (RESPONSE-1b)
	e.	Indicators of anomalous activity have been defined and are monitored across the operational environment
	f.	Monitoring activities are aligned with the function's threat profile (THREAT-1d)

MIL3	g. Monitoring requirements are based on the risk to the function h. Monitoring is integrated with other business and security processes (e.g., incident response, asset management) i. Continuous monitoring is performed across the operational environment to identify anomalous activity j. Risk register (RISK-2j) content is used to identify indicators of anomalous activity k. Alarms and alerts are configured according to indicators of anomalous activity

3. Establish and Maintain a Common Operating Picture (COP)

MIL1	*No practice at MIL1*
MIL2	a. Monitoring data are aggregated to provide near-real-time understanding of the operational state of the function (i.e., a common operating picture; a COP may or may not include visualization or be presented graphically) b. Methods of communicating the current state of cybersecurity for the function are established and maintained c. Information from across the organization is available to enhance the common operating picture
MIL3	d. Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the common operating picture e. Information from outside the organization is collected to enhance the common operating picture f. Pre-defined states of operation are defined and invoked (manual or automated process) based on the common operating picture

Common Objective and Practices

4. Manage SITUATION Activities

MIL1	*No practice at MIL1*
MIL2	a. Documented practices are followed for logging, monitoring, and COP activities b. Stakeholders for logging, monitoring, and COP activities are identified and involved c. Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities d. Standards and/or guidelines have been identified to inform logging, monitoring, and COP activities
MIL3	e. Logging, monitoring, and COP activities are guided by documented policies or other organizational directives f. Policies include compliance requirements for specified standards and/or guidelines g. Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy h. Responsibility and authority for the performance of logging, monitoring, and COP activities is assigned to personnel i. Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities

4.3.6 Information Sharing and Communications (SHARING)

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

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

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

1. Share Cybersecurity Information
2. Manage SHARING Activities *(common objective)*

Sharing cybersecurity information begins with gathering cybersecurity information relevant to the function. This information is available from many sources, including vendors, government entities, and peers. Essential to the well-being of the grid is the sharing of different types of risk-related information, which makes the secure distribution of this information important to the security of the subsector. As threats are responded to and vulnerabilities are discovered, utilities should ensure that relevant data is effectively and appropriately shared so that peers may also reduce their risk and improve grid resilience. Forums such as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) can facilitate this sharing.

EXAMPLE: INFORMATION SHARING AND COMMUNICATIONS

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

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

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

Domain-Specific Objectives and Practices

1. Share Cybersecurity Information

MIL1	a.	Information is collected from and provided to selected individuals and/or organizations
	b.	Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT, law enforcement)
MIL2	c.	Information sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected utilities, vendors, sector organizations, regulators, internal entities)
	d.	Information is collected from and provided to identified information sharing stakeholders
	e.	Technical sources are identified that can be consulted on cybersecurity issues
	f.	Provisions are established and maintained to enable secure sharing of sensitive or classified information)
	g.	Information sharing practices address both standard operations and emergency operations
MIL3	h.	Information sharing stakeholders are identified based on shared interest in and risk to the health of the electricity subsector
	i.	The function participates with information sharing and analysis centers
	j.	Information sharing requirements have been defined for the function and address timely dissemination of cybersecurity information
	k.	Procedures are in place to analyze and de-conflict received information
	l.	A network of internal and external trust relationships (both formal and informal) has been established to vet and validate information about cyber events

Common Objective and Practices

2. Manage SHARING Activities

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

4.3.7 Event and Incident Response, Continuity of Operations (RESPONSE)

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

A *cybersecurity event* in a system or network is any observable occurrence that is related to a cybersecurity requirement (confidentiality, integrity, or availability of assets). A *cybersecurity incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

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

1. Detect Cybersecurity Events
2. Escalate Cybersecurity Events
3. Respond to Escalated Cybersecurity Events
4. Plan for Continuity
5. Manage RESPONSE Activities *(common objective)*

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

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

Responding to escalated cybersecurity events requires the organization to have a process to limit the impact of cybersecurity events to subsector functions. The process should describe how the organization manages all phases of the incident lifecycle (e.g., triage, handling, communication, coordination, and closure). Conducting lessons-learned reviews as a part of cybersecurity event and incident response helps the organization eliminate the exploited vulnerability that led to the incident.

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

EXAMPLE: EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS

Anywhere Power has purchased a helpdesk tracking system to log and track important cybersecurity events. On the wall in their shared working area, Anywhere Power has posted a chart that identifies criteria for escalating cybersecurity events, which include who must be notified and response time objectives. When the utility experiences a cybersecurity incident, the incident response plan requires that the incident be logged and communicated to key stakeholders. The reporting process includes those responsible for communicating the common operating picture described in the SITUATION domain.

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

Domain-Specific Objectives and Practices

1. Detect Cybersecurity Events

MIL1	a. There is a point of contact (person or role) to whom cybersecurity events are reported b. Cybersecurity events are detected and reported c. Cybersecurity events are logged and tracked
MIL2	d. Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events) e. There is a repository where cybersecurity events are logged based on the established criteria
MIL3	f. Event information is correlated to support incident analysis by identifying patterns, trends, and other common features g. Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RISK-2j) and threat profile (THREAT-1d) to help detect known threats and monitor for identified risks h. The common operating picture for the function is monitored to support the identification of cybersecurity events

2. Escalate Cybersecurity Events

MIL1	a. Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria b. Cybersecurity events are analyzed to support escalation and the declaration of cybersecurity incidents c. Escalated cybersecurity events and incidents are logged and tracked
MIL2	d. Cybersecurity event escalation, including cybersecurity incident criteria, are established based on the potential impact to the function e. Cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency f. There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure

MIL3	g. Cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization's risk register and threat profile (THREAT-1d) h. Escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (SITUATION-3a) for the function i. Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features

3. Respond to Escalated Cybersecurity Events

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

4. Plan for Continuity

MIL1	a.	The activities necessary to sustain minimum operations of the function are identified
	b.	The sequence of activities necessary to return the function to normal operation is identified
	c.	Continuity plans are developed to sustain and restore operation of the function
MIL2	d.	Business impact analyses inform the development of continuity plans
	e.	Recovery time objectives for the function are incorporated into continuity plans
	f.	Continuity plans are evaluated and exercised
MIL3	g.	Business impact analyses are periodically reviewed and updated
	h.	Recovery time objectives are aligned with the function's risk criteria (RISK-1c)
	i.	The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly
	j.	Continuity plans are periodically reviewed and updated
	k.	Restored assets are configured appropriately and inventory information is updated following execution of continuity plans

Common Objective and Practices

5. Manage RESPONSE Activities

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

4.3.8 Supply Chain and External Dependencies Management (DEPENDENCIES)

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

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

This model classifies external dependencies as upstream or downstream. *Upstream dependencies* are external parties, including suppliers, on which the delivery of the function depends. *Downstream dependencies* are external parties that depend on the delivery of the function, such as customers and some operating partners.

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

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

1. Identify Dependencies
2. Manage Dependency Risk
3. Manage DEPENDENCIES Activities *(common objective)*

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

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

EXAMPLE: SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT

Anywhere Power receives products and services from multiple vendors. As part of a recent initiative to support Advanced Metering Infrastructure (AMI), the utility began to work with a new AMI vendor who, during the normal course of business, will have access to sensitive data and systems.

Within the contract for the project, Anywhere Power mandated the nondisclosure of sensitive data. It also specified cybersecurity requirements for the handling, communication, and storage of its information, requiring that it would be encrypted both in transit and in storage. The cybersecurity requirements also stated that passwords and cryptographic keys would be properly managed, and they specified strict limits and controls on the vendor personnel and systems that will have access to Anywhere Power's systems and data during deployment, operations, and maintenance. Additionally, Anywhere Power conducted a review of the vendor's practices (including the vendor's cybersecurity practices with respect to its suppliers), participated in a security design review of the vendor's proposed system, and plans to conduct periodic audits of the delivered AMI system to ensure that the vendor continues to meet its obligations.

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

Domain-Specific Objectives and Practices

1. Identify Dependencies

MIL1	a.	Important upstream IT and OT dependencies are identified (i.e., external parties on which the delivery of the function depend, including suppliers)
	b.	Important downstream dependencies are identified (i.e., external parties that are dependent on the delivery of the function)
MIL2	c.	Upstream dependencies are identified according to established criteria
	d.	Downstream dependencies are identified according to established criteria
	e.	Single-source and other essential dependencies are identified
	f.	Dependencies are prioritized
MIL3	g.	Dependency prioritization and identification are based on the function's risk criteria (RISK-1c)

2. Manage Dependency Risk

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

Common Objective and Practices

3. Manage DEPENDENCIES Activities

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

4.3.9 Workforce Management (WORKFORCE)

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

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

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

The Workforce Management (WORKFORCE) domain comprises five objectives:

1. Assign Cybersecurity Responsibilities
2. Control the Workforce Lifecycle
3. Develop Cybersecurity Workforce
4. Increase Cybersecurity Awareness
5. Manage WORKFORCE Activities *(common objective)*

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

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

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

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

EXAMPLE: WORKFORCE MANAGEMENT

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

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

Domain-Specific Objectives and Practices

1. Assign Cybersecurity Responsibilities

MIL1	a. Cybersecurity responsibilities for the function are identified b. Cybersecurity responsibilities are assigned to specific people
MIL2	c. Cybersecurity responsibilities are assigned to specific roles, including external service providers d. Cybersecurity responsibilities are documented (e.g., in position descriptions)
MIL3	e. Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate f. Cybersecurity responsibilities are included in job performance evaluation criteria g. Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage

2. Control the Workforce Lifecycle

MIL1	a.	Personnel vetting (e.g., background checks, drug tests) is performed at hire for positions that have access to the assets required for delivery of the function
	b.	Personnel termination procedures address cybersecurity
MIL2	c.	Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of the function
	d.	Personnel transfer procedures address cybersecurity
MIL3	e.	Risk designations are assigned to all positions that have access to the assets required for delivery of the function
	f.	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation
	g.	Succession planning is performed for personnel based on risk designation
	h.	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures

3. Develop Cybersecurity Workforce

MIL1	a.	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities
MIL2	b.	Cybersecurity knowledge, skill, and ability gaps are identified
	c.	Identified gaps are addressed through recruiting and/or training
	d.	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training)
MIL3	e.	Cybersecurity workforce management objectives that support current and future operational needs are established and maintained
	f.	Recruiting and retention are aligned to support cybersecurity workforce management objectives
	g.	Training programs are aligned to support cybersecurity workforce management objectives
	h.	The effectiveness of training programs is evaluated at an organization-defined frequency and improvements are made as appropriate
	i.	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities

4. Increase Cybersecurity Awareness

MIL1	a.	Cybersecurity awareness activities occur
MIL2	b.	Objectives for cybersecurity awareness activities are established and maintained
	c.	Cybersecurity awareness content is based on the organization's threat profile (THREAT-1d)
MIL3	d.	Cybersecurity awareness activities are aligned with the pre-defined states of operation
	e.	The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate

Common Objective and Practices

5. Manage WORKFORCE Activities

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

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

4.3.10 Cybersecurity Program Management (CYBER)

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

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

The Cybersecurity Program Management (CYBER) domain comprises five objectives:

1. Establish Cybersecurity Program Strategy
2. Sponsor Cybersecurity Program
3. Establish and Maintain Cybersecurity Architecture
4. Perform Secure Software Development
5. Manage CYBER Activities *(common objective)*

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

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

A cybersecurity architecture is an integral part of the enterprise architecture. It describes the structure and behavior of an enterprise's security processes, cybersecurity systems, personnel, and subordinate organizations and aligns them with the organization's mission and strategic plans. An important element of the cybersecurity architecture is effective isolation of IT systems from OT systems.

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

EXAMPLE: CYBERSECURITY PROGRAM MANAGEMENT

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

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

The head of customer service and vice president of accounting are counting on the new program to address both immediate and collateral damage from potential incidents and the pubic relation issues that follow. The head of IT and the vice president for engineering are expecting guidance on systems development and methods to mitigate risks.

Domain-Specific Objectives and Practices

1. Establish Cybersecurity Program Strategy

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

2. Sponsor Cybersecurity Program

MIL1	a.	Resources (people, tools, and funding) are provided to support the cybersecurity program
	b.	Senior management provides sponsorship for the cybersecurity program
MIL2	c.	The cybersecurity program is established according to the cybersecurity program strategy
	d.	Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a cybersecurity program aligned with the program strategy
	e.	Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities is regularly communicated by senior management)
	f.	If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program
	g.	The development and maintenance of cybersecurity policies is sponsored
	h.	Responsibility for the cybersecurity program is assigned to a role with requisite authority
MIL3	i.	The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy
	j.	The cybersecurity program is independently reviewed for achievement of cybersecurity program objectives
	k.	The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate
	l.	The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives

3. Establish and Maintain Cybersecurity Architecture

MIL1	a.	A strategy to architecturally isolate the organization's IT systems from OT systems is implemented
MIL2	b.	A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy
	c.	Architectural segmentation and isolation is maintained according to a documented plan
MIL3	d.	Cybersecurity architecture is updated at an organization-defined frequency to keep it current

4. Perform Secure Software Development

MIL1		*No practice at MIL1*
MIL2	a.	Software to be deployed on assets that are important to the delivery of the function is developed using secure software development practices
MIL3	b.	Policies require that software to be deployed on assets that are important to the delivery of the function be developed using secure software development practices

Common Objective and Practices

5. Manage CYBER Activities

MIL1		*No practice at MIL1*
MIL2	a.	Documented practices are followed for cybersecurity program management activities
	b.	Stakeholders for cybersecurity program management activities are identified and involved
	c.	Standards and/or guidelines have been identified to inform cybersecurity program management activities
MIL3	d.	Cybersecurity program management activities are guided by documented policies or other organizational directives
	e.	Cybersecurity program management activities are periodically reviewed to ensure conformance with policy
	f.	Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities

5 USING THE MODEL

The model was designed to be usable across the electricity subsector to evaluate cybersecurity capabilities consistently, communicate capability levels in meaningful terms, and guide an organization in prioritizing cybersecurity investments. The model is supported by an evaluation survey and scoring mechanism that can be used by an organization to evaluate its cybersecurity capabilities based on the model. The survey is available from the DOE upon request.

This section describes a recommended approach for using the model, summarized in Figure 6.

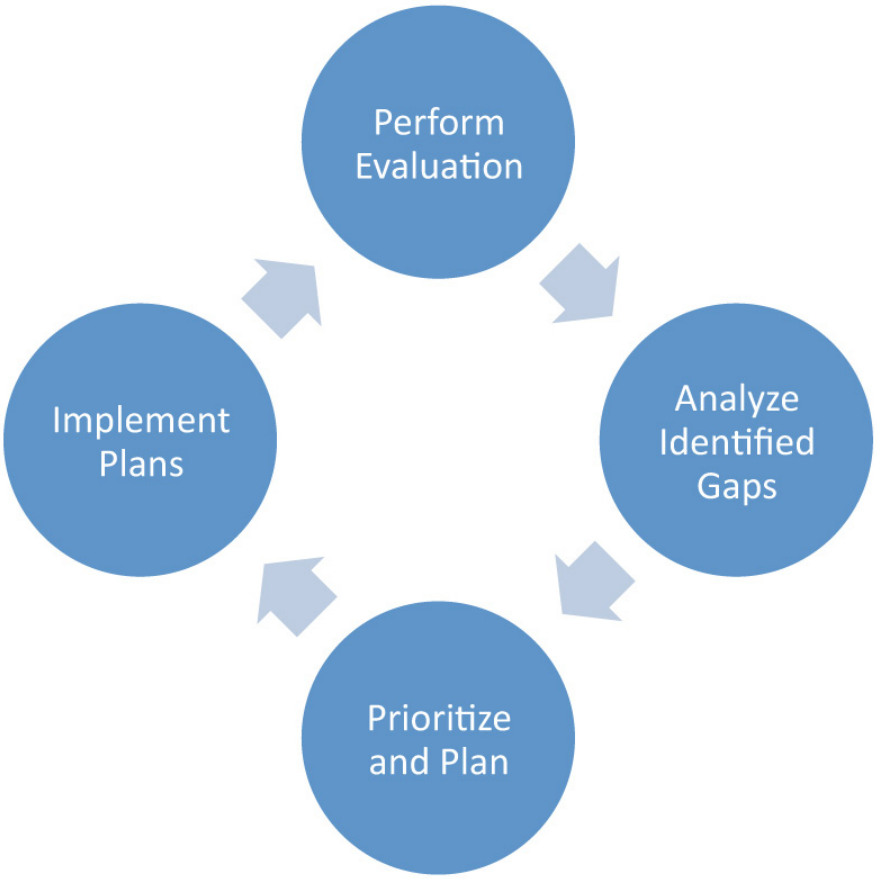


Figure 6: Recommended Approach for Using the Model

Perform an Evaluation

The model and evaluation survey were designed to enable an organization to complete a self-evaluation in less than one day without extensive study or preparation. After quickly familiarizing itself with the model and receiving the evaluation survey, the organization should identify which part of the organization it wishes to evaluate. Guidance for defining the scope of the evaluation for the organization is provided in the survey instrument documentation.

The organization should select the appropriate personnel to answer the questions in the survey. Participation by a broad representation across the part of the organization being evaluated yields the best results and enables internal information sharing about the model practices. It is recommended that the personnel selected to complete the survey include operational personnel, management stakeholders, and any others who could provide useful information on the organization's performance of cybersecurity practices in the model.

It is recommended that the evaluation survey be completed in a workshop setting, led by a facilitator who is familiar with the model content and use. Pilot users of the model found that a facilitated workshop provided value in consistent interpretation of model practices and in catalyzing discussions among the participants to explore the performance of the model practices by the organization.

Upon completion of the evaluation, a scoring report for the evaluated scope is generated. This report provides a picture of the current state of organizational practices against the model. This report should be reviewed with the evaluation workshop participants and any discrepancies and other issues identified and addressed.

Analyze Identified Gaps

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

It is recommended that the organization identify its desired capability profile—a target MIL rating for each domain in the model. The desired profile is determined by selecting the practices in the model that the organization wishes to implement based on its business objectives and the risk to critical infrastructure. The selection of the desired profile should performed by the appropriate organizational stakeholders. This might be a single individual who has expertise in the function's operations and management, but it is likely to be a collection of individuals.

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

Prioritize and Plan

Gaps identified in the previous step should be prioritized for action. The following questions may be considered when prioritizing the gaps for action.

- Which gaps are most important in the context of the organization's objectives?
- Which gaps are most important in the context of the organization's role in critical infrastructure?
- Can the necessary resources be made available to address the gap?
- Are there efficiencies that can be realized by addressing the gap? (Efficiencies may include streamlining controls or compliance activities.)

When prioritizing gaps, it is important to consider time, costs, and risks associated with closing the gaps.

Once the identified gaps are prioritized, plans should be developed to address selected gaps in a timely manner.

Implement Plans and Periodically Re-evaluate

Plans developed in the previous step should be implemented to address the identified gaps.

Model evaluations should be conducted periodically to track progress. Re-evaluations should also be considered in response to major changes in the business, technology, market, or threat environments to ensure that the current profile matches the organization's desired state.

Sharing Results

The DOE is developing an information sharing capability that will enable an organization's evaluation results to be anonymously shared in exchange for benchmarking data. The DOE encourages organizations to share their evaluation data and receive the benchmarking data so they can compare their capabilities with peer organizations in the subsector. Information about the availability and structure of this program can be requested from the DOE.

APPENDIX A: REFERENCES

The right-hand columns of the reference table below show where each referenced source was either used in the development of this document or may serve as a source for further information regarding the practices identified within the model in one or more domains or in the glossary. References that informed the document more broadly have no marker in any of the right-hand columns.

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[CEII] Federal Energy Regulatory Commission. *Critical Energy Infrastructure Information (CEII) Regulations*. June 28, 2010. <http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp>						•				•	
[CERT CSIRT FAQs] Software Engineering Institute, Carnegie Mellon University. *CSIRT FAQ*. May 2012. <http://www.cert.org/csirts/csirt_faq.html>		•					•				•
[CERT CSIRTs] West Brown, Moira; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Software Engineering Institute, Carnegie Mellon University. April 2003. <http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm>							•				
[CERT RMM] Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT®-RMM Version 1.1)*. Addison-Wesley, 2011.	•	•	•	•	•	•	•	•	•	•	•
[CERT SGMM] CERT – The SGMM Team. *Smart Grid Maturity Model (SGMM) Version 1.2 (CMU/SEI-2011-TR-025)*. Software Engineering Institute, Carnegie Mellon University. September 2011. <http://www.sei.cmu.edu/reports/11tr025.pdf>	•	•			•	•		•	•	•	
[CERT State of the Practice of CSIRTs] Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; Zajicek, Mark. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-TR-001). Software Engineering Institute, Carnegie Mellon University. October 2003. <http://www.cert.org/archive/pdf/03tr001.pdf>							•				

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[CNSSI 4009] Committee on National Security Systems, National Information Assurance (IA) Glossary, CNSSI 4009 Instructions no. 4009, April 26, 2010. <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>	•									•	•
[DHS Cross-Sector Roadmap] Industrial Control Systems Joint Working Group. *Cross-Sector Roadmap for Cybersecurity of Control Systems, Revision 3.0.* United States Computer Emergency Readiness Team. September 30, 2011.				•		•				•	
[DHS ICS-CERT] Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team. May 2012. <http://www.us-cert.gov/control_systems/ics-cert/>		•					•				
[DHS ICSJWG] Department of Homeland Security, Industrial Control Systems Joint Working Group. May 2012. <http://www.us-cert.gov/control_systems/icsjwg/>						•			•		
[DHS PCII] Department of Homeland Security (DHS). *Who Can Access Protected Critical Infrastructure Information (PCII).* May 2012. <http://www.dhs.gov/files/programs/gc_1193089801658.shtm>						•				•	
[DHS Procurement] Department of Homeland Security, Control Systems Security Program, National Cyber Security Division. *Department of Homeland Security: Cyber Security Procurement Language for Control Systems.* September 2009.					•			•			
[DOE RMP] U.S. Department of Energy. *Electricity Subsector Cybersecurity Risk Management Process.* May 2012.	•									•	•
[DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity] Energy Sector Control Systems Working Group. *Roadmap to Achieve Energy Delivery Systems Cybersecurity.* Department of Energy (DOE). September 2011. <http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf>		•		•		•	•	•		•	
[EOPUS Policy Framework] Executive Office of the President of the United States. *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future.* June 2011. <http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf>											

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[ES-CCMM] Definitions labeled ES-CCMM were produced by the Electric Electricity Subsector Cybersecurity Capability Maturity Model team during the development of the model definition document, May 2012.											•
[ES-ISAC] Electricity Sector Information Sharing and Analysis Center (ES-ISAC). May 2012. <http://www.esisac.com/SitePages/Home.aspx>						•	•		•		
[ES-SPP] Energy Sector Specific Plan: An Annex to the National Infrastructure Protection Plan 2010. <http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf>	•			•	•		•	•	•		
[FERC] Federal Energy Regulatory Commission (FERC) Glossary. <http://www.ferc.gov/market-oversight/guide/glossary.asp>											•
[FIRST] Forum of Incident Response Teams (FIRST). May 2012. <http://www.first.org/_assets/resources/guides/csirt_case_classification.html>					•	•	•				
[HSPD-7] Homeland Security Presidential Directive – 7 <http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1>	•					•				•	
[IACCM BRM3] International Association for Contract & Commercial Management (IACCM). *The IACCM Business Risk Management Maturity Model (BRM3).* January 2003.	•									•	
[ISA 99] International Society of Automation (ISA). *ANSI/ISA-99.02.01-2009, Industrial Automation and Control Systems Security: Establishing an Industrial Automation and Control Systems Security Program.* 2009.											
[ISACs] National Council of Information Sharing and Analysis Centers (ISACs). May 2012. <http://www.isaccouncil.org/>					•	•	•			•	
[ISO 27005:2011] International Organization for Standardization. *ISO 27005:2011 Information Security Risk Management.* May 2011.	•									•	

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[ISO/IEC 21827:2008] International Organization for Standardization. I*SO/IEC 21827:2008 Systems Security Engineering – Capability Maturity Model (SSE-CMM).* October 2008.			•	•		•				•	
[ISO/IEC 27001:2005] International Organization for Standardization. *ISO/IEC CD 27001:2005 Information security management systems.* October 2008.		•	•	•	•	•	•			•	
[ISO/IEC 27002:2005] International Organization for Standardization. I*SO/IEC27002:2005 Code of practice for information security management.* April 2008.		•	•	•	•	•	•			•	
[ISO 28001:2007] International Organization for Standardization. I*SO/IEC20001:*2007 Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance.								•		•	
[MIT SCMM] Rice, Jr., James B.; Tenney, William. *Supply Chain Strategy.* "How Risk Management Can Secure Your Business Future." Massachusetts Institute of Technology. July 2007. <http://web.mit.edu/scresponse/repository/rice_tenney_SCS_RMM_june-july_2007.pdf>								•			
[NASA RMMM] National Aeronautics and Space Administration (NASA). *NASA RMC VI: Continuous Risk Management Maturity Assessment. Pages 5-7.* December 2005. <http://www.rmc.nasa.gov/presentations/Powell_CRM_Maturity_Assessment.pdf>	•			•							
[NDIA ESA] National Defense Industrial Association (NDIA), System Assurance Committee. *Engineering for System Assurance, Version 1.0.* October 2008.	•			•				•			
[NERC CATF] North American Electric Reliability Corporation (NERC). *Cyber Attack Task Force Final Report.* May 2012. <http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf>				•	•	•					
[NERC CIP-001] North American Electric Reliability Corporation (NERC). *Standard CIP-001-1 – Sabotage Reporting.* June 2007. <http://www.nerc.com/files/CIP-001-1.pdf>				•		•				•	

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[NERC CIP-002] North American Electric Reliability Corporation (NERC). *Standard CIP-002-3 – Cyber Security - Critical Cyber Asset Identification.* December 2009. <http://www.nerc.com/files/CIP-002-3.pdf>	•	•	•	•		•					
[NERC CIP-003] North American Electric Reliability Corporation (NERC). *Standard CIP-003-3 – Cyber Security – Security Management Controls.* December 2009. <http://www.nerc.com/files/CIP-003-3.pdf>	•					•				•	
[NERC CIP-004] North American Electric Reliability Corporation (NERC). *Standard CIP-004-3 – Cyber Security – Personnel & Training.* December 2009. <http://www.nerc.com/files/CIP-004-3.pdf>						•			•		
[NERC CIP-005] North American Electric Reliability Corporation (NERC). *Standard CIP-005-3 – Cyber Security – Electronic Security Perimeter(s).* February 2010. <http://www.nerc.com/files/CIP-005-3.pdf>	•	•	•	•						•	
[NERC CIP-006] North American Electric Reliability Corporation (NERC). *Standard CIP-006-3 – Cyber Security –Physical Security Perimeter(s).* February 2010. <http://www.nerc.com/files/CIP-006-3.pdf>	•	•	•	•						•	
[NERC CIP-007] North American Electric Reliability Corporation (NERC). *Standard CIP-007-3 – Cyber Security –Systems Security Management.* January 2011. <http://www.nerc.com/files/CIP-007-3.pdf>	•	•	•	•	•	•	•			•	
[NERC CIP-008] North American Electric Reliability Corporation (NERC). *Standard CIP-008-3 – Cyber Security –Incident Reporting and Response Planning.* December 2009. <http://www.nerc.com/files/CIP-008-3.pdf>						•	•		•	•	
[NERC CIP-009] North American Electric Reliability Corporation (NERC). *Standard CIP-009-3 – Cyber Security –Recovery Plans for Critical Cyber Assets.* December 2009. <http://www.nerc.com/files/CIP-009-3.pdf>		•					•			•	
[NERC CRPA] North American Electric Reliability Corporation (NERC). *NERC Cyber Risk Preparedness Assessment: Improving the Cyber Security Posture of the North American Bulk Power System.* 2012. <http://www.esisac.com/Public%20Library/Reports/CRPA%202010%20Report.pdf >				•			•	•	•	•	

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[NERC RTSA] Real-Time Tools Best Practices Task Force. *Section 2.0 Reliability Tools for Situational Awareness.* North American Electric Reliability Corporation (NERC). 2008. <http://www.nerc.com/docs/oc/rtbptf/Section%202_2_1_08.pdf>				•	•					•	
[NERC Security Guideline: Information Protection] North American Electric Reliability Corporation (NERC). *Security Guideline for the Electricity Sector: Protecting Potentially Sensitive Information.* August 2011. <http://www.nerc.com/docs/cip/sgwg/Protecting%20Sensitive%20Information%20Guideline%20Draft%20Revision%208-30-11%20v04.pdf >		•				•				•	
[NERC Security Guideline: Threat and Incident Reporting] North American Electric Reliability Corporation (NERC). *Security Guideline for the Electricity Sector: Threat and Incident Reporting.* August 2011. <http://www.nerc.com/files/Incident-Reporting.pdf>				•		•		•		•	
[NESCO Logging] Bromberger, Seth; Maschino, Cliff. *Security Logging in the Utility Sector: Roadmap to Improved Maturity.* National Electric Sector Cybersecurity Organization (NESCO); Southern California Edison. 2012.				•	•	•	•	•			
[NESCO] National Electric Sector Cybersecurity Organization (NESCO). May 2012. <http://www.energysec.org/nesco>		•		•	•	•	•			•	
[NESCOR Failure Scenarios] National Electric Sector Cybersecurity Organization Resource (NESCOR). *Electric Sector Representative Failure Scenarios by Domain.* July 2011.	•	•	•	•	•	•	•	•	•		
[NIST Framework] National Institute of Standards and Technology (NIST). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.* February 2012. <http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/IKBFramework/NIST_Framework_Release_2-0_corr.pdf>											
[NIST Security Considerations in SDLC] Radack, Shirley. *SECURITY CONSIDERATIONS IN THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE.* National Institute of Standards and Technology (NIST). 2008. <http://www.itl.nist.gov/lab/bulletns/bltndec03.htm>	•									•	

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[NIST SP800-16] Wilson, Mark; Stine, Kevin; Bowen, Pauline. *NIST Special Publication 800-16 Revision 1.0 Information Security Training Requirements: A Role- and Performance-Based Model.* National Institute of Standards and Technology (NIST). March 2009. <http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf>									•	•	
[NIST SP800-37] Joint Task Force Transformation Initiative. *NIST Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems.* National Institute of Standards and Technology (NIST). February 2010. <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>	•				•	•		•		•	
[NIST SP800-40] Mell, Peter; Bergeron, Tiffany; Henning, David. *NIST Special Publication 800-40 Version 2.0 Creating a Patch Management and Vulnerability Management Program.* National Institute of Standards and Technology (NIST). November 2005. <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>				•			•				
[NIST SP800-50] Wilson, Mark; Hash, Joan. *NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program.* National Institute of Standards and Technology (NIST). October 2003. <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>									•		
[NIST SP800-53] Joint Task Force Transformation Initiative. *NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations.* National Institute of Standards and Technology (NIST). August 2009. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf>	•	•	•	•		•	•		•	•	
[NIST SP800-61] Scarfone, Karen; Grance, Tim; Masone, Kelly. *NIST Special Publication 800-61 Revision 1 Computer Security Incident Handling Guide.* National Institute of Standards and Technology (NIST). March 2008. <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>							•			•	
[NIST SP800-64] Kissel, Richard; Stine, Kevin; Scholl, Matthew; Rossman, Hart; Fahlsing, Jim; Gulick, Jessica. *NIST Special Publication 800-64 Revision 2 Security Considerations in the System Development Life Cycle.* National Institute of Standards and Technology (NIST). October 2008. <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>				•			•			•	

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[NIST SP800-82] Stouffer, Kevin; Falco, Joe; Scarfone, Karen. *NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology (NIST). June 2011. <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>							•				
[NIST SP800-83] Mell, Peter; Kent, Karen; Nusbaum, Joseph. *NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling.* National Institute of Standards and Technology (NIST). November 2005. <http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>							•				
[NIST SP800-128] Guide for Security-Focused Configuration Management of Information Systems, Special Publication 800-128, August 2011. <http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf>		•								•	
[NIST SP800-137] Dempsey, Kelley; Chawla, Nirali Shah; Johnson, Arnold; Johnston, Ronald; Jones, Alicia Clay; Orebaugh, Angela; Scholl, Matthew; Stine, Kevin. *NIST Special Publication 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* National Institute of Standards and Technology (NIST). September 2011. <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>					•	•		•		•	
[NIST NVD] National Institute of Standards and Technology (NIST). *National Vulnerability Database.* NIST, [Online]. May 2012. <http://nvd.nist.gov/cvss.cfm>	•			•	•	•	•				
[NISTIR 7622] Marianne Swanson, Nadya Bartol, and Rama Moorthy, Piloting Supply Chain Risk Management for Federal Information Systems, Draft NISTIR 7622, June 2010. <http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf>								•		•	
[NISTIR 7628 Vol. 1] The Smart Grid Interoperability Panel – Cyber Security Working Group. *NISITIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1,Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.* National Institute of Standards and Technology (NIST). August 2010. <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf>	•	•	•							•	

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[NISTIR 7628 Vol. 3] The Smart Grid Interoperability Panel – Cyber Security Working Group. *NISITIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References.* National Institute of Standards and Technology (NIST). August 2010. <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf>				•		•				•	•
[NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan] National Rural Electric Cooperative Association (NRECA). *Guide to Developing a Cyber Security and Risk Mitigation Plan.* 2011. < http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2[1].pdf>	•			•	•	•	•			•	
[NRECA Interoperability and Cyber Security Plan] National Rural Electric Cooperative Association (NRECA). *Interoperability and Cyber Security Plan.* May 2010. <http://www.nreca.coop/press/NewsReleases/Documents/InteroperabilityCyberSecurityPlan.pdf>					•			•			
[NRECA Security Questions for Vendors] National Rural Electric Cooperative Association (NRECA). *Security Questions for Vendors.* May 2012. <https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx>								•		•	
[OE-417] U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability. *Form OE-417 The Electric Emergency Incident and Disturbance Report.* February 2011. <http://www.oe.netl.doe.gov/oe417.aspx>						•			•		
[OECD Reducing Systemic Cybersecurity Risk] Sommer, Peter; Brown, Ian. *"Reducing Systemic Cybersecurity Risk".* Organisation for Economic Co-operation and Development (OECD). January 2011. <http://www.oecd.org/dataoecd/57/44/46889922.pdf>					•			•			
[SANS Securing a Smarter Grid] Luallen, Matt. *Securing a Smarter Grid: Risk Management in Power Utility Networks.* SANS. October 2009. <http://www.sans.org/reading_room/analysts_program/NitroSecurity_Securing_Smarter_Grid.pdf>	•			•							
[SEI CMM] Mark Paulk, Charles Weber, Suzanne Garcia, Mary Beth Chrissis, and Marilyn Bush, Key Practices of the Capability Maturity Model, Version 1.1, Technical Report CMU/SEI-93-TR-25, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, February 1993. <http://www.sei.cmu.edu/reports/93tr025.pdf>										•	•

Reference Name	Domains										
	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber	Glossary
[SCADA AU RMF] IT Security Expert Advisory Group. *Generic SCADA Risk Management Framework For Australian Critical Infrastructure.* March 2012. <http://www.tisn.gov.au/Documents/SCADA-Generic-Risk-Management-Framework.pdf>	•									•	
[SSE-CMM] Carnegie Mellon University. *Systems Security Engineering Capability Maturity Model (SSE-CMM) Version 3.0.* June 2003. < http://www.sse-cmm.org/docs/ssecmmv3final.pdf>					•			•		•	
[Situation Awareness in Dynamic Systems] Endsley, M. *Human Factors.* "Toward a Theory of situation Awareness in Dynamic Systems." Pp. 32-64. 1995.					•	•				•	
[Supply Chain Risk Management Awareness] Jarrellann Filsinger, National Archives and Records Administration, Barbara Fast, CGI, Daniel G. Wolf, Cyber Pack Ventures, James F. X. Payne, Telecordia, Mary Anderson, Booz Allen Hamilton - February 2012. <http://www.afcea.org/committees/cyber/documents/Supplychain.pdf>	•				•			•		•	
[WH Trusted Identities in Cyberspace] The White House. *National Strategy For Trusted Identities In Cyberspace.* April 2011. <http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>			•							•	

APPENDIX B: ANNOTATED BIBLIOGRAPHY

This appendix describes key resources for each domain of the model.

Risk Management (RISK)

[DOE RMP]
The DOE *Risk Management Process* (RMP) is an electricity-utility-specific guideline for approaching the practices of a strong risk management program. This recent document references best practices and communications and contains a glossary of risk terminology.

[NIST SP800-30]
A critical practice of good risk management is an assessment of threats and vulnerabilities. The much-used NIST 800-30 guidance addresses how to perform risk assessment. Although written to guide federal agencies, businesses could also use it to address their cybersecurity.

[NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan]
NRECA offers free guides that can be used by any utility. *The Guide to Developing a Cyber Security and Risk Mitigation Plan* has a risk mitigation checklist of security activities associated with the creation of a cybersecurity plan.

[ISO 27005:2011]
This ISO document contains an overview of information systems risk management practice, including vetted practices for vulnerability assessment, threat identification, and risk assessment. As with other ISO practice documents, this document describes processes for program maturity and ongoing practices. *Note: This document is not freely available*.

[SCADA AU RMF]
This is a reference created by the Australian government as a generic business and government framework for risk management of SCADA-specific devices. It contains a number of references, examples, and a glossary that could inform any utility risk management program. It illustrates a process that mostly follows ISO 27005, as well as some of the RMP methods.

Asset, Change, and Configuration Management (ASSET)

[ISO/IEC 27002:2005]
ISO 27001/2:2005 defines best practice recommendations on information security management domains. The ISO Asset Management domain provides best practices relevant to the ASSET domain of this model as part of a holistic approach to security management. *Note: This document is not freely distributed*.

[NISTIR 7628 Vol. 1]
NISTIR 7628 Volume I (of three) presents an analytical framework that an organization can use to develop effective cybersecurity strategies for utilities looking at smart grid architecture. Much of its information on controls and best practices is derived from NIST 800-53. Sections of interest for the ASSET domain include 3.11 on configuration management.

[NERC CIP-002]
The NERC CIP standards address cybersecurity protections relevant to critical cyber assets. They present an approach to identifying and protecting utility assets. Standards of interest for the ASSET domain include NERC CIP-002.

Identity and Access Management (ACCESS)

[NISTIR 7628 Vol. 1]
Volume I of the three-volume report presents an analytical framework that organizations can use to develop effective cybersecurity strategies. The "Access Control" and "Identification and Authentication" sections are relevant to the ACCESS domain.

[NERC CIP-002, NERC CIP-004, NERC CIP-005, NERC CIP-007]
The NERC CIP standards describe cybersecurity compliance requirements for critical cyber assets. Requirements in CIP-002, CIP-004, CIP-005, and CIP-007 address items pertaining to the ACCESS domain.

[NIST SP800-53]
NIST SP 800-53 Rev. 3 describes controls for access, identification and authentication, and physical and environmental protection.

Threat and Vulnerability Management (THREAT)

[NIST SP800-40]
This NIST guideline provides detailed information on creating a patch and vulnerability management program.

[ES-ISAC]
ES-ISAC shares critical information (threat, vulnerabilities, and protective strategies) with industry participants regarding infrastructure protection. ES-ISAC works with the electricity subsector to better understand cross-industry dependencies and to account for them in emergency response planning.

[DHS ICS-CERT]
ICS-CERT, in collaboration with US-CERT, focuses on control system security, in part to share and coordinate vulnerability information and threat analysis through information products and alerts.

Situational Awareness (SITUATION)

[NIST SP800-137]
NIST SP800-137 offers guidance on the practices of continuous monitoring of federal information systems, but it can be useful for utilities and other businesses as well. The work describes how to set up a monitoring program for the entire enterprise and link it to risk management and response strategy.

[NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan]
The NRECA's cybersecurity planning guidance addresses monitoring as part of a utility's (co-op or otherwise) security planning and operational process. See pages 75, 82-85, 108-109, and 121-122. The appendixes address compliance requirements for monitoring.

[NERC RTSA]
The NERC Real-Time Tools Best Practices Task Force (RTBPTF) has created a number of documents about tools specifically designed to be used by utilities for real-time monitoring and improving security awareness. Section 2.0 is designed to help utilities choose and evaluate tools and techniques. The website http://www.nerc.com/filez/rtbptf.html has further guidance.

Information Sharing and Communications (SHARING)

[NERC Security Guideline: Information Protection]
This document provides detailed, sector-specific guidance for information sharing within and outside organizations. The guidance addresses identification, classification, labeling, security, and sharing of sensitive information.

[ES-ISAC]
ES-ISAC shares critical information (threat, vulnerabilities, and protective strategies) with industry participants regarding infrastructure protection. ES-ISAC works with the electricity subsector to better understand cross-industry dependencies and to account for them in emergency response planning.

[CEII]
FERC provides the CEII protection mechanism for energy facilities by restricting public access to information designated as CEII. Specifically, CEII is engineering, vulnerability, or detailed design information about proposed or existing (physical or virtual) critical infrastructure.

[DHS PCII]
The PCII program is an information-protection program that enhances voluntary information-sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data.

Event and Incident Response, Continuity of Operations (RESPONSE)

[NIST SP 800-40, NIST SP 800-61, NIST SP 800-82, NIST SP 800-83, NIST SP 800-86]
NIST Special Publications cover best practices and guidance on protection of information systems. The referenced Special Publications are relevant to a utility designing and implementing an incident response program or specific practices in incident detection.

[ES-ISAC]
The NERC ES-ISAC website shares critical information with industry participants regarding infrastructure protection. This is a resource for any incident response program and is particularly focused on threats to electric utilities.

[DHS ICS-CERT]
ICS-CERT, in collaboration with US-CERT, focuses on control system security, in part to share and coordinate vulnerability information and threat analysis through information products and alerts. Utilities could regularly use this resource as part of their incident awareness programs.

Supply Chain and External Dependencies Management (DEPENDENCIES)

[NRECA Security Questions for Vendors]
NRECA's Security Questions for Vendors is part of a collection of resource documents to facilitate utility security practices. *Security Questions for Vendors* provides a checklist of practices for setting up supply contracts.

[NISTIR 7622]
This NIST draft guidance document provides methods, approaches, and best practices for supply chain risk management. Although focused on federal organizations, it could inform any organization.

[MIT SCMM]
This article provides insights on practices for supply chain security. It discusses why supply chain security risks and practices require greater planning and strategy for the utility sector.

[ISO 28001:2007]
This international standard gives guidance organizations developing and implementing supply chain security processes and establishing and documenting a minimum level of security within a supply chain. *Note: This document is not freely distributed*.

[Filsinger 2012]
This white paper is on supply chain risk management as a needed practice to counter threats. The document addresses risk factors to business and government and addresses organization models such as public-private partnerships.

Workforce Management (WORKFORCE)

[NERC CIP-004]
The NERC CIP standards describe cybersecurity compliance requirements for critical cyber assets. The CIP-004 requirements address items such as personnel risk assessments, awareness, and training and are relevant to the WORKFORCE domain.

[CERT RMM, PM; CERT RMM, HRM; CERT RMM, OTA]
The People Management (PM), Human Resource Management (HRM), and Organizational Training and Awareness (OTA) process areas of the CERT-RMM describe generic goals and practices that are relevant to the WORKFORCE domain.

[NIST SP800-16, NIST SP 800-50, NIST SP 800-53, NIST SP 800-82, NIST SP 800-35]
NIST Special publications cover best practices and guidance on workforce management. For example, SP 800-53 Rev 3 describes personnel security as well as awareness and training controls, SP 800-82 describes personnel security controls from an ICS perspective, and SP 800-16 Rev 1 provides guidance on designing basic literacy or role-based training courses for workforce.

Cybersecurity Program Management (CYBER)

[NERC CIP-001, NERC CIP-002, NERC CIP-003, NERC CIP-004, NERC CIP-005, NERC CIP-006, NERC CIP-007, NERC CIP-008, NERC CIP-009]

The NERC CIP standards describe cybersecurity compliance requirements relevant to critical cyber assets. The standards include various requirements relevant to managing cybersecurity activities.

[NIST SP800-35, NIST SP800-53, NIST SP800-64, NIST SP800-82]

NIST Special publications cover best practices and guidance on cybersecurity programs, establishing and maintaining cybersecurity architecture, performing secure software development, and managing cybersecurity program management activities. For example, SP 800-53 Rev 3 describes program management controls, and SP 800-82 describes program management controls from an ICS perspective.

APPENDIX C: GLOSSARY

Term	Definition	Source
access	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	CNSSI 4009
ad hoc	In the context of this model, *ad hoc* (i.e., an ad-hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. The methods, tools, and techniques used, the priority given a particular instance of the practice, and the quality of the outcome may vary significantly depending on who is performing the practice, when it is performed, and the context of the problem being addressed. With experienced and talented personnel, high-quality outcomes may be achieved even though practices are ad-hoc. However, because lessons learned are typically not captured at the organizational level, approaches and outcomes are difficult to repeat or improve across the organization.	ES-C2M2
anomalous / anomaly	(i.e., anomalous access attempts) Inconsistent with or deviating from what is usual, normal, or expected.	Merriam-webster.com
architecture	See *cybersecurity architecture.*	
assessment	See *risk assessment.*	
asset	Something of value to the organization. Assets include many things, including technology, information, roles performed by personnel, and facilities. For the purposes of this model, assets to be considered are information technology (IT) and operations technology (OT) hardware and software assets, as well as information essential to operating the function.	
Asset, Change, and Configuration Management (ASSET)	Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.	ES-C2M2
asset owner	A person or organizational unit, internal or external to the organization, that has primary responsibility for the viability, productivity, and resilience of an organizational asset.	CERT RMM
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IT and industrial control system (ICS).	DOE RMP

Term	Definition	Source
availability	Ensuring timely and reliable access to and use of information. For an asset, the quality of being accessible to authorized users (people, processes, or devices) whenever it is needed.	DOE RMP & CERT RMM
business impact assessment	A mission impact analysis that prioritizes the impact associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets.	SP800-30
change control (change management)	A continuous process of controlling changes to information or technology assets, related infrastructure, or any aspect of services, enabling approved changes with minimum disruption.	CERT RMM
common operating picture	Activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains.	ES-C2M2
computer security incident	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet. Also, see *incident.*	NIST 800-61 (computer security incident)
confidentiality	The preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. For an information asset, confidentiality is the quality of being accessible only to authorized people, processes, and devices.	DOE RMP & Adapted from CERT RMM
configuration baseline	A documented set of specifications for an IT or OT system or asset, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time, and which should be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.	Adapted from NIST 800-53 Glossary
configuration management	A collection of activities focused on establishing and maintaining the integrity of assets, through control of the processes for initializing, changing, and monitoring the configurations of those assets throughout their lifecycle.	NIST SP 800-128
contingency plan	Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The contingency plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the continuity of operations plan or disaster recovery plan for major disruptions.	CNSSI 4009

Term	Definition	Source
controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information.	DOE RMP
critical infrastructure	Assets that provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.	HSPD-7
current	Updated at an organization-defined frequency (e.g., as in the asset inventory is kept "current") that is selected such that the risks to critical infrastructure and organization objectives associated with being out-of-date by the maximum interval between updates are acceptable the organization and its stakeholders.	ES-C2M2
cyber attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure, or for destroying the integrity of the data or stealing controlled information.	DOE RMP
cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.	DOE RMP
cybersecurity architecture	An integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, cybersecurity systems, personnel, and subordinate organizations, showing their alignment with the organization's mission and strategic plans. See *enterprise architecture.*	DOE RMP
cybersecurity event	See *event.*	
cybersecurity impact	See *impact.*	
cybersecurity incident	See *incident.*	
cybersecurity incident lifecycle	See *incident lifecycle*.	
cybersecurity plan	Formal document that provides an overview of the cybersecurity requirements for an IT and ICS and describes the cybersecurity controls in place or planned for meeting those requirements.	DOE RMP
cybersecurity policy	A set of criteria for the provision of security services.	DOE RMP
cybersecurity program strategy	A plan of action designed to achieve the performance targets that the organization sets to accomplish its mission, vision, values, and purpose.	CERT RMM

Term	Definition	Source
Cybersecurity Program Management (CYBER)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.	ES-C2M2
cybersecurity requirements	Requirements levied on an IT and OT that are derived from organizational mission and business case needs (in the context of applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, procedures) to ensure the confidentiality, integrity, and availability of the services being provided by the organization and the information being processed, stored, or transmitted.	Adapted from DOE RMP
cybersecurity responsibilities	Obligations for ensuring the organization's cybersecurity requirements are met.	ES-C2M2
cybersecurity risk	The risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS. See *risk*.	DOE RMP
cybersecurity workforce management objectives	Performance targets for personnel with cybersecurity responsibilities that the organization sets to meet cybersecurity requirements.	Adapted from CERT RMM
defined practice	A practice that is planned and executed in accordance with policy.	Adapted from CERT RMM
deprovisioning	The process of revoking or removing an identity's access to organizational assets. See also *provisioning.*	CERT RMM
domain	In the context of the model structure, a domain is a logical grouping of cybersecurity practices.	ES-C2M2
downstream dependencies	External parties dependent on the delivery of the function, such as customers and some operating partners.	ES-C2M2
electricity subsector	A portion of the energy sector that includes the generation, transmission, and distribution of electricity.	ES-SPP
enterprise	The largest (i.e., highest-level) organizational entity to which the organization participating in the ES-C2M2 survey belongs. For some participants, the organization taking the survey is the enterprise itself. See *organization.*	Adapted from SGMM v1.1 Glossary
enterprise architecture	The design and description of an enterprise's entire set of IT and OT: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.	DOE RMP (but changed ICS to OT)
entity	Something having separate or distinct existence.	Merriam-webster.com

Term	Definition	Source
establish and maintain	The development and maintenance of the object of the practice (such as a program). For example, "Establish and maintain identities" means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements.	CERT RMM
event	Any observable occurrence in a system or network. Depending on their potential impact, some events need to be escalated for response. To ensure consistency, criteria for response should align with the organization's risk criteria.	NIST 800-61
Event and Incident Response, Continuity of Operations (RESPONSE)	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.	ES-C2M2
function	Scope of the ES-C2M2 evaluation. The function is the organizational line-of-business (generation, transmission, distribution, markets, or retail) that is being evaluated by completing the model survey.	ES-C2M2
governance	An organizational process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organization is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).	Adapted from CERT RMM
identity	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	CNSSI 4009
Identity and Access Management (ACCESS)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.	ES-C2M2
impact	Negative consequence to subsector functions.	ES-C2M2
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) critical infrastructure and/or organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts. See also *computer security incident* and *event*.	Adapted from CERT RMM

Term	Definition	Source
incident lifecycle	The stages of an incident from detection to closure. Collectively, the incident lifecyle is the processes of detecting, reporting, logging, triaging, declaring, tracking, documenting, handling, coordinating, escalating and notifying, gathering and preserving evidence, and closing incidents.	Adapted from CERT RMM
information assets	Information or data that is of value to the organization, including diverse information such as operational data, intellectual property, customer information, and contracts.	Adapted from CERT RMM
information sharing	See *Information Sharing and Communications (SHARING).*	
Information Sharing and Analysis Center (ISAC)	An Information Sharing and Analysis Center (ISAC) shares critical information with industry participants regarding infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning. In particular, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) serves the electricity sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to help electricity sector participants take protective actions.	Adapted from Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website home page
Information Sharing and Communications (SHARING)	Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.	ES-C2M2
Information Technology (IT)	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate.	DOE RMP
institutionalization	The extent to which a practice or activity is ingrained into the way an organization operates. The more an activity becomes part of how an organization operates, the more likely it is that the activity will continue to be performed over time, with a consistently high level of quality. ("Incorporated into the ingrained way of doing business that an organization follows routinely as part of its corporate culture." – CERT RMM). See also *maturity indicator level.*	ES-C2M2

Term	Definition	Source
integrity	Guarding against improper information modification or destruction. Integrity includes ensuring information nonrepudiation and authenticity. For an asset, integrity is the quality of being in the condition intended by the owner and therefore continuing to be useful for the purposes intended by the owner.	DOE RMP & CERT RMM
least privilege	A security control that addresses the potential for abuse of authorized privileges. The organization employs the concept of least privilege by allowing only authorized access for users (and processes acting on behalf of users) who require it to accomplish assigned tasks in accordance with organizational missions and business functions. Organizations employ the concept of least privilege for specific duties and systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary to achieving least privilege. Organizations also apply least privilege concepts to the design, development, implementation, and operations of IT and OT systems.	Adapted from NIST 800-53,
markets	Venues where participants buy and sell products and services. In the context of this model, *markets* refers to trading involving wholesale electricity.	FERC
maturity	The extent to which an organization has institutionalized the cybersecurity practices of the model.	ES-C2M2
Maturity indicator level (MIL)	A measure of the cybersecurity maturity of an organization in a given domain of the model. The model currently defines four maturity indicator levels (MILs) and holds a fifth level in reserve for use in future versions of the model. Each of the four defined levels is designated by a number (0 through 3) and a name, for example, “MIL3: Managed.” A MIL is a measure of the progression within a domain from individual and team initiative, as a basis for carrying out cybersecurity practices, to organizational policies and procedures that institutionalize those practices, making them repeatable with a consistently high level of quality. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the core activities in the domain.	ES-C2M2
MIL0: Incomplete	A model score meaning that MIL1 has not been achieved in a domain.	ES-C2M2
MIL1: Initiated	A model score indicating that all MIL1 practices of a given domain are being performed. Practices performed at MIL1 may be ad hoc, and repeat performance may rely on the knowledge and expertise of individuals.	ES-C2M2

Term	Definition	Source
MIL2: Performed	A model score indicating that all MIL1 and MIL2 practices of a given domain are being performed. Four common practices support this progression: 1. Practices are documented. 2. Stakeholders of the practice are identified and involved. 3. Adequate resources are provided to support the process (people, funding, and tools). 4. Standards and/or guidelines have been identified to guide the implementation of the practices. The practices at MIL2 are more complete and are no longer performed irregularly in their implementation. As a result, the organization stabilizes performance of practices through management communication.	ES-C2M2
MIL3: Managed	A model score indicating that all MIL1, MIL2, and MIL3 practices of a given domain are being performed. At MIL3, the activities in a domain have been further institutionalized and are now being managed. Four common practices support this progression: 1. Activities are guided by policies (or other organizational directives) and governance. 2. Activities are periodically reviewed to ensure they conform to policy. 3. Responsibility and authority for performing the practice is clearly assigned to personnel. 4. Personnel performing the practice have adequate skills and knowledge.	ES-C2M2
MILX	A maturity indicator level that is reserved for future use.	ES-C2M2
monitoring	Collecting, recording, and distributing information about the behavior and activities of systems and persons to support the continuous process of identifying and analyzing risks to organizational assets and critical infrastructure that could adversely affect the operation and delivery of services.	Adapted from CERT RMM (monitoring, and risk management)
monitoring requirements	The requirements established to determine the information gathering and distribution needs of stakeholders.	CERT RMM

Term	Definition	Source
operating picture	Real-time (or near-real-time) awareness of the operating state of a system or function. An operating picture is formed from data collected from various trusted information sources that may be internal or external to the system or function (e.g., voltage, current, temperature, weather events and warnings, cybersecurity alerts, status information from interconnects). The operating picture may or may not be presented graphically. It involves the collection, analysis (including fusion), and distribution of what is important to know to make decisions about the operation of the system. A common operating picture (COP) is a single operating picture that is available to the stakeholders of the system or function so that all stakeholders can make decisions based on the same reported operating state. See common operating picture.	ES-C2M2
operating states	See *pre-defined states of operation*.	ES-C2M2
operational risk	The potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events. In the context of this model, our focus is on operational risk from cybersecurity threats.	Adapted from CERT RMM
operational risk taxonomy	The collection and cataloging of common operational risks that the organization is subject to and must manage. The risk taxonomy is a means for communicating these risks and for developing mitigation actions specific to an organizational unit or line-of-business if operational assets and services are affected by them.	CERT RMM
Operations Technology (OT)	In this model, operations technology (OT) is synonymous with industrial control systems (ICS).	
organization	An electricity subsector organization of any size, complexity, or positioning within an organizational structure that is charged with carrying out assigned mission and business processes and that uses IT and OT (i.e., ICS) in support of those processes. In the context of the model, the organization is the entity using the model or that is under examination.	Adapted from DOE RMP
periodic review / activity	A review or activity that occurs at specified, regular time intervals, where the organization-defined frequency is commensurate with risks to organizational objectives and critical infrastructure.	Adapted from SEI CMM Glossary

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

Term	Definition	Source
risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.	DOE RMP
risk analysis	See *risk assessment*.	
risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation, resulting from the operation of an IT and ICS.	DOE RMP
risk criteria	Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on areas of impact.	CERT RMM (risk measurement criteria)
risk designation, as in "position risk designation"	"Risk designation. Agency heads must designate every covered position within the agency at a high, moderate, or low risk level as determined by the position's potential for adverse impact to the efficiency or integrity of the service."	OPM
risk disposition	A statement of the organization's intention for addressing an operational risk. Typically limited to "accept," "transfer," "research," or "mitigate."	CERT RMM
risk management	The program and supporting processes to manage cybersecurity risk to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation. It includes (1) establishing the context for risk-related activities, (2) assessing risk, (3) responding to risk once determined, and (4) monitoring risk over time.	DOE RMP
Risk Management (RISK)	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.	ES-C2M2
risk management strategy	Strategic-level decisions on how senior executives manage risk to an organization's operations, resources, and other organizations.	DOE RMP
risk mitigation	Prioritizing, evaluating, and implementing appropriate risk-reducing controls.	DOE RMP
risk mitigation plan	A strategy for mitigating risk that seeks to minimize the risk to an acceptable level.	CERT RMM
risk parameter / risk parameter factors	Organization-specific risk tolerances used for consistent measurement of risk across the organization. Risk parameters include risk tolerances and risk measurement criteria.	CERT RMM
risk register	A structured repository where identified risks are recorded to support risk management.	ES-C2M2
risk response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, resources, and other organizations.	DOE RMP
risk taxonomy	See *operational risk taxonomy*.	

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

Term	Definition	Source
sponsorship	Enterprise-wide support of cybersecurity objectives by senior management as demonstrated by formal policy or by declarations of management's commitment to the cybersecurity program along with provision of resources. Senior management monitors the performance and execution of the cybersecurity program and is actively involved in the ongoing improvement of all aspects of the cybersecurity program.	ES-C2M2
states of operation	See *pre-defined states of operation.*	
supply chain	The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. The supply chain encompasses the full product lifecycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain.	NISTIR 7622 Source of 1st paragraph cited as [NDIA ESA]
Supply Chain and External Dependencies Management (DEPENDENCIES)	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.	ES-C2M2
threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through IT, OT, or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	Adapted from DOE RMP
Threat and Vulnerability Management (THREAT)	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.	ES-C2M2
threat assessment	The process of evaluating the severity of threat to an IT and ICS or organization and describing the nature of the threat.	DOE RMP
threat profile	A characterization of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT and OT of an organization and to the organization itself, delineating the feasible threats, describing the nature of the threats, and evaluating their severity.	ES-C2M2

Term	Definition	Source
threat source	An intent and method targeted at the intentional exploitation of a vulnerability or a situation, or a method that may accidentally exploit a vulnerability.	DOE RMP
upstream dependencies	External parties on which the delivery of the function depends, including suppliers and some operating partners.	ES-C2M2
validate	Collect and evaluate evidence to confirm or establish the quality of something (e.g., information, a model, a product, a system, or component) with respect to its fitness for a particular purpose.	ES-C2M2
vulnerability	A cybersecurity vulnerability is a weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat source. A *vulnerability* class is a grouping of common vulnerabilities.	Adapted from NISTIR 7628 Vol. 1, pp. 8
vulnerability assessment	Systematic examination of an IT and ICS or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.	DOE RMP
Workforce Management (WORKFORCE)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.	ES-C2M2
workforce management objectives	See *cybersecurity workforce management objectives.*	

APPENDIX D: ACRONYMS

ACCESS	Identity and Access Management domain
AMI	Advanced Metering Infrastructure
ASSET	Asset, Change, and Configuration Management domain
CATF	Cyber Attack Task Force
CERT®-RMM	CERT® Resilience Management Model
CIP	Critical Infrastructure Protection
COP	common operating picture
COTS	commercial off-the-shelf
CRPA	Cyber Risk Preparedness Assessment
CVSS	Common Vulnerability Scoring System
CYBER	Cybersecurity Program Management domain
DEPENDENCIES	Supply Chain and External Dependencies Management domain
DHS	Department of Homeland Security
DOE	Department of Energy
DOE-OE	Department of Energy, Office of Electricity Delivery and Energy Reliability
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
EU	European Union
FERC	Federal Energy Regulatory Commission
GWAC	GridWise Architecture Council
HR	human resources
IAM	identity and access management
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICSJWG	Industrial Control Systems Joint Working Group
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
IT	Information Technology

MIL	maturity indicator level
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operations Technology
RAWG	Reference Architecture Working Group
RESPONSE	Event and Incident Response, Continuity of Operations domain
RISK	Risk Management domain
RMP	Electricity Subsector Cybersecurity Risk Management Process
SCADA	supervisory control and data acquisition
SEI	Software Engineering Institute
SGIP	Smart Grid Interoperability Panel
SHARING	Information Sharing and Communications domain
SITUATION	Situational Awareness domain
SLA	Service Level Agreement
SME	subject matter expert
THREAT	Threat and Vulnerability Management domain
US-CERT	United States Computer Emergency Readiness Team
WORKFORCE	Workforce Management domain

APPENDIX E: RELATED INITIATIVES

The model builds upon and ties together a number of existing cybersecurity resources and initiatives. Listed below are the key related initiatives that were referenced by the team during the development of the model.

CERT® Resilience Management Model (CERT®-RMM), Carnegie Mellon Software Engineering Institute

The CERT Resilience Management Model is the foundation for a process improvement approach to security, business continuity, and aspects of IT operations management. It establishes an organization's resilience management process: a collection of essential capabilities that the organization performs to ensure that its important assets stay productive in supporting business processes and services [CERT RMM].

(Supports the following domains: RISK, ASSET, ACCESS, THREAT, SITUATION, SHARING, REPONSE, DEPENDENCIES, WORKFORCE, and CYBER)

Cross-Sector Roadmap to Secure Control Systems, Department of Homeland Security

The Cross-Sector Roadmap to Secure Control Systems describes a plan for voluntarily improving cybersecurity across all critical infrastructure/key resources (CIKR's) that employ industrial control systems [DHS Cross-Sector Roadmap].

(Supports the following domains: RISK, THREAT, SITUATION, SHARING, REPONSE, DEPENDENCIES, WORKFORCE, and CYBER)

Cyber Attack Task Force Final Report, North American Electric Reliability Corporation

The Cyber Attack Task Force (CATF) Final Report profiles the elements of a coordinated cyber attack and provides measures for preventing, detecting, and responding to various types of attacks. The CATF provides recommendations for deterring a coordinated cyber attack and improving the resiliency of the bulk power system [NERC CATF].

(Supports the following domains: THREAT, SITUATION, SHARING, and REPONSE)

Cyber Risk Preparedness Assessment, North American Electric Reliability Corporation

The Cyber Risk Preparedness Assessment (CRPA) provides bulk power system entities with a program for assessing the cyber resiliency capabilities. The CRPA evaluates the cybersecurity posture of bulk power system entities based on seven performance areas: Vulnerability Management Process; Cybersecurity Management; Information Sharing and Communications; Supply Chain Language; Security Awareness Training; Technical Measures for Deterence, Detection, and Defend; Incident Response Planning and Execution [NERC CRPA].

(Supports the following domains: THREAT, SITUATION, SHARING, REPONSE, DEPENDENCIES, WORKFORCE, and CYBER)

Cybersecurity Risk Management Process, Department of Energy

The Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline provides a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector. This guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures. [DOE RMP]

(Supports the following domain: RISK and CYBER)

Department of Homeland Security: Cybersecurity Procurement Language for Control Systems, Department of Homeland Security

The Cybersecurity Procurement Language for Control Systems summarizes security principles to be considered when designing and procuring control systems products and services, and provides example language to incorporate into procurement specifications [DHS Procurement].

(Supports the following domain: DEPENDENCIES)

Guide to Developing a Cyber Security and Risk Mitigation Plan, NRECA / Cooperative Research Network

As part of a Smart Grid Investment Grant from the American Reinvestment and Recovery Act, the NRECA developed the Guide to Developing a Cyber Security and Risk Mitigation Plan. The guide aims to improve an organization's security posture through a risk based approach that provides cybersecurity controls and practices tied to specific categories of physical and cyber risks [NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan].

(Supports the following domains: RISK, ASSET, ACCESS, THREAT, SITUATION, SHARING, REPONSE, DEPENDENCIES, WORKFORCE, and CYBER)

NESCOR Electric Sector Representative Failure Scenarios by Domain

This document includes a set of cybersecurity failure scenarios that affect the reliability of the electric grid. The failure scenarios are grouped into the following domains: Advanced Metering Infrastructure (AMI), Distributed Energy Resources (DER), WAMPAC (Wide Area Monitoring, Protection, and Control), Electric Transportation (ET), Demand Response (DR), Distribution Grid Management (DGM), and Generic. The document identifies the relevant vulnerabilities, impacts, and potential mitigations for each failure scenario [NESCOR Failure Scenarios].

(Supports the following domains: ASSET, ACCESS, THREAT, SITUATION, SHARING, REPONSE, DEPENDENCIES, and WORKFORCE)

NIST IR 7628 – Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology

The three-volume report, NISTIR 7628, Guidelines for Smart Grid Cyber Security, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities [NISTIR 7628 Vol. 1, NISTIR 7628 Vol. 3].

(Supports the following domains: RISK, ASSET, ACCESS, THREAT, REPONSE, WORKFORCE, and CYBER)

Roadmap to Achieve Energy Delivery Systems Cybersecurity, Department of Energy

The Roadmap to Achieve Energy Delivery Systems Cybersecurity provides a plan to improve the cybersecurity of the energy sector. The strategic framework within the roadmap presents the vision for energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade [DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity].

(Supports the following domains: RISK, THREAT, RESPONSE, DEPENDENCIES, WORKFORCE, and CYBER)

Security Logging in the Utility Sector: Roadmap to Improved Maturity, National Electric Sector Cybersecurity Organization and Southern California Edison

The Roadmap to Improved Maturity provides a capability maturity model for security logging and monitoring for electric sector utilities. The capability maturity model provides a six-level model for assessing critical aspects of security logging and monitoring and includes data sources that organizations should consider logging [NESCO Logging].

(Supports the following domains: THREAT, SITUATION, and REPONSE)

Smart Grid Maturity Model (SGMM), Carnegie Mellon Software Engineering Institute

The Smart Grid Maturity Model (SGMM) is a management tool that utilities can leverage to plan their smart grid journeys, prioritize their options, and measure their progress as they move toward the realization of a smart grid [CERT SGMM].

(Supports the following domains: ASSET, SITUATION, SHARING, DEPENDENCIES, WORKFORCE, and CYBER)

NOTICES

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

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

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.