Sol-ReMM Solar Resiliency Maturity Model

DRAFT

SOLAR CYBERSECURITY RESILIENCE MATURITY MODEL (Sol-REMM) Primary User Guide



Version 1.0

Dec. 2024

Pacific Northwest NATIONAL LABORATORY

SOLAR ENERGY TECHNOLOGIES OFFICE U.S. Department Of Energy

TABLE OF CONTENTS

ACKNOWLEDGMENTS iv
CAUTIONARY NOTE vi
Intended Scope and Use of This Publication vi
1. INTRODUCTION 1
1.1 Intended Audience 2
1.2 Document Organization 2
2. BACKGROUND 4
3. CORE CONCEPTS 5
3.1 Maturity Models 5
3.2 Enterprise, Organization, and Function 5
3.3 Assets 7
3.3.1 IT Assets, OT Assets, and Information Assets 7
3.3.2 Additional Asset Subgroupings 8
4. MODEL ARCHITECTURE 10
4.1 Domains, Objectives, and Practices 10
4.2 Maturity Indicator Levels 14
4.3 Progression 16
4.4 Enterprise-Focused Domains 17
4.5 Considerations for the Cybersecurity Architecture Domain 17
4.5.1 Cybersecurity Architecture Defined 17
4.5.2 Cybersecurity Architecture Framework 17
4.5.3 Implementing the Cybersecurity Architecture 18
4.5.4 Considering the Cybersecurity Architecture in Sol-ReMM 18
4.6 Example Lists Included in Practices 19
4.7 Practice Reference Notation 19
5. USING THE MODEL 20
5.1 Step 1: Perform a Self-Evaluation 20
5.2 Step 2: Analyze Identified Gaps 21
5.3 Step 3: Prioritize and Plan 22
5.4 Step 4: Implement Plans and Periodically Reevaluate 22

6. MODEL DOMAINS 24
6.1 Asset Inventory Management (INVENTORY) 24
6.2 Asset Configuration and Change Management (CHANGE-MGMT) 27
6.3 Access and Authorization Management (ACCESS) 30
6.4 Threat and Vulnerability Management (THREAT) 34
6.5 Risk Assessments and Management (RISK) 37
6.6 Supply Chain Management (SUPPLY-CHAIN) 41
6.7 Procurement Process (PROCUREMENT) 45
6.8 Cybersecurity Architecture (CYBER-ARCH) 47
6.9 Workforce Management (WORKFORCE) 51
6.10 Situational Awareness (AWARENESS) 55
6.11 Event and Incident Response (RESPONSE) 58
6.12 Resilience Program Management (PROG-MGMT) 62

LIST OF FIGURES

Figure 1: Example of the Structure of a Notional Entity 6
Figure 2: Model and Domain Elements 10
Figure 3: Example List Included in Practice ASSET-1e 19
Figure 4: Potential Approach for Using the Model 20

TABLE OF CONTENTS

LIST OF TABLES

Table 1: Examples of IT Assets, OT Assets, and Information Assets 9
Table 2: Description of Self-Evaluation Response Options 14
Table 3: Summary of Maturity Indicator Levels 15
Table 4: Inputs, Activities, and Outputs: Breakdown of Potential Approach..... 23

ACKNOWLEDGMENTS

This Solar Cybersecurity Resilience Maturity Model (Sol-ReMM) was sponsored by the United States Department of Energy Solar Energy Technologies Office (SETO).

The authors of this Sol-ReMM user guide are Cliff Glantz, Scott Mix, Joseph Loftus, Edward Nguyen, Robert Harrington, Brian Dean, Grace McNally, Caleb Ng, Julian Martinov, Angelica Vargas, Isabella Hessler, Varun Sabbineni, Advaitha Motkuri, Anish Yenduri, Viru Repalle, and Eric Zegzula.

The team at PNNL supporting the production of Sol-ReMM includes:

- Clifford Glantz (Project manager)
- Scott Mix (Project manager)
- Joseph Loftus (Programming lead)
- Brian Dean
- Robert Harrington
- Edward Nguyen
- Grace McNally
- Jesus Fernandez
- Garrett Fuchs
- Avinash Joshi
- Thomas Joppich
- Gwendolyn Kidd
- Christopher McCall
- Jun Nguyen
- Patricia Prison
- Dylan Wright-Mockler
- Aiden Arends
- Angelica Vargas Escobar
- Tobiah Goetz
- Kidist Gustafsson
- Isabella Hessler
- Julian Martinov
- Xylan Moon
- Advaitha Motkuri
- Caleb Ng
- Amy Pollom
- Viru Repalle
- Varun Sabbineni
- Vladyslav Tsepenok
- Anish Yenduri
- Eric Zegzula

The authors are grateful for the assistance provided by Marissa Morales-Rodriguez (DOE SETO), Aris Riepnieks (PNNL), and Shuchismita Biswas (PNNL).

Sol-ReMM is based on the C2M2 Version 2.1 maturity modeling framework developed by PNNL and our many project partners under the sponsorship and guidance of the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Information on C2M2 Version 2.1 is available at https://C2M2.doe.gov and https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

This user guide is based on the C2M2 Version 2.1 guidance document. Contributors to the C2M2 user guide included representatives from DOE, PNNL, Axio, Nexight, Carnegie Mellon University, and others. Key individuals included Fowad Muneer, Lindsay Kishter, Brian Benestelli, Richard Caralli, Pamela Curtis, John Fry, Paul Skare, Clifford Glantz, Cynthia Hsu, Annabelle Lee, Julia Mullaney, David White, and Ryan Subers.

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 resilience and cybersecurity practices often associated with information technology (IT) and operations technology (OT) assets and the environments in which they operate. This guidance is not intended to replace or subsume other resilience- or cybersecurity-related activities, programs, processes, or approaches that organizations have implemented or intend to implement, including any resilience or cybersecurity activities associated with legislation, regulations, 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 resilience and cybersecurity program. Although it is anticipated that entities subject to compliance requirements would use this model, compliance requirements are not altered in any way by this model. Please consult your compliance authority for any questions on regulatory compliance.

1. INTRODUCTION

The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of a natural and human-caused threats. The solar energy sector is a component of our energy infrastructure.

The solar energy sector is facing a range of threats to its functionality that are either new or more severe than experienced in earlier years, including more frequent and more severe cyberattacks, extreme weather events, wildfires, droughts, physical attacks. The increasing frequency and severity of these threats implies that parts of our solar energy infrastructure may need to be hardened or strengthened and resilience capabilities and planning may need to be reassessed.

The Solar Cybersecurity and Resilience Maturity Model (Sol-ReMM) is a tool that solar energy organizations and facilities can use to self-evaluate the resilience of their systems and components against natural and human-caused threats, with an emphasis on cybersecurity threats. Solar organizations can use the model to make more informed decisions about cybersecurity- and resilience-related policies, programs, and investments.

The Sol-ReMM was developed to address the unique characteristics of solar energy stakeholders. The model can enable users to:

- Evaluate and benchmark their organization's cybersecurity and resilience capabilities.,
- Prioritize actions and investments to improve the cybersecurity and resilience of their systems.
- Share cybersecurity and resilience -related knowledge, best practices, and relevant references as a means to improve resilience capabilities.
- Contribute to increasing the overall resilience of the Nation's energy systems.

The Sol-ReMM is offered as an online tool that maintains all data on the users' computer, All model output is also generated on the user's computer using instructions provided by the Sol-ReMM server. No data or model output is ever shared with the Sol-ReMM server in order to preserve the security and privacy of user data. A self-evaluation using the Sol-ReMM can be completed in as little as one day or it can be spread out over week or more to permit the unhurried scheduling and participation of diverse subject matter experts.

The Sol-ReMM provides descriptive rather than prescriptive guidance. The model content is presented at a high level of abstraction so that it can be applied by solar sector organizations of various types, structures, sizes, and locations. Broad use of the model within the sector can support the voluntary benchmarking of the sector's solar cybersecurity and resilience capabilities.

1.1 Intended Audience

Within an organization, various stakeholders may benefit from a Sol-ReMM self-evaluation. This document specifically targets people in the following organizational roles:

- Decision makers (executives) who control the allocation of resources and the management of risk in their organizations; these are typically senior leaders
- Leaders with responsibility for managing organizational resources and operations associated with the domains of this model (See Section 4.1 for more information on the content of each Sol-ReMM domain.)
- Practitioners with responsibility for supporting the organization in the use of the model (planning and managing changes in the organization based on the model)
- Facilitators with responsibility for leading a self-evaluation of the organization based on the model and an evaluation tool and analyzing the self-evaluation results[1]

1.2 Document Organization

This document, along with several others, supports organizations in the effective use of the Sol-ReMM. It introduces the model and provides the Sol-ReMM's main structure and content.

- Section 2: Introduces the model and details the model's purpose, intended audience, and the organization of the content within this document.
- Section 3: Describes several core concepts that are important for interpreting the content and structure of the Sol-ReMM .
- Section 4: Describes the architecture of Sol-ReMM.
- Section 5: Provides guidance on how to use the model.
- Section 6: Contains the model itself—its domains, objectives and, practices, organized into domains.
- Appendix A: Includes references that either were used in the development of this document or that provide further information.
- Appendix B: Provides definitions for terms used in Sol-ReMM.
- Appendix C: Defines the acronyms used in this document.

[1] For more information about the facilitator role, refer to the *Sol-ReMM Self-Evaluation Process Guide* which may be downloaded from the Sol-ReMM Nuclear "Resources" webpage.

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

- Decision makers: Sections 1, 2, and 3
- Leaders or managers: Sections 1, 2, 3, and 4
- Practitioners and Facilitators: Entire document

2. BACKGROUND

The original maturity modeling technical approach that unpins Sol-ReMM was first released in the Cybersecurity Capability Maturity Model (C2M2) in 2012. The C2M2 was updated to:

- Version 1.1 in 2014 in support of the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, an initiative led by the U.S. Department of Energy (DOE) in partnership with the U,S, Department of Homeland Security (DHS) and in collaboration with industry, private- sector, and public-sector experts.
- Version 2.0 in 2021 to build upon existing efforts, models, and cybersecurity best practices to advance the model and address new technologies, practices, and changes in the threat environment. This version improved model usability and introduced user-friendly online tools and expanded data analytics capabilities.
- Version 2.1 in 2022. This made some enhancement to the model practices and usability.

Up-to-date Information on C2M2 Version 2.1 is available at https://C2M2.doe.gov and https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

Sol-ReMM development began in late 2023 and continued throughout 2024. It uses the C2M2 methodology and programming framework. Its development to focus on solar sector applications was led by representatives of the U.S DOE's Pacific Northwest National Laboratory (PNNL). The PNNL project team developed the Sol-ReMM's Domains, Objectives, and Practices; performed the code development of the Sol-ReMM website and online tool; and hosts the Sol-ReMM server.

The development and implementation of Sol-ReMM is sponsored by DOE's Solar Energy Technologies Office (SETO). SETO works to:

- Drive innovation in technology and soft cost reduction to make solar affordable and accessible for all Americans.
- Enable solar to support the reliability, resilience, and security of the grid.

  Create a sustainable industry that supports job growth, manufacturing, and the circular economy in a wide range of applications.to help build or improve nuclear security capabilities (https://www.energy.gov/eere/solar/goals-solar-energy-technologies-office).

3. CORE CONCEPTS

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

3.1 Maturity Models

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

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

To measure progression, maturity models typically have a scale defining levels of maturity. Sol-ReMM uses a scale of maturity indicator levels (MILs) ranging from 0 to 3, which are described in Section 4.2. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scale to:

- Define its current state.
- Determine its future, more mature state.
- Identify the capabilities it must attain to reach that future state.

3.2 Enterprise, Organization, and Function

The terms *enterprise*, *organization*, and *function* identify which part of an entity the text of the model is referring to. *Function* refers to the part of an entity to which the Sol-ReMM will be applied (as described further in Section 3.2.1). *Organization* is a higher-level administrative unit in which the function resides (e.g., an operating company). *Enterprise* refers to the highest-level administrative unit within an entity using the Sol-ReMM (e.g., a parent company).

It is also important to consider that the Sol-ReMM was designed to apply to a wide variety of entity types. Some enterprises may consist of multiple organizations (e.g., a holding

company with multiple operating companies); other organizations may have a more homogenous structure that does not necessitate any differentiation between the terms *enterprise* and *organization*. For those organizations, *enterprise* and *organization* may be used interchangeably. Figure 1 depicts how the enterprise, organization, and function may be organized in a notional entity.

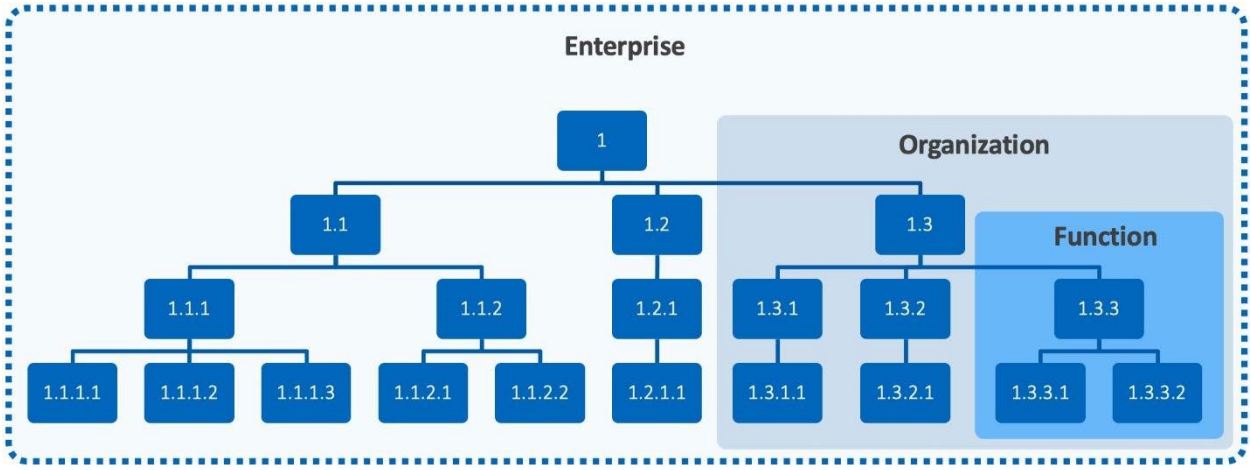


Figure 1: Example of the Structure of a Notional Entity

In the model, the term *function* refers to the part of the organization that is being evaluated based on the model. It is common for an organization to use the model to evaluate a subset of its operations. The model broadly defines the function to allow organizations the greatest degree of flexibility in determining the scope of the self-evaluation that is appropriate for them. Functions can align with organizational boundaries, or they can align to a single product line or system. They might include departments; lines of business; distinct facilities; network security zones; groupings of assets; or assets, processes and resources managed externally, such as assets that reside in the cloud.

Selection of the function defines which assets will be in scope for the evaluation including interconnected or interdependent business, operations, and technology systems and the environment in which they operate. The function also defines the people who should participate in the self-evaluation. Specifically, appropriate participants should be included to ensure there is someone familiar with the way that the activities described in each of the Sol-ReMM domains are implemented for the selected function.

Picking the right scope improves the accuracy of self-evaluation results. Care should be given to select a scope that provides a good balance between accuracy and time spent performing individual self-evaluations. A general rule for finding the right balance is to identify the fewest number of self-evaluations that still provides an accurate picture of the organization's solar-related cybersecurity and resilience practices.

3.3 Assets

Many Sol-ReMM practices refer to *assets*. For the purposes of the Sol-ReMM tool, the term *assets* include all assets within the selected function, including interconnected or interdependent business, operations, and technology systems and the environment in which they operate. This may also include virtualized assets, regulated assets, cloud assets, and mobile assets. Additionally, this may include assets managed by a third party, software as a service, platform as a service, and infrastructure as a service, as well as public, private, or hybrid cloud assets.

3.3.1 IT Assets, OT Assets, and Information Assets

The Sol-ReMM uses the following definitions when referring to information technology (IT), operational technology (OT) assets, and information assets:

- IT assets: 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 interdependent business and technology systems and the environment in which they operate.
- OT assets: OT assets refer to assets that are on the OT segment of the organization's network and are necessary for service delivery or production activities. Most modern control systems include assets traditionally referred to as IT, such as workstations that use standard operating systems, database servers, or domain controllers.
- Information assets: Any communication or representation of knowledge such as facts, data, or opinions that is of value to the organization. Information Assets may be in any media or form, including digital or non-digital.

Table 1 provides examples of IT assets, OT assets, and Information assets.

Table 1: Examples of IT Assets, OT Assets, and Information Assets

Examples of IT Assets	Examples of OT Assets	Examples of Information Assets
▪ Workstations ▪ Switches, routers, and firewalls ▪ Servers ▪ Virtual machines ▪ Software ▪ Mobile computing devices ▪ Cloud assets	▪ Workstations ▪ Switches, routers, and firewalls ▪ Servers ▪ Virtual machines ▪ Software ▪ Mobile computing devices ▪ Cloud assets ▪ Programmable Logic Controllers ▪ Remote Terminal Units ▪ Industrial Control Systems (ICS) ▪ Safety Instrumented Systems ▪ Physical access control devices	▪ Business data ▪ Intellectual property ▪ Customer information ▪ Contracts ▪ Security logs ▪ Metadata ▪ Set points ▪ Operational data ▪ Financial records ▪ Security information and event management log files ▪ Historian data ▪ Configuration files

3.3.2 Additional Asset Subgroupings

In some cases, Sol-ReMM practices refer to specific subgroupings of assets. These subgroupings focus on importance to the function and potential impact if accessed or misused by a threat actor. They may include any combination of assets. These subgroupings are defined as:

- Assets that are important to the delivery of the function: Assets that are required for a normal state of operation of the function and output of the function's products or services. Loss of an asset that is considered important to the delivery of the function may not directly result in an inability to deliver the function but could result in operations being degraded. Identification of an important asset should focus on loss of the service or role performed by that asset and should not include consideration of asset redundancy or other protections applied to assets.

- Assets within the function that may be leveraged to achieve a threat outcome: Assets that may be used in the pursuit of the tactics or goals of a human-caused threat that are of concern to the organization. Identifying assets within the function that may be leveraged to achieve a threat enables the organization to view assets from the perspective of a threat actor. Examples of assets within the function that may be leveraged to accomplish a threat include:
  - assets that are important to delivery of the function
  - public-facing assets that may serve as an initial access point
  - assets that, if compromised, may allow lateral movement within an organization's network
  - assets with administrative rights that would enable privilege escalation
  - information assets such as personally identifiable information that may cause harm to the organization or its stakeholders if lost, stolen, or disclosed.

  A threat actor is any individual or group with the potential to adversely impact organizational operations. Threat outcomes are the potential goals of threat actor activities that are of concern because they would have negative impacts on the organization. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage.

  Threat actors may leverage multiple tactics or techniques, like those defined in MITRE ATT&CK [MITRE ATT&CK] or MITRE ATT&CK for Industrial Control Systems [MITRE ATT&CK for ICS]), to achieve their goals. Threat goals may be described in an organization's threat profile and may change over time or in different situations. Examples include data manipulation or theft, damage to property, denial of control, loss of safety, or operational outage.

  Note that an organization's inventory of assets that are important to the delivery of the function might include assets within the function that may be leveraged to achieve a threat outcome and vice versa. It is not the intention of the model that all assets be categorized as assets that might be leveraged to achieve by a , but only those that a risk-based approach identifies as being worthy of attention and further analysis.

- All assets within the function: All assets that operate or are used within the function. These assets may not be considered important to the delivery of the function and may not be likely to be leveraged to achieve a threat (for example, printers, radios, badge readers, or telephones).

4. MODEL ARCHITECTURE

The model is organized into 12 domains. Figure 2 illustrates the model structure. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objective. Objectives are target achievements that support the domain. Within each objective, practices are provided to evaluate performance at three different maturity indicator levels (MILs).

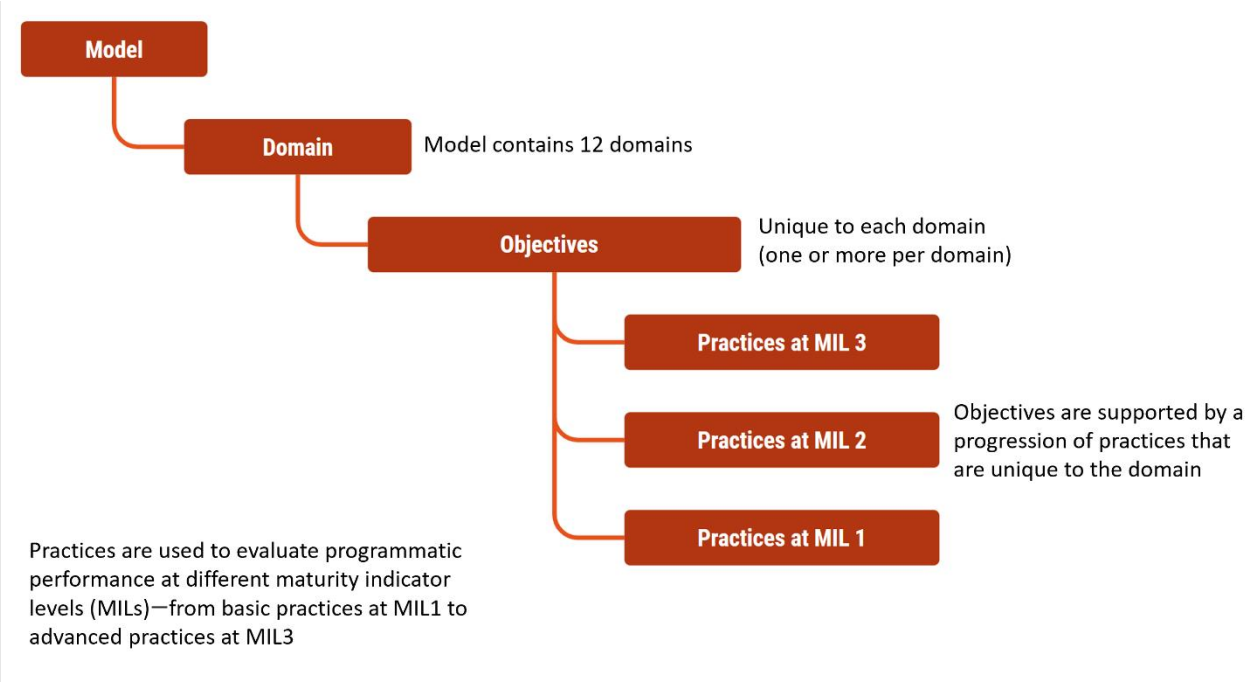


Figure 2: Model and Domain Elements

4.1 Domains, Objectives, and Practices

For each domain, the model provides a purpose statement, which is a high-level summary of the intent of the domain and introductory notes providing more context. The purpose statement for each of the 12 domains follows in the order in which the domains appear in the model. Next to each of the domain names, a short name is provided that is used throughout the model.

Asset Inventory (ASSET)

Inventory the organization's critical assets including information technology (IT) and operations technology (OT) assets. Consider both hardware and software assets. The need for an inventory of certain assets should be commensurate with the risk to operational resilience and goals. The inventory should be maintained throughout the lifecycle of the assets.

Asset Configuration and Change Management (CHANGE-MGMT)

Manage the configuration and change management program for the organization's critical assets including information technology (IT), operations technology (OT), and information assets. Change management is the process of managing the changes that are made to configurable assets. This includes proposed addition, deletion, or modification of any asset in a system. Configuration management establishes and maintains processes for initializing, changing, and monitoring the configurations of assets throughout their life cycle, Asset configurations are aligned with organizational requirements and resilience best practices. Changes to assets are systematically evaluated, approved, and documented to maintain asset integrity and operational resilience.

Access and Authorization Management (ACCESS)

Create and manage processes for handling identities, credentials, and access controls to the organization's assets. Personnel, devices, and services are authorized based on documented procedures and robust mechanisms for identity provisioning, credential management, and access control. Align these processes with organizational security requirements and resilience best practices.

Threat and Vulnerability Management (THREAT)

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to resilience and cybersecurity threats and vulnerabilities, Threat and vulnerability management should be commensurate with the risk to the organization's operations and goals.

Risk Assessment and Management (RISK)

Establish and maintain a resilience and cybersecurity risk management program to identify, assess, prioritize, and address risks. Risk management should

consider both natural and human-caused threats to resilience. The program documents processes, integrates stakeholder input, and aligns with organizational goals to effectively manage and mitigate risks.

Supply Chain Management (SUPPLY)

Establish and manage relationships with key suppliers to ensure resilience and security in the supply chain, including evaluation, performance oversight, and backup arrangements. Regularly review and update practices to align with policies, industry best practices, and evolving conditions.

Procurement Process (PROCURE)

Establish and manage a procurement process that incorporates cybersecurity and resilience considerations to obtain products and services that meet security requirements and support operational continuity. This includes documenting procurement procedures, integrating cybersecurity and resilience into contracts, and including stakeholder engagement. Regular reviews and adherence to best practices are crucial for maintaining an effective procurement program.

Cybersecurity Architecture (ARCHITECTURE)

Design and maintain the organization's cybersecurity configurations, security controls, and cybersecurity processes in alignment with resilience and cybersecurity requirements and risk tolerance. A key focus should be network and system integrity. Regularly review and adjust these elements to address risk and support organizational objectives.

Workforce Management (WORKFORCE)

Develop and manage plans and procedures to allow the workforce to be well-prepared and competent in handling resilience and cybersecurity events. This includes defining roles and responsibilities, providing necessary training and tools, and fostering a culture of resilience and cybersecurity awareness, all aligned with organizational risk tolerance and goals. Regular programmatic reviews and updates maintain workforce readiness and effectiveness.

Situational Awareness (SITUATION)

Develop and maintain a framework for situational awareness that integrates activities and technologies to collect, analyze, and communicate operational and

cybersecurity information. This includes implementing comprehensive logging, evaluating log data, and consolidating monitoring information into a Common Operating Picture (COP). Ensure the framework supports real-time operations and resilience objectives, with regular updates and resources aligned with organizational risks and best practices.

Event and Incident Response, Continuity of Operations (RESPONSE)

Establish, maintain, and exercise plans, procedures, and technologies to detect, analyze, respond to, and recover from resilience-challenging events and incidents. This includes the ability to respond to natural and human-caused events. This program is designed to maintain continuity of operations and be regularly reviewed and updated to address evolving threats and organizational needs, aligning with resilience risks and goals.

Resilience Program Management (PROGRAM)

Establish and manage a comprehensive resilience and cybersecurity program that aligns with the organization's overall strategy and operational goals, providing an appropriate level of preparedness for, and recovery from, resilience-challenging events. This includes integrating strategic planning, governance, and regular updates to address evolving threats and organizational needs, while maintaining alignment with resilience, cybersecurity, and operational objectives.

The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the *Asset Inventory Management* domain comprises four objectives:

1. Manage IT Asset Inventory
2. Manage OT Asset Inventory
3. Manage Information Asset Inventory
4. Management Activities

Each of the objectives in a domain comprises a set of practices.

Practices represent the activities an organization can perform to establish and mature capability in the domain. For example, the *Asset Inventory Management* domain is a group of practices that an organization can perform to establish and mature asset management, change management, and configuration management capabilities.

Each individual practice is associated with a given MIL. The performance of the practices is evaluated by subject matter experts. Four potential evaluation scores may be considered when evaluating the performance of each practice. These four implementation scores are "Fully Implemented", "Largely Implemented", "Partially Implemented", and "Not Implemented". These implementation scores are described in Table 2.

Table 2: Description of Self-Evaluation Response Options

Response	Description
Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete; there are multiple opportunities for improvement
Not Implemented	Absent; the practice is not performed by the organization

Each Objective has at least one practice and as many as six practices that evaluate performance at each MIL (i.e., MIL1, MIL2, and MIL3). The Sol-ReMM includes a total of 451 practices grouped into 12 domains.

4.2 Maturity Indicator Levels

The model defines four maturity indicator levels (MILs), MIL0 through MIL3, which apply independently to each domain in the model. Summary definitions of the MILs are provided in Table 3.

Table 3: Summary of Maturity Indicator Levels

Level	Characteristics
MIL0	Practices are not performed
MIL1	Initial practices are performed, but may be ad hoc (i.e., makeshift, improvised, undocumented)
MIL2	• Practices are documented • Adequate resources are provided to support the process • Practices are more complete or advanced than at MIL1
MIL3	• Activities are guided by policies (or other organizational directives) • Responsibility, accountability, and authority for performing the practices are assigned • Personnel performing the practices have adequate skills and knowledge • The effectiveness of activities is evaluated and tracked • Practices are more complete or advanced than at MIL2

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

- The maturity indicator levels apply independently to each domain. As a result, an organization using the model may be operating at different MIL ratings in different domains. For example, an organization could be operating 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 practices in that level and in the preceding level(s) with an implementation score of "Fully Implemented" or "Largely Implemented". For example, an organization must perform all the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization must perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3. In the Sol-ReMM, a practice is considered performed if it is evaluated as "Fully Implemented" or "Largely Implemented". A single practice in a domain that has a "Partially Implemented" or "Not Implemented" score for its MIL will keep that domain from achieving that MIL or and higher MIL. However, the model's spotlighting of that lagging practice or practices, provides useful information to users on what programmatic improvements might be needed to achieve the associated maturity level.

- Establishing a target MIL for each domain is an effective strategy for using the model to guide cybersecurity program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Then, they can focus gap analysis activities and improvement efforts on achieving those target levels. The Sol-ReMM website offers a tool for decision makers to use to select and document their target MIL selections.
- Practice performance and MIL achievement need to align with business goals and the organization's cybersecurity and resilience program strategy. Striving to achieve the highest MIL in all domains may not be optimal. Organizations should evaluate the costs of achieving a specific MIL versus its potential benefits. However, the model was designed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

4.3 Progression

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

To achieve MIL1, these 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.

In the context of the model, *ad hoc* (that is, formed or used for a special purpose without policy or a plan for repetition) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team, without much organizational guidance, such as a prescribed plan, policy, or training. The quality of the outcome may vary significantly depending on who performs the practice, when it is performed, the context of the problem being addressed, the methods, tools, and techniques used, and the priority given to performance of the practice. High-quality outcomes may be achieved with experienced and talented personnel even if practices are ad hoc. However, at this MIL, lessons learned are typically not captured at the organizational level, so approaches and outcomes are difficult to repeat or improve across the organization. It is important to note that, while documented policies or procedures are not essential to the performance of a practice in an ad hoc manner, the effective performance of many practices may result in documented artifacts such as a documented asset inventory or a documented cybersecurity program strategy.

4.4 Enterprise-Focused Domains

As with all organizational functions and activities, resilience and cybersecurity programs operate in an enterprise context. The enterprise imposes requirements on the programs in the form of missions and goals, and in turn, provides some of the tools and capabilities that are needed for program success. Some enterprise functions, such as risk management, directly influence resilience and cybersecurity decisions and actions, and require coordination to ensure shared goals can be achieved.

The Sol-ReMM is generally applied to a specific scope or organizational function. Several domains (e.g., Risk Management, Cybersecurity Architecture, Resilience Program Management) may operate in an enterprise context in that they often define practices that benefit general activities in the organization, regardless of the model scope.

Model users should recognize that these domains may constitute enterprise programs that may be established and operate independently of the in-scope function.

4.5 Considerations for the Cybersecurity Architecture Domain

To better understand the objectives and practices in the Cybersecurity Architecture domain, the fundamental definition and features of a cybersecurity architecture must be understood.

4.5.1 Cybersecurity Architecture Defined

A cybersecurity architecture is a framework that defines the organization's system of tools, techniques, methods, and controls that ensure cyber threats can be prevented, detected, and corrected across all levels and layers of information and operational technologies (IT and OT). The cybersecurity architecture is a fundamental component of the organization's enterprise architecture which, in simple terms, defines, documents, and standardizes the IT and OT infrastructure that supports business needs, goals, and objectives. Because the cybersecurity architecture operates within the enterprise architecture, these frameworks must align and integrate, and the cybersecurity architecture must objectively ensure the operational consistency, reliability, and continuity of the enterprise architecture.

4.5.2 Cybersecurity Architecture Framework

In practice, a cybersecurity architecture is typically documented through a series of reference diagrams that establish a plan for and working definition of the organization's cybersecurity infrastructure and the way in which it aligns with and integrates to the IT and OT infrastructure.

Details of the cybersecurity architecture are often established as a series of requirements described in reference architectures. For example, a reference architecture for securing

mobile computing (such as the use of phones and tablets) may establish the requirements, acceptable technologies, and controls for connecting devices to wireless routers, including acceptable encryption methodologies, and guidelines for segmentation of mobile network traffic into subnets that can be monitored with more granular policies and rulesets.

The cybersecurity architecture must be comprehensive and inclusive of all potential types of platforms (such as cloud, IoT, mobility, networks, endpoints, and external connections), systems (such as in-house applications and applications-as-a-service), data (stored, transmitted, and processed in-house or in the cloud), and operational technologies (such as field automation devices, industrial control systems, and physical security components).

4.5.3 Implementing the Cybersecurity Architecture

The cybersecurity architecture establishes the organization's plan for securing the IT and OT infrastructure and contributing to its resiliency when threatened or compromised. In operation, the cybersecurity architecture guides the selection of tools, techniques, methods, and controls to meet the organization's cybersecurity objectives. For example, a cybersecurity architecture may include a defense-in-depth strategy that reflects specific tools and technologies for perimeter defense (such as firewalls, intrusion prevention and detection, demilitarized zones [DMZs]), web traffic filtering (such as proxies, web filters, content filtering), and endpoint protection (such as antivirus, antimalware, data loss prevention).

The cybersecurity architecture also serves as a compliance reference as changes occur in the IT and OT infrastructure or as cybersecurity goals change. These changes may result from many sources, including upgrading of technologies, sunsetting of old technologies, changes in business structure, new business initiatives, merger and acquisition activity, or regulatory changes. In addition, changes to the cybersecurity and IT and OT infrastructure may be informed by perceived threats and vulnerabilities, or events and incidents that the organization has experienced. Many organizations establish an architecture review board or similar group to provide collaborative discussion, consideration, and approval of proposed technology changes. For all proposed changes, the architecture review board examines the change or reconfiguration of existing technologies or addition of any new technology with reference to the cybersecurity and enterprise architectures to ensure proper interoperability, preservation of controls, continuity of operation, maintainability, and limited impact on user functionality.

4.5.4 Considering the Cybersecurity Architecture in Sol-ReMM

The objectives and practices in the Cybersecurity Architecture domain prioritize establishing a strategy and plan that reflects their cybersecurity goals, is implemented in alignment with the organization's enterprise architecture, and provides proper oversight as changes are proposed and made. The domain's practices also reflect foundational controls expected in a cybersecurity architecture (such as segmenting IT and OT networks) and proper coverage of

infrastructure layers (IT and OT assets, networks, software, and data). Finally, support practices that establish mechanisms such as documentation, policy, and accountability are included to support making the architecture institutionalized as part of the organization's security culture.

4.6 Example Lists Included in Practices

Several practices within the model and Help Text entries include lists of examples to help illustrate the meaning of the practices. These example lists are introduced by parenthetical statements "for example", "e.g.,", or "such as." The purpose of these example lists is to better communicate the intended meaning of practices. Example lists (sch as Illustrated in Figure 3) should not be interpreted as an authoritative description of how a practice should be implemented. Each organization and function to which the model is applied is likely to have a unique risk profile and operating environment, and so the provided examples may not be applicable to all organizations and functions. Users of Sol-ReMM may leverage example lists to generate ideas about what considerations may be applicable but should not interpret an example list as indicating a minimum baseline or as an exhaustive list of what might be considered for implementation of a practice.

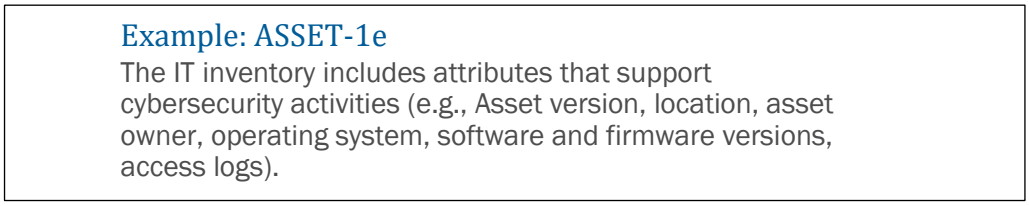


Figure 3: Example List Included in Practice ASSET-1e

4.7 Practice Reference Notation

Several practices are related to other model practices. When this occurs, the related practice is referenced using a notation that begins with the domain short name, a hyphen, the objective number, and the practice letter. Related practices may be in different objectives or even different domains.

5. USING THE MODEL

The Sol-ReMM is meant to be used by an organization to evaluate its resilience and cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its resilience and cybersecurity investments. Figure 4 summarizes a potential approach for using the model. An organization performs a self-evaluation using the model, uses that self-evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves the process is repeated. Each step in this approach is described in the following sections.



Figure 4: Potential Approach for Using the Model

5.1 Step 1: Perform a Self-Evaluation

Performing a Sol-ReMM self-evaluation provides a measurement of the implementation of resilience and cybersecurity activities within an organization. A design goal of the model is to enable organizations to complete a self-evaluation for a single function in a couple of days without extensive study or preparation. To begin preparation, the organization first establishes the scope of the model application, or the *function*. Next, the organization should identify the assets, (including IT, OT, and information assets) that are important to the delivery of the function.

The organization should select the appropriate personnel to evaluate the function against the model practices. An effective facilitator who is familiar with model content should be

identified to guide the self-evaluation. Participation by stakeholders from across the organization yields the best results, increases shared situational awareness of relevant cybersecurity risks and concrete steps to mitigate them using the model practices, and offers an opportunity to clarify roles and responsibilities. More thorough guidance on preparing to use the model, selecting a facilitator, and scoping the self-evaluation can be found in the supporting *Sol-ReMM Self-Evaluation Process Guide*.[2]

Upon completion of the self-evaluation, a scoring report is generated that provides summary-level depictions of performance relative to the model, as well as practice-level implementation status. This report provides a point-in-time view of the resilience and cybersecurity posture of the in-scope function. The report should be reviewed with the self-evaluation workshop participants, and any discrepancies or questions should be addressed. It is important to note that the self-evaluation report may include sensitive information and should be protected accordingly.

5.2 Step 2: Analyze Identified Gaps

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

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

For organizations using the model for the first time, a target profile is typically identified after the initial self-evaluation. This gives the organization an opportunity to develop more familiarity with the model. Organizations that have more experience with the model have often identified a target profile before undergoing a self-evaluation. An appropriate mix of organizational stakeholders should be included in the selection of the target profile. This might be a single individual with expertise in the function's operations and management, but it is likely to be a collection of individuals representing business, technology, and operational considerations from across the organization.

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

[2] The *Sol-ReMM Self-Evaluation Process Guide* is available for download from the Sol-ReMM website.

5.3 Step 3: Prioritize and Plan

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

Next, a plan should be developed to address the selected gaps. Planning should follow standard organizational planning processes and align to the strategic goals of the organization . These plans can span a period of weeks, months, or years, depending on the extent of improvements needed to close the selected gaps and achieve the desired capability. An individual with sufficient authority to carry out the plan should be identified and assigned as the plan owner. Regular reviews by organizational leadership should be conducted to evaluate status, clear obstacles, and identify any necessary course corrections as implementation progresses.

5.4 Step 4: Implement Plans and Periodically Reevaluate

Plans developed in the previous step should be implemented to address the identified gaps. Model self-evaluations are particularly useful in tracking implementations and should be conducted periodically to ensure that desired progress is achieved. Reevaluations should also be considered in response to major changes in business, technology, market, or threat environments so that the current profile matches the organization's desired state. Table 4 Summarizes the four-step approach for using the model.

Table 4: Inputs, Activities, and Outputs: Breakdown of Potential Approach

	Inputs	Activities	Outputs
1. Perform a Self-Evaluation	1. Sol-ReMM self-evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct Sol-ReMM self-evaluation with appropriate attendees	Sol-ReMM self-evaluation report
2. Analyze Identified Gaps	1. Sol-ReMM self-evaluation report 2. Organizational objectives 3. Impact to critical infrastructure	1. Develop a target profile 2. Analyze gaps 3. Evaluate potential consequences from gaps 4. Determine which gaps need attention	List of gaps and potential consequences
3. Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Conduct cost-benefit analysis (CBA) on actions 3. Prioritize actions 4. Plan to implement prioritized actions	Prioritized implementation plan
4. Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

6. MODEL DOMAINS

6.1 Asset Inventory Management (INVENTORY)

Purpose: Manage the organization's information technology (IT), operations technology (OT), and information assets through a structured program for identifying, inventorying, and maintaining essential assets. Ensure accurate documentation and tracking of assets throughout their lifecycle to support operational efficiency and cybersecurity objectives.

The Asset Inventory Management (INVENTORY) domain is crucial for maintaining visibility and control over IT, OT, and information assets to minimize risks and ensure resilience. The core objectives for this domain are:

1. Manage IT Asset Inventory
2. Manage OT Asset Inventory
3. Manage Information Asset Inventory
4. Management Activities

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

Objectives and Practices

1. Manage IT Asset Inventory

MIL1	a. IT assets that are essential to facility operations are identified, at least in an ad hoc manner. b. IT assets are inventoried, at least in an ad hoc manner.
MIL2	c. IT assets are inventoried following a documented process. d. The IT asset inventory identifies IT assets that are essential to facility operation. e. The IT inventory includes attributes that support cybersecurity activities (e.g., Asset version, location, asset owner, operating system, software and firmware versions, access logs).
MIL3	f. The inventory of IT is complete and updated at an organization-defined frequency. g. There is a plan to sanitize or securely dispose of IT assets prior to redeployment or at their end of life.

2. Manage OT Asset Inventory

MIL1	a. OT assets that are essential to facility operations are identified, at least in an ad hoc manner. b. OT assets are inventoried, at least in an ad hoc manner.
MIL2	c. OT assets are inventoried following a documented process. d. The OT asset inventory identifies OT assets that are essential to facility operation. e. The OT inventory includes attributes that support cybersecurity activities (e.g., Asset version, location, asset owner, operating system, software and firmware versions, and access logs).
MIL3	f. The inventory of OT is complete and updated at an organization-defined frequency. g. There is a plan to sanitize or securely dispose of OT assets prior to redeployment or at their end of life. h. The OT inventory includes a parameter that indicates the level of consequences that could occur if the OT asset is compromised by an adversary

3. Manage Information Asset Inventory

MIL1	a. Information assets that are essential to facility operations are identified, at least in an ad hoc manner. b. Key information assets (e.g., set point data, intellectual property, contracts, security, and event management log data) are inventoried, at least in an ad hoc manner.
MIL2	c. High-value information assets are inventoried following a documented process. d. The information asset inventory identifies OT assets that are essential to facility operation. e. Inventoried information assets are categorized based on their general level of sensitivity, value, or criticality. f. The information asset inventory includes attributes that support cybersecurity activities (e.g., storage location and name of information asset owner).
MIL3	g. The information asset inventory is complete and updated at an organization-defined frequency. h. There is a plan to sanitize or destroy key information assets when they are no longer used or needed. i. The information asset inventory includes a parameter that indicates the level of consequences that could occur if the information asset is compromised by an adversary.

4. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified—even if they are not allocated—to support asset inventory management. b. Key internal stakeholders are identified and involved in decision making for asset inventory management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving asset inventory management. d. Adequate resources (people, funding, training, and tools) are provided to support activities involving asset inventory management. e. Personnel performing activities involving asset inventory management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of activities involving asset inventory management are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of asset inventory management activities. h. The effectiveness of asset inventory management activities is tracked and evaluated at an organization-defined frequency to confirm they meet organizational goals.

6.2 Asset Configuration and Change Management (CHANGE-MGMT)

Purpose: Manage the configuration and change management program for the organization's critical assets including information technology (IT), operations technology (OT), and information assets. Change management is the process of managing the changes that are made to configurable assets. This includes proposed addition, deletion, or modification of any asset in a system. Configuration management establishes and maintains processes for initializing, changing, and monitoring the configurations of assets throughout their life cycle, Asset configurations are aligned with organizational requirements and resilience best practices. Changes to assets are systematically evaluated, approved, and documented to maintain asset integrity and operational resilience.

The Asset Configuration and Change Management (CHANGE-MGMT) domain comprises four objectives:

1. Manage Asset Configuration
2. Manage Changes to Assets
3. Asset/Equipment Maintenance
4. Management Activities

Asset configuration refers to the settings, parameters, and installed components of an asset (hardware, software, or information system) that define how it operates. Configuration management involves establishing a baseline for these settings, ensuring they align with organizational security and operational goals, and regularly monitoring the asset to ensure that it remains in compliance with the baseline configuration. Any deviations or changes from the baseline are tracked and managed.

Change Management is the process of managing changes to an organization's assets. It involves assessing and evaluating the need for a change, approving the change, implementing it, and ensuring that the change is well-documented. The aim is to ensure that changes do not introduce vulnerabilities or cause disruptions to operations. Change management typically includes detailed processes for testing changes before deployment, monitoring for unintended consequences, and ensuring traceability of all changes.

A key component of this strategy is the definition of configuration baselines, which serve as the standard reference for asset configurations. These baselines should be regularly reviewed and updated to reflect emerging security threats, technological advancements, and operational needs. In addition, a change control

process must be established, ensuring that all changes undergo impact analysis and approval before implementation. This process helps mitigate risks associated with unauthorized or poorly managed changes.

To support this strategy, a change log or configuration register is crucial. This document or database tracks all changes to assets, including details such as the nature of the change, the assets affected, the rationale behind the change, and its approval and implementation status. A well-maintained change log ensures transparency and accountability, facilitating audits and supporting future decision-making.

Objectives and Practices

1. Manage Asset Configuration

MIL1	a. Configuration baselines for assets are established, at least in an ad hoc manner.
MIL2	b. Documented processes are established for setting configuration baselines. c. +Configuration baselines are used to configure assets at deployment and restoration d. Configuration baselines incorporate cybersecurity good practices and organization requirements.
MIL3	e. Configuration baselines are reviewed and updated at an organization-defined frequency and according to defined triggers such as significant system changes f. A formal process is in place to validate selected asset configurations for compliance with the configuration management program.

2. Manage Changes to Assets

MIL1	a. Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner. b. Changes to assets are documented, at least in an ad hoc manner.
MIL2	c. Change management policies are established and maintained. d. Changes to assets that are essential to facility operation are tested for their functionality impacts prior to being deployed. e. Changes and updates to assets are implemented in a secure manner. f. The capability to reverse changes is established and maintained for critical assets that are important to the delivery of key functions.
MIL3	g. Changes to critical assets are tested for cybersecurity impact prior to being redeployed. h. Change management processes are reviewed and updated at an organization-defined frequency and for defined triggers (e.g., significant system changes or changes in the threat and vulnerability environment).

3. Asset/Equipment Maintenance

MIL1	a. The facility's assets undergo recommended maintenance, at least in an ad hoc manner, to support their proper operation.
MIL2	b. There is a documented maintenance process that supports the proper operation of key facility systems. c. The facility's assets undergo maintenance at prescribed intervals. d. Maintenance activities are documented and a historical record of maintenance activities is maintained. e. Maintenance processes prioritize assets based on their criticality to the operation of the facility.
MIL3	f. The organization has a security plan that covers maintenance activities and maintenance is conducted in accordance with that plan. g. Maintenance activities conducted by contractors/vendors are implemented and reviewed according to the organization's security plan. h. After maintenance activities are completed, assets that are essential to facility operation are tested for their functionality impacts prior to being redeployed. i. Maintenance processes are reviewed and updated at an organization-defined frequency and for defined triggers (e.g., significant system changes or changes in the threat and vulnerability environment).

4. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support asset configuration and change management. b. Key internal stakeholders are identified and involved in decision making for asset configuration and change management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving asset configuration and change management. d. Adequate resources (people, funding, training, and tools) are provided to support activities for asset configuration and change management. e. Personnel performing activities involving asset configuration and change management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of activities involving asset configuration and change management are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of asset configuration and change management activities. h. The effectiveness of asset configuration and change management activities is tracked and evaluated at an organization-defined frequency to confirm they meet organizational goals.

6.3 Access and Authorization Management (ACCESS)

Purpose: Create and manage processes for handling identities, credentials, and access controls to the organization's assets. Personnel, devices, and services are authorized based on documented procedures and robust mechanisms for identity provisioning, credential management, and access control. Align these processes with organizational security requirements and resilience best practices.

For the purposes of this domain, access control applies to logical access to assets used in the delivery of the function, physical access to 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 access to critical resources, including systems and services. This in turn could result in security breaches, disruption of operations, and exposure to cybersecurity risks. Effective access control limits the potential for unauthorized access, supports compliance with security policies, protects sensitive information, and helps maintain the integrity of organizational assets.

Access and Authorization Management (ACCESS) domain comprises four objectives:

1. Identity and Authentication Management
2. Logical Access Control Management
3. Physical Access Control Management
4. Management Activities

Establishing and maintaining identities involves provisioning and deprovisioning identities for entities, including individuals, devices, and systems. This provides traceability for valid access, with compensatory measures for shared identities as needed.

Controlling logical and physical access involves defining access requirements, granting access based on those requirements, and revoking access when no longer needed. For solar facilities and systems, access requirements are designed to limit access to critical assets to only authorized entities, with logical access often requiring multi-factor authentication and physical access controlled by visible measures like signage, fencing, and locks.

As maturity increases, access privileges may be granted based on risk assessments, and access reviews are conducted periodically to evaluate compliance with security policies and minimize exposure to threats.

Objectives and Practices

1. Identity and Authentication Management

MIL1	a. Identities for personnel and other entities (e.g., devices and services that require access to assets) are established, at least in an ad hoc manner. b. Credentials (e.g., passwords, smart cards, certificates, keys) are issued to personnel and other entities requiring asset access, at least in an ad hoc manner. c. Identities when no longer required are deprovisioned, at least in an ad hoc manner.
MIL2	d. Credentials (e.g., passwords, smart cards, certificates, keys) are issued to personnel and other entities requiring asset access following a documented process. e. Identities for personnel and other entities (e.g., devices, services) requiring asset access are provisioned following a documented process. f. Identities when no longer required are deprovisioned following a documented process. g. Criteria for password strength and reuse are established and enforced. h. Stronger credentials, single-use credentials, or multi-factor authentication are required for access to assets or methods that pose an elevated risk (e.g., critical assets, assets that can be remotely accessed).
MIL3	i. Identity repositories are reviewed and updated at an organization-defined frequency or if/when defined triggers occur (e.g., system changes, changes in the threat profile). j. Multi-factor authentication, when and where feasible, is required for access to critical assets or assets that can be remotely accessed. k. Identities are disabled, when and where feasible, after a defined period of inactivity.

2. Logical Access Control Management

MIL1	a. Logical access controls are implemented, at least in an ad hoc manner b. Logical access privileges are revoked when no longer needed, at least in an ad hoc manner
MIL2	c. Logical access controls are developed and deployed following a documented process. d. Logical access privileges are terminated following a documented process when these privileges are no longer needed. e. Requirements for logical access are established and maintained (e.g., who is allowed to access an asset, access limits, remote access constraints, authentication parameters). f. Logical access requirements include the principle of least privilege. g. Logical access requirements involve the principle of separation of duties. h. Logical access requests are reviewed and approved by the asset owner.

	i. Logical access that poses elevated risks undergoes additional scrutiny and monitoring.
MIL3	j. Logical access authorizations are reviewed and updated at an organization-defined frequency and when defined triggers occur (e.g., changes to systems, organizational structure, threat profiles). k. Anomalous logical access attempts are monitored as potential indicators of malicious events.

3. Physical Access Control Management

MIL1	a. Controls for physical access (e.g., locks, fences, signage) are employed, at least in an ad hoc manner. b. Physical access privileges are terminated when no longer needed, at least in an ad hoc manner.
MIL2	c. Controls for physical access (e.g., locks, fences, signage) are developed and deployed following a documented process d. Physical access privileges are terminated following a documented process when these privileges are no longer needed. e. Requirements for physical access (e.g., rules for who is allowed to access an asset, how access is granted, allowed access limits) are developed and maintained. f. Physical access requirements include the principle of least privilege. g. Physical access requirements involve the principle of separation of duties. h. Physical access requests are reviewed and approved by the asset owner. i. Physical access that poses elevated risks undergoes additional scrutiny and monitoring.
MIL3	j. Physical access authorizations are reviewed and updated at an organization-defined frequency and when defined triggers occur (e.g., changes to systems, organizational structure, threat profiles). k. Monitoring of physical access is conducted to identify incidents and patterns that may be indicative of a security event.

4. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support access and authorization management. b. Key internal stakeholders are identified and involved in decision-making for access and authorization management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving access and authorization management. d. Adequate resources (people, funding, training, and tools) are provided to support access and authorization management activities.

	e.	Personnel performing activities involving access and authorization management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f.	Responsibility, accountability, and authority for the performance of access and authorization management activities are assigned to personnel.
	g.	External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of access and authorization management activities.

6.4 Threat and Vulnerability Management (THREAT)

Purpose: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to resilience and cybersecurity threats and vulnerabilities, Threat and vulnerability management should be commensurate with the risk to the organization's operations and goals.

A threat is defined as any circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image, or reputation), resources, or other organizations. Threats may impact IT, OT, or communications infrastructure via destruction, unauthorized access, disclosure, modification of information, and/or denial of service. Threats to information, IT, OT, and communication infrastructure assets vary and may include natural events, the actions of malicious actors, malware (such as viruses and worms), and distributed denial-of-service (DDoS) attacks.

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

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

1. Manage Cybersecurity Vulnerabilities
2. Threat Response Management
3. Management Activities

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

Reducing vulnerabilities begins with collecting and analyzing vulnerability information. The discovery of cybersecurity vulnerabilities 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 performing other activities.

Objectives and Practices

1. Manage Cybersecurity Vulnerabilities

MIL1	a. Information sources to facilitate the discovery of cybersecurity and other product or service vulnerabilities are identified, at least in an ad hoc manner. b. Cybersecurity and other vulnerability information is gathered and interpreted, at least in an ad hoc manner. c. Cybersecurity and other vulnerability assessments are conducted, at least in an ad hoc manner. d. Identified cybersecurity and other vulnerabilities are prioritized, at least in an ad hoc manner.
MIL2	e. Information sources used in the discovery of cybersecurity and other vulnerabilities are identified and documented. f. Cybersecurity and other vulnerability information is gathered and interpreted following a documented process. g. Cybersecurity and other vulnerability assessment are conducted, following a document process. h. Identified cybersecurity and other vulnerabilities are prioritized following a documented process. i. Cybersecurity and other vulnerability information sources for high-priority assets are routinely monitored.
MIL3	j. Relevant cybersecurity and other vulnerability information is shared with organization-approved internal and external stakeholders. k. Cybersecurity and other vulnerability assessments are conducted at an organized-defined frequency and after defined triggers (e.g., major system changes, changes in the threat environment). l. Cybersecurity and other vulnerability monitoring activities include a validation step to check that effective security measures are planned or were implemented in response to significant vulnerabilities. m. Vulnerability information, including cybersecurity information, is consolidated, and maintained in a secure risk register or risk information database.

2. Threat Response Management

MIL1	a. Internal and external information sources are identified to support threat management activities, at least in an ad hoc manner. b. The goals of those who may perpetrate a threat are identified, at least in an ad hoc manner. c. The organization acts on threat information that may involve their high-priority assets, at least in an ad hoc manner.
MIL2	d. Internal and external information sources to support threat management activities, including cybersecurity threats, are identified following a documented process. e. The potential impacts of threats, including cybersecurity threats, are determined following a documented process. f. The organization acts on threat information that may involve their high-priority assets following a documented process.
MIL3	g. A threat profile is established that includes the potential outcomes and additional characteristics of the threat (e.g., threat actor types, motives, capabilities, targets). h. The profile of each identified threat is updated periodically and according to defined triggers involving system changes or external events. i. Threat monitoring has the ability to trigger predefined states of operation as part of the response to an emerging threat. j. Secure and near-real-time methods are employed to receive and share threat information, including cybersecurity threats, to enable rapid analysis and response to an emerging threat. k. Threat information, including cybersecurity threat information, is consolidated and maintained in a secure risk register or risk information database.

3. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support threat and vulnerability management. b. Key internal stakeholders are identified and involved in decision-making for threat and vulnerability management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving threat and vulnerability management. d. Adequate resources (people, funding, training, and tools) are provided to support threat and vulnerability management activities. e. Personnel performing activities involving threat and vulnerability management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of threat and vulnerability management activities are assigned to personnel g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of threat and vulnerability management activities.

6.5 Risk Assessments and Management (RISK)

Purpose: Establish and maintain a resilience and cybersecurity risk management program to identify, assess, prioritize, and address risks. Risk management should consider both natural and human-caused threats to resilience. The program documents processes, integrates stakeholder input, and aligns with organizational goals to effectively manage and mitigate risks.

Risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations may result from natural and human-caused events. The latter include the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information, IT, or OT assets. Resilience and security risks cannot be completely eliminated, but they can be managed through informed decision-making processes.

The Risk Management (RISK) domain comprises six objectives:

1. Develop and Maintain a Risk Management Strategy and Program that Support Resilience
2. Identify the Consequences of Resilience Events
3. Identify Resilience Risks
4. Analyze Resilience Risks
5. Risk Responses
6. Management Activities

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

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 (Situational Awareness and Event and Incident Response) may refer to the risk register or risk databased as means for documenting risks.

Objectives and Practices

1. Develop and Maintain a Risk Management Strategy and Program that Support Resilience

MIL1	a. The organization has a risk management strategy that addresses resilience and the continuity of operations, even if that strategy is informal.
MIL2	b. The organization has a documented risk management strategy that addresses resilience and the continuity of operations. c. The risk management strategy aligns with the organization's resilience and cybersecurity program. d. A risk management program is implemented and addresses resilience issues, including cybersecurity. e. Risk management information is shared with relevant internal stakeholders.
MIL3	f. Risk management information is shared with relevant external stakeholders. g. The risk management strategy and program are reviewed and updated at an organization-defined frequency and for defined triggers (e.g., significant system changes, changes in the threat environment).

2. Identify the Consequences of Resilience

MIL1	a. Consequences for resilience and continuity of operation that are based upon perceived threats and vulnerabilities are identified, at least in an ad hoc manner. b. Consequences for resilience and continuity of operation are characterized by level of impact (e.g., minor, moderate, severe), at least in an ad hoc manner. c. The likelihood of the consequence from resilience events is characterized (e.g., negligible, unlikely, credible), at least in an ad hoc manner.
MIL2	d. Consequences for resilience and continuity of operation (based upon perceived threats and vulnerabilities, including those associated with cybersecurity) are identified following a documented process. e. Consequences for resilience and continuity of operation (based upon perceived threats and vulnerabilities, including those associated with cybersecurity) are identified following a documented process. f. Consequences for resilience and continuity of operation are characterized by level of impact (e.g., minor, moderate, severe), following a documented process. g. The likelihood of the consequence from resilience events, including cyberattacks, is characterized (e.g., negligible, unlikely, credible) following a documented process. h. Consequence information is shared with relevant internal stakeholders. i. Consequence information is shared with relevant external stakeholders

MIL3	j. Consequences for resilience and continuity of operation (based upon perceived threats and vulnerabilities, including those associated with cybersecurity) are identified following a documented process. k. Consequences for resilience and continuity of operation are characterized by level of impact (e.g., minor, moderate, severe), following a documented process. l. The likelihood of the consequence from resilience events, including cyberattacks, is characterized (e.g., negligible, unlikely, credible) following a documented process. m. Consequence information is shared with relevant internal stakeholders. n. Consequence information is shared with relevant external stakeholder
3. Identify Resilience Risks	
MIL1	a. Resilience risks are identified, at least in an ad hoc manner.
MIL2	b. Resilience risks, including those associated with cyberattacks, are identified following a documented process. c. Stakeholders from relevant operational and business areas are consulted and involved in identifying resilience risks. d. The identification of resilience risks, including cybersecurity risks, utilizes information obtained during threat and vulnerability assessments. e. Resilience risk identification activities, including those involving cybersecurity risks, are conducted periodically and in response to defined triggers such as system updates and external events.
MIL3	f. Resilience risk identification activities are reviewed and updated at an organization-defined frequency and in response to defined triggers (e.g., significant system changes, changes in the threat and vulnerability environment). g. Resilience risk identification information is recorded in a secure risk register or risk information database.
4. Analyze Resilience Risks	
MIL1	a. Resilience risks are prioritized according to their estimated likelihood and impact, at least in an ad hoc manner.
MIL2	b. Resilience risks, including cybersecurity risks, are prioritized following a documented process based on their estimated likelihood and impact. c. A structured approach is employed to provide greater attention and quantification for risks, including cybersecurity risks, that rank high after initial assessments. d. Stakeholders from relevant operational and business areas within the organization participate in the more detailed analysis of risks that rank high after initial assessments.
MIL3	e. Resilience risk analyses are reviewed and updated at an organization-defined frequency and for defined triggers (e.g., significant changes in systems, changes in the threat and vulnerability environment). f. Resilience risks, including cybersecurity risks, are documented in a secure risk register or risk information database.

	g. Resilience risks are delisted from the risk register once circumstances change and they no longer require tracking and response.

5. Risk Responses

MIL1	a. Risk responses (e.g., mitigate, accept, ignore, or transfer) to address resilience risks are applied, at least in an ad hoc manner.
MIL2	b. Risk responses for resilience events, including cybersecurity events, are determined following a documented process. c. Risk responses prioritize addressing high risk events.
MIL3	d. Implemented risk responses are assessed to confirm that they are appropriately designed and are functioning as intended to mitigate the identified risks. e. Senior leadership reviews outcomes from risk responses to determine if risks are adequately mitigated and risk tolerances are not exceeded. f. The risk response process is reviewed at an organization-defined frequency by leadership and is updated if/when required.

6. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support risk assessments and management. b. Key internal stakeholders are identified and involved in decision-making for risk assessments and management activities, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving risk assessments and management. d. Adequate resources (people, funding, training, and tools) are provided to support risk assessments and management activities. e. Personnel performing activities involving risk assessments and management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of risk assessments and management activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of risk assessments and management activities.

6.6 Supply Chain Management (SUPPLY-CHAIN)

Purpose: Establish and manage relationships with key suppliers to ensure resilience and security in the supply chain, including evaluation, performance oversight, and backup arrangements. Regularly review and update practices to align with policies, industry best practices, and evolving conditions.

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

The quality of products provided by suppliers can vary widely. In addition, the responsiveness of suppliers to customer needs, particularly during a resilience-challenging event, can also vary widely, It is helpful for organizations to characterize suppliers, including considering the quality of their products, security features, support, the reliability of their products, and the ability of the supplier to support the organization during a resilience-challenging event. Organizations should also identify and characterize potential backup suppliers in the event primary suppliers are unable to meet the organization's needs. An effective spare parts program is also helpful to provide continuity of operations during a resilience challenging event.

The Supply Chain Management (SUPPLY-CHAIN) domain comprises five objectives:

1. Identify and characterize Suppliers
2. Prioritize and Select Suppliers
3. Manage Suppliers
4. Identify and Characterize Backup Suppliers
5. Develop and Coordinate a Spare Equipment Program
6. Management Activities

Objectives and Practices

1. Identify and Characterize Suppliers

MIL1	a. Suppliers of key products (both hardware and software) and services are identified and characterized at least in an ad hoc manner. b. The organization characterizes, at least in an ad hoc manner, the reliability and security posture of key suppliers of products and services.
MIL2	c. The organization has a documented process to identify and characterize its suppliers of products and services d. The organization has a documented process that governs the characterization of the reliability and security of its suppliers of products and services.

MIL3	e. The organization has a documented process for evaluating the ability of its suppliers of products and services to help the organization respond and recover from a resilience-challenging event. f. Information on the reliability and security status of suppliers of products and services is reviewed and updated at an organization-defined frequency.

2. Prioritize and Select Suppliers

MIL1	a. Suppliers of key products and services are prioritized for the organization's attention and oversight, at least in an ad hoc manner, based on their importance to the organization. b. Potential suppliers and service providers are engaged in a discussion of their supply chain risks and potential mitigation steps, at least in an ad hoc manner. c. Cybersecurity requirements are considered, at least in an ad hoc manner, when establishing relationships with potential suppliers of products and services.
MIL2	d. Using a documented process, suppliers of key products and services are prioritized for the organization's attention and oversight based on their importance to the organization. e. The evaluation and selection of vendors/suppliers is conducted through a documented process that considers their ability to meet cybersecurity requirements.
MIL3	f. The documented process used to prioritize and select suppliers is reviewed and updated at an organization-defined frequency g. The process used to prioritize and select suppliers is based on industry best practices for supply chain security.

3. Manage Suppliers

MIL1	a. The acquisition of products and services from suppliers is overseen by designated organization staff members, at least in an ad hoc manner. b. Guidelines for managing suppliers are established, even if undocumented and/or implemented in an ad hoc manner.
MIL2	c. A documented supplier management program is established to monitor the performance of suppliers of products and services in accordance with their contractual obligations. d. Following the documented supplier management program, organization staff periodically monitor the performance of suppliers of products and services to assess whether the supplier is in accordance with their contractual obligations. e. The supplier management program establishes provisions for transitioning between suppliers offering comparable or replacement products/services. f. The organization has a documented process to guard against the acquisition of counterfeit or compromised products. g. The supplier management program directs organization staff on how to addresses such issues as supplier organizational changes, supplier subcontracting, and supplier breach of contract. h. Any failure to comply with contractual requirements is promptly communicated to the supplier of the product or service.

MIL3	i. The supplier management program directs the organization to consider the need for emergency supplier agreements (e.g., if the original supplier is unable to fulfill their obligations) j. The supplier management program is reviewed and updated as needed at an organization-defined frequency and in response to changing circumstances. k. The supplier management program meets or exceeds industry best practices.

4. Identify and Characterize Backup Suppliers

MIL1	a. Potential backup suppliers of key products (both hardware and software) and services are identified at least in an ad hoc manner. b. The organization characterizes, at least in an ad hoc manner, the reliability and security posture of potential backup suppliers of products and services.
MIL2	c. The organization has a documented process to identify and characterize backup suppliers and service providers. d. The organization has a documented process that governs the assessment of the reliability and security of backup suppliers of key products and services.
MIL3	e. The organization has a documented process for evaluating the ability of its backup suppliers of products and services to support the organization in responding and recovering from a resilience-challenging event. f. Information on the reliability and security status of backup suppliers of products and service is reviewed and updated at an organization-defined frequency or when changes in circumstances warrant a review.

5. Develop and Coordinate a Spare Equipment Program

MIL1	a. The organization has spare equipment in stock or is prepared to quickly acquire spare equipment during a resilience challenging event, even if only organized in an ad hoc manner.
MIL2	b. The spare equipment program is guided by documented policies and procedures. c. The documented spare equipment program considers resilience in addition to reliability in determining optimal inventory amounts, supplier diversity, appropriate levels of redundancy, locations (e.g., staging location and transportation needs), to support timely restoration of operations. d. The documented spare equipment program prioritizes classes of components based on the need for equipment during events that challenge resilience.
MIL3	e. The documented spare equipment program includes requirements for the organization to perform spare equipment maintenance and operability tests (e.g., periodic testing and maintenance of warehouse stock, deployment of spare equipment as replacements and the replenishment of spare equipment inventory). f. The documented spare equipment program is coordinated with neighboring utilities, as well as through industry partnerships). g. The spare equipment program is reviewed at an organization-defined frequency and if/when triggered by significant system changes or external events. h. The spare equipment program adopts standard designs to facilitate the efficient use of spares, including replacement and sharing of assets when needed (e.g., plug-n-play).

6. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support supply chain management. b. Key internal stakeholders are identified and involved in decision making for supply chain management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving supply chain management. d. Adequate resources (people, funding, training, and tools) are provided for supply chain management. e. Personnel performing activities involving supply chain management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of supply chain management activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of supply chain management activities.

6.7 Procurement Process (PROCUREMENT)

Purpose: Establish and manage a procurement process that incorporates cybersecurity and resilience considerations to obtain products and services that meet security requirements and support operational continuity. This includes documenting procurement procedures, integrating cybersecurity and resilience into contracts, and including stakeholder engagement. Regular reviews and adherence to best practices are crucial for maintaining an effective procurement program.

Procurement Process (PROCUREMENT) domain comprises three objectives:

1. Establish and Maintain Security-Conscious Procurement Program
2. Establish Procurement Controls and Requirements
3. Management Activities

A key step in addressing supply chain risks is the incorporation of security and support requirements in contracts with suppliers, vendors, and contractors. This involves establishing a strategy for procurement, and a resulting procurement program, that directs the organization's procurement and legal staff to include security and support requirements in contracts, Controls should be in place to validate that procurement requirements are being followed and steps are taken to address non-compliance.

Objectives and Practices

1. Establish and Maintain Security-Conscious Procurement Program

MIL1	a. Cybersecurity and resilience are considered in the procurement process, at least in ad hoc manner.
MIL2	b. The process for considering cybersecurity and resilience during procurement is documented. c. The documented process for considering cybersecurity and resilience during procurement is effectively implemented by the organization. d. The organization's documented process for addressing cybersecurity and resilience issues in the procurement process is risk-based (e.g., higher risk procurements get additional attention).
MIL3	e. The procurement process encourages the organization to seek the right to take a more active role in monitoring the supplier's activities for higher risk procurements (e.g., require a hardware or software bill of materials; review and approve hosting environments; set limits on who, when, and how the supplier can access the organization's assets or systems). f. The procurement program is reviewed at an organization-defined frequency to address its consideration of evolving cybersecurity and resilience issues. g. The procurement program follows applicable guidelines or industry best practices for the consideration of cybersecurity and resilience in the procurement process.

2. Establish Procurement Controls and Requirements

MIL1	a. Cybersecurity and resilience are considered to some degree in procurement contracts even if there is no documented organizational requirement to do so. b. Suppliers of key equipment generally are required in the procurement contracts to provide product support (e.g., security patches) for their products when a cybersecurity vulnerability is discovered.
MIL2	c. Procurement contracts include organization-defined cybersecurity and resilience requirements for suppliers. d. Procurement contracts require suppliers to provide product support when a cybersecurity vulnerability is discovered. e. Procurement contracts require suppliers to notify the organization when they discover a security vulnerability and take action to address identified vulnerabilities.
MIL3	f. Procurement contracts establish secure product design and development requirements based on risk to the organization (e.g., suppliers have a mature software and/or hardware secure design and development program, suppliers provide a bill of materials for their hardware and software products). g. In case of a cybersecurity incident involving a supplier's product or a provider's service, the procurement contract calls for the provider to offer technical support to the organization. h. The current security policy and program of suppliers is evaluated at an organization-defined frequency to determine if it still meets contractual requirements.

3. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support procurement activities. b. Key internal stakeholders are identified and involved in decision making for procurements, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving procurement. d. Adequate resources (people, funding, training, and tools) are provided to support procurement activities. e. Personnel performing activities involving procurement have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of procurement activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of procurement activities

6.8 Cybersecurity Architecture (CYBER-ARCH)

Purpose: Design and maintain the organization's cybersecurity configurations, security controls, and cybersecurity processes in alignment with resilience and cybersecurity requirements and risk tolerance, A key focus should be network and system integrity. Regularly review and adjust these elements to address risk and support organizational objectives.

The Cybersecurity Architecture (CYBER-ARCH) domain comprises seven objectives:

1. Develop Cybersecurity Architecture and Program Strategy
2. Secure Network Design Management
3. Establish IT Cybersecurity Protections
4. Establish OT Cybersecurity Protections
5. Establish Software/Firmware Protections
6. Data Security Management
7. Management Activities

The cybersecurity architecture provides an overarching plan for how security is to be engineered in a way that transcends point solutions for individual assets. This domain provides a structured architectural framework for considering for detecting, resisting, reacting to, and recovering from cybers disruptions. This includes tactics including segmentation, choice of hosting solutions, cryptographic controls, and audit trails. Aligned with an organization's enterprise architecture strategy and program, the cybersecurity architecture informs practices related to risk management, situation analysis, and event and incident response.

Cybersecurity architecture extends beyond networks and digital assets; it also includes application security including processes such as secure software design and development. Data security, for data at rest and in motion, is also an objective for cybersecurity architecture.

To be effective, the cybersecurity architecture must be sufficiently documented so that it can be communicated to stakeholders. It must also be governed to the extent that it is periodically reviewed and updated as necessary to address security concerns and align with the organization's cybersecurity and resilience program.

Objectives and Practices

1. Develop Cybersecurity Architecture and Program Strategy

MIL1	a. The organization has a cybersecurity strategy, even if it is developed and managed in an ad hoc manner.
MIL2	b. The organization has a cybersecurity strategy that is developed and managed following a documented process c. A cybersecurity program is developed and documented that aligns with the organization's cybersecurity strategy. d. The organization's cybersecurity strategy and program cover all IT and OT systems and networks.
MIL3	e. Self-evaluations of the organization's cybersecurity strategy and program are conducted at an organization-defined frequency and in response to defined triggers (e.g., significant changes to computer systems or networks, the organizational structure, or the threat environment). f. Threat and risk assessments are used to inform the organization's cybersecurity program. g. The developed cybersecurity program supports the organization's predefined states of operation.

2. Secure Network Design Management

MIL1	a. Network design is constructed with resilience in mind, at least in an ad hoc manner. b. Uninterrupted power supply is incorporated in network design for network hops (switches connecting inverters), at least in an ad hoc manner. c. Redundant SCADA controllers are generally incorporated in network design (in case a primary SCADA controller fails), at least in an ad hoc manner.
MIL2	d. Resilience is incorporated into the network design following a documented process. e. Uninterrupted power supply is incorporated in network design for network hops (switches connecting inverters) following a documented process. f. Redundant SCADA controllers are incorporated in network design following a documented process. g. Assets that are critical for operations are logically or physically placed into higher security zones than those that support non-critical functions. h. Network security protections implement the principles of least privilege and least functionality.
MIL3	i. Network design is reviewed and updated (as needed) at an organization-defined frequency and when defined triggers occur (e.g., system and threat environment changes). j. All assets are segmented into specific security zones based on cybersecurity requirements. k. OT systems operate autonomously from IT systems to ensure continuation of OT operations in case of IT system outage. l. Network security controls only allow authorized devices to have access to a network. m. The network architecture enables the isolation of compromised assets.

3. Establish IT Cybersecurity Protections

MIL1	a. IT systems are separated, at least in an ad hoc manner, using either physical or logical methods of segmentation. b. Endpoint protections (e.g., security applications, secure configuration, host monitoring) are implemented, at least in an ad hoc manner, to protect high priority IT assets.
MIL2	c. IT systems are separated employing either physical or logical methods of segmentation following a documented process. d. Endpoint protections (e.g., host monitoring, security applications, secure configuration, host monitoring) are implemented to protect high priority IT assets when/where feasible, following a documented process. e. Utilization of removable media on IT systems is regulated by policy and/or technological controls. f. The physical operating environment of IT assets (e.g., temperature, moisture) is regulated to safeguard their operation.
MIL3	g. Physical or logical methods to separate IT systems (and IT and OT systems) are inspected and updated at an organization-defined frequency or when defined triggers occur (e.g., significant changes to systems or the threat environment). h. Firmware configuration and changes are regulated throughout the IT asset lifecycle. i. Security controls (e.g., allowlists, configuration settings) are implemented on IT assets to prevent the execution of unauthorized code.

4. Establish OT Cybersecurity Protections

MIL1	a. OT systems are separated, at least in an ad hoc manner, from each other and IT systems using either physical or logical methods of segmentation. b. Endpoint protections (e.g., security applications, secure configuration, host monitoring) are implemented, at least in an ad hoc manner, to protect high priority OT assets.
MIL2	c. OT systems are separated, following a documented process, from each other and IT systems using either physical or logical methods of segmentation. d. Endpoint protections (e.g., security applications, secure configuration, host monitoring) are implemented, following a documented process, to protect high priority OT assets when/where feasible. e. Utilization of removable media on OT systems is regulated by methods such as limiting USB devices usage and overseeing external hard drives. f. The physical operating environment of OT assets (e.g., temperature, moisture) is regulated to safeguard their operation.
MIL3	g. Physical or logical methods to separate OT systems (and IT and OT systems) are reviewed and updated at an organization-defined frequency or when defined triggers occur (e.g., significant changes to systems or the threat environment). h. Firmware configuration and changes are regulated throughout the OT asset lifecycle. i. Security controls (e.g., allowlists, configuration settings) are implemented on OT assets to prevent the execution of unauthorized code.

5. Establish Software/Firmware Protections

MIL1	a. Before deploying software, the software's security is considered, at least in an ad hoc manner.
MIL2	b. Before deploying software, the software's security is considered following a documented process.

	c. Internally created software for high priority assets is developed following secure software design and development practices.
MIL3	d. Internally created software deployed on any asset is developed following secure software design and development practices. e. Before deployment, the security of new and updated applications is independently evaluated (by a party not involved in the development of the software—this may be a member of the organization or an external consultant). f. Software security testing (e.g., static, dynamic, penetration testing) is conducted on internally developed software and customized applications on an organization-defined frequency and when triggered by system changes and external events.

6. Data Security Management

MIL1	a. Sensitive data at rest is safeguarded, at least in an ad hoc manner.
MIL2	b. Sensitive data at rest is safeguarded following a documented process. c. The transmission of sensitive data is safeguarded, when practical, following a documented process. d. Cryptographic controls are applied to both data at rest and data in transit for sensitive data when practical. e. A cryptographic “key management” infrastructure (including the key generation, storage, destruction, update, and revocation) is implemented to facilitate the use of cryptographic controls. f. Security controls to limit data exfiltration (e.g., the use of data loss prevention tools) are implemented.
MIL3	g. The cybersecurity architecture incorporates additional safeguards for data stored on assets susceptible to loss or theft (e.g., full-disk encryption). h. The cybersecurity architecture incorporates safeguards to prevent unauthorized alterations to software, firmware, and data.

7. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support cybersecurity architecture activities. b. Key internal stakeholders are identified and involved in decision making for cybersecurity architecture, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving cybersecurity architecture. d. Adequate resources (people, funding, training, and tools) are provided to support cybersecurity architecture activities. e. Personnel performing activities involving cybersecurity architecture have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of cybersecurity architecture activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of cybersecurity architecture activities.

6.9 Workforce Management (WORKFORCE)

Purpose: Develop and manage plans and procedures to allow the workforce to be well-prepared and competent in handling resilience and cybersecurity events. This includes defining roles and responsibilities, providing necessary training and tools, and fostering a culture of resilience and cybersecurity awareness, all aligned with organizational risk tolerance and goals. Regular programmatic reviews and updates maintain workforce readiness and effectiveness.

To effectively carryout a security and resilience program, an aware and well-trained workforce is required. s organizations increasingly adopt advanced digital technology, the existing workforce and new hires require the education, training, and experience to address emerging security and resilience threats to digital assets and systems.

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

The Workforce Management (WORKFORCE) domain comprises five objectives:

1. Assign Resilience Responsibilities
2. Develop Cybersecurity Workforce
3. Implement Workforce Controls
4. Enhance Employee Cybersecurity Awareness
5. Management Activities

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

Implementing workforce controls includes personnel vetting, such as background checks, with extra vetting performed for positions that have access to assets needed to deliver important services. For example, system administrators typically have the ability to change configuration settings, modify or delete log files, create new accounts, and change passwords on critical systems, and specific measures are needed for protection of these systems from accidental or malicious behavior by this category of personnel.

Increasing the cybersecurity and resilience awareness of the workforce can be as important as technological approaches for improving these capabilities within the organization. For example, a cyberattack on an organization often starts with gaining some foothold into a company's IT or OT systems—for example, by gaining the trust of an unwary employee or contractor who then introduces media or devices into the organization's networks. The organization should share

information with its workforce on methods and techniques to identify suspicious behavior, avoid spam and spear phishing, and recognize social engineering attacks to avoid providing information about the organization to potential adversaries.

Objectives and Practices

1. Resilience Responsibilities

MIL1	a. Organization personnel understand, at least in an ad hoc manner, their roles and responsibilities during a resilience event. b. Organization staff who would need to respond to resilience events have at least some level of expertise or training, even if acquired in an ad hoc manner.
MIL2	c. Staff roles and responsibilities during a resilience event are a documented. d. The training requirements for organization staff who need to respond to a resilience event are documented. e. Specific personnel are designated as having primary and backup roles for key response and recovery activities during a resilience event.
MIL3	f. Responsibilities for identifying and addressing resilience events are reviewed and updated at an organization-defined frequency or when triggered by organizational changes. g. Roles and responsibilities during a resilience event are reviewed and updated at an organization-defined frequency and in response to defined triggers (e.g., significant system changes, organization/personnel changes, and threat profile changes).

2. Develop Cybersecurity Workforce

MIL1	a. Personnel with designated cybersecurity responsibilities during a resilience event have access to cybersecurity training, at least in an ad hoc manner. b. To support resilience in the event of a cyberattack, cybersecurity knowledge, skills, and ability requirements are understood, at least in an ad hoc manner.
MIL2	c. There is a documented process covering cybersecurity training for personnel with designated resilience responsibilities. d. To support resilience in the event of a cyberattack, cybersecurity knowledge, skill, and ability requirements and gaps are identified following a documented process. e. Identified gaps in cybersecurity knowledge, skills, and abilities are addressed through training, recruitment, and retention initiatives. f. Before granting access to high priority assets, individuals must undergo required cybersecurity training.
MIL3	g. The evaluation of cybersecurity training programs is conducted at an organization-defined frequency to assess their effectiveness, and appropriate adjustments are made when warranted. h. Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities.

3. Implement Workforce Controls

MIL1	a. Personnel vetting (e.g., background checks, drug tests) is conducted during the hiring process, at least in an ad hoc manner. b. Employee separation and transfer addresses potential cybersecurity and resilience program issues, at least in an ad hoc manner.
MIL2	c. Personnel vetting (e.g., background checks, drug tests) is conducted following a documented process during the hiring process. d. Periodic vetting is conducted at an organization specified frequency for members of the workforce with access to high priority assets. e. There is a documented process covering employee separation and transfer that addresses cybersecurity issues. f. Workforce staff responsibilities are documented regarding the safeguarding and appropriate utilization of IT, OT, and information assets.
MIL3	g. Workforce vetting is conducted for all positions (including those filled by external members of the workforce) at a level proportional to the risk associated with their position. h. A structured accountability process that incorporates disciplinary measures is enforced for personnel who violate the established cybersecurity policies and procedures.

4. Enhance Employee Cybersecurity Awareness

MIL1	a. Cybersecurity awareness activities are conducted, at least in an ad hoc manner, to foster a culture of cybersecurity and resilience among the workforce.
MIL2	b. Goals for the cybersecurity awareness program are developed and maintained. c. Goals for cybersecurity awareness align with identified threat profiles and risk estimates. d. A documented process directs cybersecurity awareness activities for the workforce.
MIL3	e. Workforce cybersecurity awareness activities are conducted at an organization-defined frequency and in response to trigger events (e.g., new types of cybersecurity threats, significant changes). f. Cybersecurity awareness activities are customized for specific job families. g. Cybersecurity awareness activities address a variety of predefined operational states, particularly those that may occur during a cyberattack that challenge operational resilience. h. The effectiveness of cybersecurity awareness activities is reviewed at an organization-defined frequency and after significant system changes or external events.

5. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified—even if they are not allocated, to support workforce management. b. Key internal stakeholders are identified and involved in decision making for the workforce management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving workforce management. d. Adequate resources (people, funding, training, and tools) are provided to support workforce management activities. e. Personnel performing activities involving workforce management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of workforce management activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of workforce management activities.

6.10 Situational Awareness (AWARENESS)

Purpose: Develop and maintain a framework for situational awareness that integrates activities and technologies to collect, analyze, and communicate operational and cybersecurity information. This includes implementing comprehensive logging, evaluating log data, and consolidating monitoring information into a Common Operating Picture (COP). Ensure the framework supports real-time operations and resilience objectives, with regular updates and resources aligned with organizational risks and best practices.

Situational awareness involves developing near-real-time knowledge of a dynamic operating environment. Internally, this may be accomplished through the logging and monitoring of IT, OT, and communication infrastructure assets important to the delivery of the function. It is also important to maintain knowledge of relevant, current events external to the enterprise. Once an organization develops situational awareness, it can align predefined states of operation to changes in the operating environment. The ability to shift from one predefined state to another can enable faster and more effective response to events or changes in the threat environment.

The Situational Awareness (AWARENESS) domain comprises four objectives:
1. Perform Logging
2. Perform Monitoring
3. Develop and Manage Situational Awareness
4. Management Activities

Logging should be enabled based on an asset's 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.

Monitoring and analyzing data collected in logs and through other means enables the organization to understand the function's operational and cybersecurity status. Effectively communicating the operational and cybersecurity status to relevant decision makers is the essence of situational awareness (sometimes referred to as a common operating picture). While many situational awareness implementations may include visualization tools, such as dashboards, maps, and other graphical displays, they are not necessarily required to achieve the goal.

Objectives and Practices

1. Perform Logging

MIL1	a. Logging access to, and the actions of, high priority assets is conducted where feasible, at least in an ad hoc manner.
MIL2	b. Logging is performed for high priority assets, where feasible, following a documented process. c. Logging requirements are established and maintained for IT and OT assets that could be targeted to achieve a threat objective. d. Logging requirements are defined and maintained for network and host monitoring infrastructure (e.g., web gateways, endpoint detection and response software, and intrusion and detection systems). e. Logging data is consolidated in a centralized location to support system monitoring.
MIL3	f. Stored logging data is backed up on a regular basis. g. Logging activities are reviewed and modified as warranted at an organization-defined frequency and when defined triggers occur (e.g., major system changes and significant changes in the threat profile or risk assessment).

2. Perform Monitoring

MIL1	a. Evaluations of log data and other cybersecurity monitoring activities are conducted, at least in an ad hoc manner. b. Log data that may be indicative of malicious activity is identified and investigated, at least in an ad hoc manner.
MIL2	c. Regular evaluations of log data and other cybersecurity monitoring activities involving IT systems are conducted following a documented process. d. Regular evaluations of log data and other cybersecurity monitoring activities involving OT systems are conducted following a documented process. e. Log data that may be indicative of malicious activity is documented and investigated following a documented process. f. Indicators for malicious activity are ingested into the organization's security, information, and event management (SIEM) system. g. Alarms and alerts are configured and used by a SIEM system to facilitate the detection of potential cyberattacks.
MIL3	h. High priority assets undergo enhanced monitoring activities. i. Indicators for anomalous activity are reviewed and updated at an organization-defined frequency and when defined triggers occur (e.g., system changes, changes in the threat or risk environment).

3. Develop and Manage Situational Awareness

MIL1	a. The organization consolidates monitoring information from various portions of the organization, including facility operations, cyber security, and physical security, to enhance situational awareness, at least in an ad hoc manner. b. Consolidated situational awareness information is communicated in at least an ad hoc manner to relevant internal stakeholders across the organization.

MIL2	c. The organization consolidates monitoring information from various portions of the organization, including facility operations, cyber security, and physical security, to enhance situational awareness following a documented process. d. Consolidated situational awareness information is communicated following a documented process to relevant internal stakeholders across the organization. e. Situational awareness reporting requirements are defined to support the timely dissemination of situational awareness information to stakeholders inside and outside of the organization.
MIL3	f. Relevant information is gathered from external sources and shared across the organization, as appropriate, to improve situational awareness. g. A process is established and maintained to gather, correlate, and analyze cybersecurity monitoring activities and enable near-real-time understanding of the cybersecurity state of facility operations. h. The processes involved in developing and disseminating situational awareness information are reviewed and updated at an organization-defined frequency and when defined triggers occur (e.g., significant system changes, changes in the threat or risk environment).

4. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support situational awareness activities. b. Key internal stakeholders are identified and involved in decision making for situational awareness, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving situational awareness. d. Adequate resources (people, funding, training, and tools) are provided to support situational awareness activities. e. Personnel performing activities involving situational awareness have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of situational awareness activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of situational awareness activities.

6.11 Event and Incident Response (RESPONSE)

Purpose: Establish, maintain, and exercise plans, procedures, and technologies to detect, analyze, respond to, and recover from resilience-challenging events and incidents. This includes the ability to respond to natural and human-caused events. This program is designed to maintain continuity of operations and be regularly reviewed and updated to address evolving threats and organizational needs, aligning with resilience risks and goals.

The Event and Incident Response domain comprises five objectives:

1. Event Detection and Reporting
2. Assess Events and Declare Incidents
3. Incident Response
4. Resilience and Continuity of Operations
5. Management Activities

Detecting resilience-challenging and cybersecurity events includes designating a forum for reporting events and establishing criteria for event prioritization. These criteria should align with the risk management strategy discussed in the Risk Management domain, ensure consistent valuation of events, and provide a means to determine what constitutes an event, when events are to be escalated, and the conditions that warrant the declaration of incidents.

Cybersecurity and other resilience-challenging events and incidents should be managed according to a response plan. Events and declared incidents may trigger external obligations, including reporting to regulatory bodies or notifying customers. Correlating multiple events and incidents and other records may uncover systemic problems within the environment.

Responding to incidents requires the organization to have a process to limit the impact of incidents to its functional and organizational units. The process should describe how the organization manages all phases of the incident life cycle, such as triage, handling, communication, coordination, and closure. Conducting lessons-learned reviews as a part of event and incident responses and continuity of operations helps the organization address the vulnerability that led to the incident.

Planning for continuity involves the necessary activities to sustain the function in the event of an interruption, such as a severe cybersecurity incident or a disaster. Ensuring that continuity plans address potential incidents requires consideration of known threats and identified categories of risk. Continuity plan testing should include cybersecurity incident scenarios that are used when assessing whether plans will function as intended during such incidents.

Objectives and Practices

1. Event Detection and Reporting

MIL1	a. Identified resilience-challenging events (including cybersecurity events) are reported to designated personnel, at least in an ad hoc manner.
MIL2	b. Identified resilience-challenging events (including cybersecurity events) are reported to designated personnel following a documented process. c. Guidelines for detecting resilience-challenging events (including cybersecurity events) are developed (e.g., what qualifies as a cybersecurity event, how to identify cybersecurity events). d. Resilience-challenging events (including cybersecurity events) are (or would be) identified and reported following the established guidelines.
MIL3	e. Resilience-challenging events (including cybersecurity events) information is (or would be) correlated to facilitate incident analysis by identifying trends, patterns, and other shared characteristics. f. Detection activities for resilience-challenging events (including cybersecurity events) are updated at an organization-defined frequency or when triggered by changes in the established threat profile or risk assessment.

2. Assess Cybersecurity Events and Declare Incidents

MIL1	a. Detected resilience-challenging events (including cybersecurity events) are evaluated, at least in an ad hoc manner. b. Resilience-challenging events (including cybersecurity events) are classified, at least in an ad hoc manner, as incidents when the event may cause harm to the organization.
MIL2	c. Guidelines for declaring a resilience-challenging event (including a cybersecurity event) as an incident are established and documented. d. Cybersecurity events are evaluated following a documented process to facilitate the declaration of cybersecurity incidents. e. Cybersecurity events and incidents are documented and tracked until resolved.
MIL3	f. Cybersecurity incident declaration guidelines are reviewed and updated as needed at an organization-defined frequency or when warranted by a triggering event (e.g., changes in cybersecurity risk). g. Guidelines for declaring incidents (including cybersecurity incidents) are aligned with the organization's cybersecurity risk tolerance. h. Resilience-challenging events and incidents (including ones associated with cybersecurity) are correlated to identify trends, patterns, and other shared characteristics.

3. Incident Response

MIL1	a. Personnel who would need to respond to a resilience-challenging event or incident (including cybersecurity ones) know their role and responsibilities, at least in an ad hoc manner. b. To limit incident impact and restore regular operations, the organization is prepared to respond to resilience-challenging incidents (including cybersecurity ones), at least in an ad hoc manner. c. Internal and external reporting of incidents is performed, at least in an ad hoc manner.

MIL2	d. Incident response personnel are identified, and roles are assigned following a documented process. e. Incident response plans and procedures are developed and managed for all phases of the incident lifecycle. f. Responses to incidents are conducted according to developed plans and procedures. g. Internal and external stakeholders (e.g., senior executives, incident response teams, affected suppliers, customers, applicable government agencies) are notified of incidents following a documented process.
MIL3	h. Incident response exercises (including those focused on cybersecurity events) are conducted at an organization-defined frequency and lessons learned are used to update response plans as warranted. i. Incident response plans are reviewed and updated as needed at an organization-defined frequency and in response to triggers (e.g., changes in the cybersecurity threat environment or risk levels). j. Root-cause analyses for cybersecurity incidents are performed and appropriate corrective measures are taken. k. Incident response personnel engage in collaborative cybersecurity exercises (including cybersecurity exercises) with other facilities or organizations. l. Incident responses (including responses to cybersecurity incidents) leverage and trigger predefined operational states.

4. Resilience and Continuity of Operations

MIL1	a. The organization's personnel are prepared, at least in an ad hoc manner, to sustain or restore normal operations in the wake of a resilience-challenging incident. b. Backups of data are available, at least in an ad hoc manner. c. Spares for specific IT and OT assets are identified, at least in an ad hoc manner.
MIL2	d. Continuity plans are developed and documented to help sustain and restore operations in the wake of a resilience-challenging incident (including a cybersecurity incident). e. Assets (IT, OT, and information) essential for continuity of operations or responding to the incident are identified and documented. f. Data backups are routinely prepared following a documented process and the backups are readily available to support restoration activities. g. Backup data have rigorous protections from natural and human-caused incidents (e.g., they are isolated both physically and logically from their source).
MIL3	h. Spares for key IT and OT assets are available for timely deployment. i. Continuity plans incorporate the recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets essential for minimum operation of the facility. j. Data backups and spare assets (IT, OT, and information) are tested for operational continuity at an organization-defined frequency. k. Continuity plans are reviewed and updated (as warranted) at an organization-defined frequency and in the case of defined triggers (e.g., system or threat profile changes) that can impact resilience capabilities. l. Outcomes of continuity plan testing are compared to recovery objectives, and the plan is updated as warranted.

5. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support cybersecurity event and incident response. b. Key internal stakeholders are identified and involved in decision making for cybersecurity event and incident response, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving cybersecurity event and incident response. d. Adequate resources (people, funding, training, and tools) are provided to support cybersecurity event and incident response activities. e. Personnel performing activities involving cybersecurity event and incident response have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of cybersecurity event and incident response activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of cybersecurity event and incident response activities.

6.12 Resilience Program Management (PROG-MGMT)

Purpose: Establish and manage a comprehensive resilience and cybersecurity program that aligns with the organization's overall strategy and operational goals, providing an appropriate level of preparedness for, and recovery from, resilience-challenging events. This includes integrating strategic planning, governance, and regular updates to address evolving threats and organizational needs, while maintaining alignment with resilience, cybersecurity, and operational goals.

A resilience program is an integrated group of activities designed and managed to meet performance goals for the organization and/or the function. This 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 Resilience Program Management (PROGRAM) domain comprises four objectives:

1. Establish and Maintain Resilience Program Strategy
2. Develop and Manage Resilience Program
3. Incorporate Resilience in Rate Making/Cost Recovery Process
4. Management Activities

The resilience program strategy is established as the foundation for the program. In its simplest form, the program strategy should include a list of resilience goals/requirements 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. Further, sponsorship includes organizational support for establishing and implementing policies or other organizational directives to guide the program.

Objectives and Practices

1. Establish and Maintain Resilience Program Strategy

MIL1	a. The organization has a resilience program strategy, at least in an ad hoc manner.
MIL2	b. The organization has a resilience program strategy that is developed and managed following a documented process. c. The resilience program strategy defines goals for the organization's recovery from any resilience challenging event.

	d. The resilience program strategy is aligned with the organization's mission, strategic objectives, and risks. e. The resilience program strategy defines managements' roles, responsibilities, and accountability for overseeing resilience activities. f. Resilience program strategy identifies any applicable standards, guidelines, and compliance requirements that the program must meet. g. The resilience program strategy considers a cyberattack as a potential initiating event.
MIL3	h. The resilience program strategy is reviewed and updated (as warranted) at an organization-defined frequency and when defined triggers occur (e.g., major system changes, significant changes in the threat profile and risk assessments). i. The resilience program is consistent with energy sector best practices for resiliency and continuity of operations.

2. Develop and Manage Resilience Program

MIL1	a. Senior management, vested with appropriate authority, offers backing to the resilience program, at least in an ad hoc manner.
MIL2	b. Senior management with appropriate authority offers backing to the resilience program following a documented process. c. Senior management supports the development, maintenance, and enforcement of the cybersecurity resilience program. d. Responsibility for the cybersecurity resilience program is entrusted to a role with adequate authority. e. Internal and external stakeholders involved in resilience program management activities are identified and engaged. f. The resilience program achieves compliance with relevant legal and regulatory requirements.
MIL3	g. The resilience program considers cybersecurity in its response and recovery program in order to maintain an appropriate level of cybersecurity during the recovery from a resilience event. h. Resilience program activities are reviewed at an organization-defined frequency to ensure that they align with the overall resilience program strategy. i. Resilience program activities undergo independent reviews to verify compliance with cybersecurity policies and procedures and overall resilience program goals. j. The organization collaborates with external entities to help develop and implement cybersecurity resilience best practices, lessons learned, and new resilience capabilities.

3. Incorporate Resilience in Rate Making/Cost Recovery Process

MIL1	a. The organization's rate making and cost recovery process addresses resilience needs (in addition to reliability needs), even if only in an ad hoc manner. b. There is someone supporting the organization who monitors rate making and cost recovery issues that may affect resilience objectives, even if only in an ad hoc manner.

MIL2	c. Specific responsibility is assigned within the organization to support it in monitoring rate making and cost recovery issues (including industry trends) that may affect resilience objectives. d. The formal rate making and cost recovery process specifically addresses the need for funding resilience program activities.
MIL3	e. Clear messaging on the importance of resilience related investments is routinely made to regulators/stakeholders in order to enhance the rate making and cost recovery process. f. Approved rates support adequate funding for key resilience program activities and objectives.

4. Management Activities

MIL1	a. Resources (people, funding, training, and tools) are identified, even if they are not allocated, to support resilience program management. b. Key internal stakeholders are identified and involved in decision making for resilience program management, even if that involvement is ad hoc.
MIL2	c. Documented policies and/or procedures are established, followed, and maintained for activities involving resilience program management. d. Adequate resources (people, funding, training, and tools) are provided to support resilience program management activities. e. Personnel performing activities involving resilience program management have the skills and knowledge needed to perform their assigned responsibilities.
MIL3	f. Responsibility, accountability, and authority for the performance of resilience program management activities are assigned to personnel. g. External sources of information (e.g., international, national, or industry standards/guidance documents; good industry practices) are consulted in the design and implementation of resilience program management activities.

APPENDIX A: REFERENCES AND BIBLIOGRAPHY

The references below were either used in the development of the C2M2 or Sol-ReMM or are a source for further information regarding the practices identified within cybersecurity maturity models.

[Bass 2013]
Bass, L., Clements, P., & Kazman, R. *Software Architecture in Practice (3rd ed.).* Reading, MA: Addison Wesley 2013.

[CERT CSIRT FAQ]
Software Engineering Institute, Carnegie Mellon University. 2017. *CSIRT Frequently Asked Questions (FAQ)*. Retrieved May 30, 2019, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652

[CERT CSIRTs]
West Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, Mark. 2003. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Retrieved May 30, 2019, from Software Engineering Institute, Carnegie Mellon University website: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305

[CERT-RMM]
Caralli, R. A., Allen, J. H., & White, D. W., Young, L. R., Mehravari, N., Curtis, P. D., *CERT® Resilience Management Model, Version 1.2*, CERT Program, Software Engineering Institute, Carnegie Mellon University, Feb. 2016.
https://resources.sei.cmu.edu/library/assetview.cfm?assetID=508084

[CERT SGMM]
The SGMM Team. 2011, version 1.2. *Smart Grid Maturity Model: Model Definition* (CMU/SEI-2011-TR-025). Retrieved May 30, 2019, from Software Engineering Institute, Carnegie Mellon University website:
https://resources.sei.cmu.edu/library/assetview.cfm?assetid=10035

[CERT State of the Practice of CSIRTs]
Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. 2003. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-TR-001). Retrieved May 30, 2019, from Software Engineering Institute, Carnegie Mellon University website: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571

[CMMC]
Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, and Futures, Inc. 2020. *Cybersecurity Maturity Model Certification (CMMC) Model Overview*. Retrieved March 31, 2022, from: https://www.acq.osd.mil/cmmc/documentation.html

[CNSSI 4009]
Committee on National Security Systems. 2010. *National Information Assurance (IA) Glossary* (CNSS Instructions No. 4009). Retrieved May 30, 2019, from https://www.dni.gov/files/NCSC/documents/nittf/CNSSI4009_National_Information_Assurance.pdf

[DHS Cross-Sector Roadmap]
Industrial Control Systems Joint Working Group. 2011, revision 3.0. *Cross-Sector Roadmap for Cybersecurity of Control Systems*. United States Computer Emergency Readiness Team.

[DHS-DOE Energy Sector]
U.S. Department of Homeland Security and U.S. Department of Energy. 2015. *Energy Sector-Specific Plan*. Retrieved June 17, 2019, from https://www.dhs.gov/publication/nippssp-energy-2015

[DHS ICS]
Department of Homeland Security. 2019. *Cybersecurity and Infrastructure Security Agency-Industrial Control Systems.* Retrieved May 30, 2019, from https://ics-cert.us-cert.gov/

[DHS ICSJWG]
Department of Homeland Security. 2019. *Industrial Control Systems Joint Working Group.* Retrieved May 30, 2019, from https://ics-cert.us-cert.gov/Industrial-Control-Systems-JointWorking-Group-ICSJWG

[DHS NIPP]
Department of Homeland Security. 2013. *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience.* Retrieved June 17, 2019, from https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructuresecurity-and-resilience

[DHS PCII]
Department of Homeland Security. 2019. *Protected Critical Infrastructure Information (PCII) Program.* Retrieved May 30, 2019, from https://www.dhs.gov/pcii-program

[DHS Procurement]
U.S. Department of Homeland Security, Control Systems Security Program, National Cyber Security Division. 2009. *U.S. Department of Homeland Security: Cyber Security Procurement Language for Control Systems.*

[DOE Framework Implementation]

U.S. Department of Energy. 2015. *Energy Sector Cybersecurity Framework Implementation Guide.* Retrieved June 17, 2019, from https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

[DOE RMP]
U.S. Department of Energy. 2012. *Cybersecurity Risk Management Process (RMP) Guideline – Final (May 2012).* Retrieved June 17, 2019, from https://www.energy.gov/ceser/downloads/cybersecurity-risk-management-process-rmpguideline-final-may-2012

[DOE Roadmap]
U.S. Department of Energy. 2011. *Roadmap to Achieve Energy Delivery Systems Cybersecurity – 2011.* Retrieved June 17, 2019, from https://www.energy.gov/ceser/downloads/roadmap-achieve-energy-delivery-systemscybersecurity-2011

[FIRST]
Forum of Incident Response and Security Teams (FIRST). 2012. *CSIRT Case Classification (Example for Enterprise CSIRT).* Retrieved May 30, 2019, from https://www.first.org/resources/guides/csirt_case_classification.html

[IACCM BRM3]
International Association for Contract & Commercial Management (IACCM). 2003. *The IACCM Business Risk Management Maturity Model (BRM3).*

[ISA 99]
International Society of Automation (ISA). 2009. *Industrial Automation and Control Systems Security: Establishing an Industrial Automation and Control Systems Security Program* (ANSI/ISA-99.02.01-2009).

[ISACs]
National Council of Information Sharing and Analysis Centers (ISACs). 2019. Retrieved May 30, 2019, from https://www.nationalisacs.org/

[ISO/IEC 2:2004]
International Organization for Standardization. 2004. *Standardization and Related Activities – General Vocabulary* (ISO/IEC 2:2004).

[ISO 27005:2011]
International Organization for Standardization. 2011. *Information Security Risk Management* (ISO 27005:2011)

[ISO/IEC 21827:2008]
International Organization for Standardization. 2008. *Systems Security Engineering – Capability Maturity Model (SSE-CMM)* (ISO/IEC 21827:2008).

[ISO/IEC 27001:2005]
International Organization for Standardization. 2008. *Information Security Management Systems* (ISO/IEC CD 27001:2005).

[ISO/IEC 27002:2005]
International Organization for Standardization. 2008. *Code of Practice for Information Security Management* (ISO/IEC27002:2005).

[ISO 28001:2007]
International Organization for Standardization. n.d. *Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans – Requirements and Guidance* (ISO/ IEC20001:2007).

[MIT SCMM]
Rice, Jr., J. B., & Tenney, W. 2007. "How risk management can secure your business future." *Massachusetts Institute of Technology Supply Chain Strategy, 3(5), 1-4*. Retrieved May 30, 2019, from http://web.mit.edu/scresponse/repository/rice_tenney_SCS_RMM_junejuly_2007.pdf

[MITRE ATT&CK]
The MITRE Corporation. 2021. MITRE ATT&CK. Retrieved May 18, 2021, from https://attack.mitre.org

[MITRE ATT&CK for ICS]
The MITRE Corporation. 2021. MITRE ATT&CK for Industrial Control Systems. Retrieved April 14, 2022, from https://collaborate.mitre.org/attackics/index.php/Main_Page

[NDIA ESA]
National Defense Industrial Association, System Assurance Committee. 2008. *Engineering for System Assurance, Version 1.0.*

[NIST CSF]
National Institute of Standards and Technology. 2018. *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Retrieved May 30, 2019, from https://www.nist.gov/cyberframework/framework

[NIST Framework]
National Institute of Standards and Technology. 2012. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.* Retrieved May 30, 2019, from https://www.nist.gov/sites/default/files/documents/smartgrid/NIST_Framework_Release_20_corr.pdf

[NIST Security Considerations in SDLC]
Ross, R., McEvilley, M. Carrier Oren, J. 2016. *Systems Security* Engineering (NIST SP 800160 Volume 1). National Institute of Standards and Technology. Retrieved June 19, 2020, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

[NIST SP800-16]
Toth, P., & Klein, P. 2014. *A Role-Based Model for Federal Information Technology/Cybersecurity Training* (3rd Draft) (NIST Special Publication 800-16, Revision 1.0, 3rd Draft). National Institute of Standards and Technology. Retrieved June 19, 2020, from https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/archive/2014-03-14

[NIST SP800-30]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2012. *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Revision 1.0). National Institute of Standards and Technology. Retrieved March 31, 2022, from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[NIST SP800-37]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (NIST Special Publication 800-37 Revision 2). Retrieved June 19, 2020, from https://csrc.nist.gov/publications/detail/sp/800-37/rev2/final

[NIST SP800-40]
Souppaya, M., Scarfone, K. 2013. *Guide to Enterprise Patch Management Technologies* (NIST Special Publication 800-40, Revision 3). National Institute of Standards and Technology. Retrieved June 19, 2020, from https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

[NIST SP800-50]
Wilson, M., & Hash, J. 2003. *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-50/final

[NIST SP800-53]
National Institute of Standards and Technology, Joint Task Force Transformation Initiative. 2020. *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53, Revision 5). Retrieved March 31, 2022, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[NIST SP800-61]
Cichonski, P., Millar, T., Grance, T., & Scarfone, K. 2012. *Computer Security Incident Handling Guide* (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[NIST SP800-64]
Ross, R., McEvilley, M., Oren, J. 2018. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (NIST Special Publication 800-160, Volume 1). National Institute of Standards and Technology. Retrieved June 19, 2010, from https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

[NIST SP800-82]
Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. *Guide to Industrial Control Systems (ICS) Security*, pg. B-14 (NIST Special Publication 800-82, Revision 2). National Institute of Standards and Technology. Retrieved May 3, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[NIST SP800-83]
Souppaya, M., Scarfone, K. 2013. *Guide to Malware Incident Prevention and Handling* (NIST Special Publication 800-83 Revision 1). National Institute of Standards and Technology. Retrieved June 19, 2019, from https://csrc.nist.gov/publications/detail/sp/800-83/rev1/final

[NIST SP800-128]
National Institute of Standards and Technology. 2011. *Guide for Security-Focused Configuration Management of Information Systems* (NIST Special Publication 800-128). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-128/final

[NIST SP800-137]
Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A.C., Orebaugh, A., Stine, K. 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (NIST Special Publication 800-137). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-137/final

[NIST SP800-150]
Johnson, C., Badger, M., Waltermire, D., Snyder, J., Skorupka, C. 2016. *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150). Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/sp/800-150/final

[NIST SP800-160]
Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. 2019. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach* (NIST Special Publication 800160 Volume 2). National Institute of Standards and Technology. Retrieved March 8, 2021, from https://csrc.nist.gov/publications/detail/sp/800-160/final

[NIST NVD]
National Institute of Standards and Technology. 2019. *National Vulnerability Database.* Retrieved May 30, 3019, from https://nvd.nist.gov/vuln-metrics/cvss

[NISTIR 7622]
Boyens, J., Paulsen, C., Bartol, N., Shankles, S., & Moorthy, R. 2012. *Notional Supply Chain Risk Management Practices for Federal Information Systems* (NISTIR 7622). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/nistir/7622/final

[NISTIR 7628 Vol. 1]
The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cybersecurity, Volume 1: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements* (NISITIR 7628). National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/nistir/7628/rev1/final

[NISTIR 7628 Vol. 3]
The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cybersecurity, Volume 3: Supportive Analyses and References* (NISITIR 7628 *).* National Institute of Standards and Technology. Retrieved May 30, 2019, from https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

[NISTIR 8053]
Garfinkel, S. L. 2015. *De-Identification of Personal Information* (NIST Internal Report 8053). National Institute of Standards and Technology. Retrieved May 3, 2021, from https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

[NISTIR 8276)
Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. 2021. *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (NISTIR 8276). National Institute of Standards and Technology. Retrieved March 31, 2022, from https://csrc.nist.gov/publications/detail/nistir/8276/final

[PPD-21]
The White House. n.d. *Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience*. Retrieved May 30, 2019, from https://obamawhitehouse.archives.gov/thepress-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-andresil

[OECD Reducing Systemic Cybersecurity Risk]
Sommer, P., & Brown, I. 2011. *Reducing Systemic Cybersecurity Risk.* Organisation for Economic Co-operation and Development. Retrieved May 30, 2019, from http://www.oecd.org/governance/risk/46889922.pdf

[SEI CMM]
Paulk, M., Weber, C., Garcia, S., Chrissis, M.B., & Bush, M. 1993. *Key Practices of the Capability Maturity Model* (Version 1.1, Technical Report CMU/SEI-93-TR-25). Software Engineering Institute, Carnegie Mellon University. Retrieved May 30, 2019, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11965

[SCADA AU RMF]
IT Security Expert Advisory Group. 2012. *Generic SCADA Risk Management Framework for Australian Critical Infrastructure.* Retrieved May 30, 2019, from http://www.tisn.gov.au/Documents/SCADA-Generic-Risk-Management-Framework.pdf

[Situation Awareness in Dynamic Systems]
Endsley, M. 1995. “Toward a Theory of Situation Awareness in Dynamic Systems.” *Human Factors*, pp. 32-64.

APPENDIX B: GLOSSARY

The following glossary presents terms used in the So;-ReMM, C2M2, and other supporting maturity modeling references.

Term	Definition	Source
Access	Ability and means to enter a facility, to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	Adapted from CNSSI 4009
access control	Limiting access to organizational assets only to authorized entities, such as users, programs, processes, or other systems. See *asset*.	Adapted from CNSSI 4009
Access and Authorization Management (ACCESS)	Create and manage processes for handling identities, credentials, and access controls to the organization's assets.	Sol-ReMM
access management	Management processes to ensure that access granted to the organization's assets is commensurate with the risk to critical infrastructure and organizational objectives. See *access control* and *asset*.	Adapted from CERT-RMM
ad hoc	In the context of the model, *ad hoc* (that is, formed or used for a special purpose without policy or a plan for repetition) 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, such as a prescribed plan (verbal or written), policy, or training. The quality of the outcome may vary significantly depending on who performs the practice; the methods, tools, and techniques used; and the priority given a particular instance of the practice. High-quality outcomes may be achieved with experienced and talented personnel; however, in an ad hoc practice the lessons learned are typically not captured at the organizational level. This may lead to approaches and outcomes that are difficult to repeat or improve across the organization. While documented policies or procedures are not essential to the performance of a practice, the long-term performance of many practices greatly benefits from documentation.	C2M2
all assets within the function	All assets that operate or are used within the function. These assets may not be considered important to the delivery of the function and may not be likely to be leveraged to achieve a threat objective (for example, printers, radios, badge readers, or telephones).	C2M2
anomalous	Inconsistent with or deviating from what is usual, normal, or expected.	Merriam-Webster.com

Term	Definition	Source
asset	IT and OT hardware and software, as well as information essential to operating the function. The definition also includes interconnected or interdependent business and technology systems and the environment in which they operate.	C2M2
Asset Inventory (ASSET)	The domain with the purpose to manage the organization's IT and OT assets,	Sol-ReMM
Asset Configuration and Change Management (CHANGE-MGMT)	The domain with the purpose to manage the configuration and change management program for the organization's critical assets including information technology (IT), operations technology (OT), and information assets	Sol-ReMM
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
assets that are important to the delivery of the function	The subset of assets that is required for a normal state of operation of the function and output of the function's products or services. Loss of an asset that is considered "important to the delivery of the function" may not directly result in an inability to deliver the function but could result in operations being degraded. Identification of this asset should focus on loss of the service or role performed by that asset and should not include consideration of asset redundancy or other protections.	C2M2
assets within the function that may be leveraged to achieve a threat objective	Assets that may be used by the threat actor to achieve their goals) e.g., extortion, data manipulation, IP theft, customer data theft, sabotage). Multiple tactics may be used by the threat actor to achieve their goals. Examples of assets that may be leveraged by the attacker are: : • public-facing assets that may serve as an initial access point • individual assets that if compromised, may allow lateral movement within an organization's network • assets with administrative rights that would enable privilege escalation • information assets such as personally identifiable information that may cause harm to the organization or its stakeholders if lost, stolen, or disclosed See also *threat objective*.	C2M2
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to IT, OT, or information assets.	DOE Electricity Subsector Cybersecurity Risk Mgmt Process (RMP) Guideline

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
capacity management	Planning adequate budget, equipment, and tools to meet current and future operational needs of the organization.	C2M2
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
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 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 800128
controls	The management, operational, and technical methods, policies, and procedures—manual or automated—(that is, safeguards or countermeasures) prescribed for IT and OT assets to protect the confidentiality, integrity, and availability of those assets and their associated information assets.	DOE RMP
critical infrastructure	Assets that provide the essential services that underpin society. Nations possess 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, such as in the asset inventory is kept “current,” that is selected such that the risks to critical infrastructure and organization objectives associated with being out-of-date by the maximum interval between updates are acceptable to the organization and its stakeholders.	C2M2

Term	Definition	Source
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	Prevention and limitation of unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, and information assets to ensure their confidentiality, integrity, and availability.	Adapted from [NIST SP80037]
Cybersecurity Architecture (ARCHITECTURE)	The domain with the purpose to design and maintain the organization's cybersecurity configurations, security controls, and cybersecurity processes in alignment with resilience and cybersecurity requirements and risk tolerance,	Sol-ReMM
cybersecurity architecture	How cybersecurity practices and controls are structured and implemented to maintain the confidentiality, integrity, and availability of the organization's assets and services. See also *enterprise architecture*.	C2M2
cybersecurity controls	The administrative, operational, and technical measures (i.e., processes, policies, devices, practices, or other actions) prescribed for IT, OT, and information assets to manage their associated risk.	Adapted from [NIST SP800-82] and [NISTIR 8053]
cybersecurity event	See *event*.	C2M2
cybersecurity incident	See *incident.*	
cybersecurity incident lifecycle	See *incident lifecycle.*	
cybersecurity objectives	The ability to protect or defend the use of cyberspace from cyber-attacks. Measures taken to protect a computer or computerized system (IT and OT) against unauthorized access or attack.	C2M2
cybersecurity program	A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization 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.	C2M2
cybersecurity program strategy	A plan of action designed to achieve the performance targets that the organization sets to accomplish its mission, vision, values, and purpose for the cybersecurity program.	CERT-RMM

Term	Definition	Source
cybersecurity requirements	Requirements levied on IT and OT systems that are derived from organizational mission and business case needs (in the context of applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, and 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.	C2M2
cyber risk	The possibility of harm or loss due to unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, or information assets. Cyber risk is a function of impact, likelihood, and susceptibility.	C2M2
data	A collection of bits that may be processed, stored, or transmitted by an IT or OT system.	C2M2
data at rest	Data that is in some kind of storage, such as a hard drive or a server.	C2M2
data in transit	Data that is being transmitted via some kind of network, such as a private network or the internet.	C2M2
dependency risk	Dependency risk is measured by the likelihood and severity of damage if an IT or OT system is compromised due to a supplier or other third party on which delivery of the function depends. Evaluating dependency risk includes an assessment of the importance of the potentially compromised system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation. See also *supply chain risk.*	Adapted from NIST 7622, pg. 10
deprovisioning	To revoke or remove an identity's access to organizational assets. See also *provision.*	CERT-RMM
domain	In the context of the model structure, a domain is a logical grouping of cybersecurity practices.	C2M2
domain objectives	The practices within each domain are organized into *objectives*. The objectives represent achievements that support the domain (such as "Manage Asset Configuration" for the ASSET domain and "Increase Cybersecurity Awareness" for the WORKFORCE domain). Each of the objectives in a domain comprises a set of practices, which are ordered by maturity indicator level.	C2M2

Term	Definition	Source
enterprise	The highest-level organizational unit that encompasses the function to which the Sol-ReMM is being applied. Some enterprises may consist of multiple organizations (e.g., a holding company with one or more operating companies). Other enterprises may have a more homogenous structure that does not necessitate any differentiation between the terms *enterprise* and *organization*. For those organizations, *enterprise* and *organization* may be used interchangeably. See also *organization* and *function.*	C2M2
enterprise architecture	The design and description of an enterprise's entire set of IT and OT assets: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. See also *cybersecurity architecture*.	Adapted from DOE RMP
entity	In the context of identity and access management, someone or something having separate or distinct existence (such as a person, object, system, or process) that requires access to an asset.	MerriamWebster.com Adapted from CERT-RMM
establish and maintain	The development, implementation, and ongoing support of the object of the practice (such as a program). Development and implementation would typically result in documentation that captures important information about the activity. Ongoing support would typically result in periodic reviews and updates when events occur that may impact operations (such as major changes to IT and OT assets or change to the threat environment). 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 kept up to date including review, corrective actions, addressing changes in requirements, and improvements.	Adapted from CERT-RMM
event	Any anomalous occurrence in a system or network that is related to a cybersecurity requirement. Depending on their potential impact, some events need to be declared as incidents. See also *cybersecurity requirements*.	NIST 800-61

Term	Definition	Source
Event and Incident Response, Continuity of Operations (RESPONSE)	The domain with the purpose to establish, maintain, and exercise plans, procedures, and technologies to detect, analyze, respond to, and recover from resilience-challenging events and incidents.	Sol-ReMM
function	In Sol-ReMM, *function* refers to the part of the organization that is being evaluated based on the model. A function may or may not align with organizational boundaries. For example, the function might be a line of business, a network security zone, or a single facility.	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
guidelines	A set of recommended practices produced by a recognized authoritative source representing subject matter experts and community consensus or produced internally by an organization. See also *standard*.	C2M2
identity	The set of attribute values (that is, characteristics) by which a person or entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that person or entity from any other.	Adapted from CNSSI 4009
Identity and Access Management (ACCESS)	The Sol-ReMM domain with the purpose to create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.	C2M2
impact	Negative consequences of an event or action. Impact is a key component in understanding the severity of a particular risk. Impact from cybersecurity incidents might include, for example, response costs, regulatory fines, and lost income from reputation damage.	C2M2
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit impact. Criteria for declaration of an incident are determined by the organization. See also *event*.	Adapted from CERT-RMM

Term	Definition	Source
incident lifecycle	The stages of an incident from detection to closure. Collectively, the incident lifecycle includes the processes of detecting, reporting, logging, triaging, declaring, tracking, documenting, handling, coordinating, escalating and notifying, gathering and preserving evidence, and closing incidents. Events also follow the incident lifecycle.	Adapted from CERT-RMM
information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.	NIST SP80039
information assets	Information of value to the organization, such as business data, intellectual property, customer information, contracts, security logs, metadata, set points, and operational data. Information Assets may be in digital or non-digital form.	Adapted from CERT-RMM
Information Sharing and Analysis Center (ISAC)	An Information Sharing and Analysis Center (ISAC) shares critical information with industry participants on infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning.	Adapted from Electricity Sector Information Sharing and Analysis Center website home page
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 interdependent business and technology 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 and is followed routinely as part of corporate culture. 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. See also *maturity indicator level.*	C2M2 & CERT-RMM

Term	Definition	Source
least privilege	A security control that addresses the potential for abuse of authorized privileges. The organization employs the concept of least privilege by allowing only authorized access for users (and processes acting on behalf of users) who require it to accomplish assigned tasks in accordance with organizational missions and business functions. Organizations employ the concept of least privilege for specific duties and systems (including specific functions, ports, protocols, and services). The concept of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and 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
logical control	A software, firmware, or hardware feature (that is, computational logic, not a physical obstacle) within an IT or OT system that restricts access to and modification of assets only to authorized entities. For contrast, see *physical control*.	Adapted from CNSSI 4009 definition of "internal security controls"
maturity	The extent to which an organization has implemented and institutionalized the cybersecurity practices of the model.	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). 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 activities in the domain.	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
multifactor authentication	Use of two or more factors to achieve verification of an identity. Factors include (1) something you know, such as a password or PIN, (2) something you have, such as a cryptographic identification device or token, (3) something you are, such as a biometric marker, and (4) something that indicates that you are where you say you are, such as a GPS token. See also *authentication*.	Adapted from NIST 800-53
objectives	*See domain objectives* and *organizational objectives*.	
operational resilience	The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk. See the related term *operational risk*.	CERT-RMM
operating states	See *predefined states of operation*.	C2M2
operations technology (OT)	In the context of the model, OT assets refer to assets that are on the OT segment of the organization's network and are necessary for service delivery or production activities. Examples include industrial control systems, building management systems, fire control systems, process control systems, safety instrumented systems, Internet of things (IoT) devices, and physical access control mechanisms. Most modern control systems include assets traditionally referred to as IT, such as workstations that use standard operating systems, database servers, or domain controllers.	C2M2
organization	In the context of the model, the organization is the part of the enterprise that encompasses the function selected for Sol-ReMM evaluation or improvement. In smaller enterprises, the terms *enterprise* and *organization* are often interchangeable. See also *function* and *enterprise*.	Adapted from DOE RMP
organizational objectives	Performance targets set by an organization. See also *strategic objectives*.	Adapted from CERT-RMM
periodically and according to defined triggers	A review or activity that occurs at defined, regular time intervals and at the occurrence of defined events. The organization-defined frequency and threshold values are commensurate with risks to organizational objective and critical infrastructure.	Adapted from SEI CMM Glossary

Term	Definition	Source
physical access control	A type of control that prevents physical access to and modification of information assets or physical access to technology and facilities. Physical controls often include such artifacts as card readers and physical barrier methods.	CERT-RMM
plan	A detailed formulation of a program of action.	Merriam-Webster.com
policy	A documented description of roles, responsibilities, and expected or required actions related to a particular area of organizational activity, such as asset management.	C2M2
position description	A set of responsibilities that describe a role or roles filled by an employee. Also known as a job description.	C2M2
practice	An activity described in the model that can be performed by an organization to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function, commensurate with the risk to critical infrastructure and organizational objectives.	C2M2
Procurement Process (PROCURE)	The domain with the purpose to establish and manage a procurement process that incorporates cybersecurity and resilience considerations to obtain products and services that meet security requirements and support operational continuity.	Sol-ReMM
predefined 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 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, 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.	C2M2
privacy	The assurance that information about an individual is collected, used, and disclosed only as authorized by that individual or as permitted under privacy laws and regulations.	C2M2
procedure	In the model, *procedure* is synonymous with *process*.	

Term	Definition	Source
process	A series of discrete activities or tasks that contribute to the fulfillment of a task or mission.	CERT-RMM (business process)
provision	To assign or activate an identity profile and its associated roles and access privileges. See also *deprovisioning*.	CERT-RMM
recovery point objectives (RPO)	The point in time to which data is restored after an incident. The point to which information used by the function must be restored to enable the activity to operate on resumption.	C2M2
recovery time objectives (RTO)	The period of time within which systems, applications, or functions must be recovered after an incident. RTO includes the time required for assessment, execution and verification. The period of time following an incident within which a product or service or function or an activity must be resumed, or resources must be recovered.	C2M2
Resilience Program Management (PROGRAM)	The domain with the purpose to establish and manage a comprehensive resilience and cybersecurity program that aligns with the organization's overall strategy and operational goals, providing an appropriate level of preparedness for, and recovery from, resilience-challenging events.	Sol-ReMM
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. See also *cyber risk*.	DOE RMP
risk analysis	A risk management activity focused on understanding the likelihood and potential impact of risks, prioritizing risks, and determining a path for addressing risks. Analysis determines the importance of each identified risk and is used to facilitate the organization's response to the risk.	Adapted from CERT-RMM
risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, and reputation), resources, other organizations, and the Nation, resulting from the operation of IT and OT systems.	DOE RMP
risk criteria	Objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches.	C2M2

Term	Definition	Source
risk management program	The program and supporting processes to manage cyber 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 Assessment and Management (RISK)	The domain with the purpose to establish and maintain a resilience and cybersecurity risk management program to identify, assess, prioritize, and address risks.	Sol-ReMM
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 register	A structured repository where identified risks are recorded to support risk management.	C2M2
risk response	Accepting, avoiding, mitigating, or transferring risk to organizational operations, resources, and other organizations.	DOE RMP
secure software development	Developing software using recognized processes, secure coding standards, best practices, and tools that have been demonstrated to minimize security vulnerabilities in software systems throughout the software development lifecycle. An essential aspect is to engage programmers and software architects who have been trained in secure software development.	C2M2
security zone	A grouping of systems and components with similar cybersecurity requirements. Zone access is restricted by network and security devices.	C2M2
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 or roles; (ii) conducting information system support functions with different individuals, such as 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

Term	Definition	Source
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 or affect how well a system functions. It involves the collection of data, such as via sensor networks, data fusion, and data analysis (which may include modeling and simulation) to support automated or human decision making (for example, concerning OT system functions). Situational awareness also involves appropriate use of alarms and the presentation of the results of the data analysis in some form, such as using data visualization techniques that aid human comprehension and allow operators or other personnel to quickly grasp the key elements needed for good decision making.	Adapted from SGMM Glossary
Situational Awareness (SITUATION)	The domain with the purpose to develop and maintain a framework for situational awareness that integrates activities and technologies to collect, analyze, and communicate operational and cybersecurity information.	Sol-ReMM 2
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.	C2M2
stakeholder	An external organization or an internal or external person or group that has a vested interest in the organization's cybersecurity practices, such as government, vendors, sector organizations, regulators, and internal business lines. Stakeholders may be involved in performing a given practice or may oversee, benefit from, or be dependent upon the quality with which the practice is performed.	Adapted from CERT-RMM
standard	A standard is a document, established by consensus, which provides rules, guidelines, or characteristics for activities or their results. See also *guidelines*.	Adapted from ISO/IEC Guide 2:2004
states of operation	See *predefined states of operation.*	
strategic objectives	The performance targets that the organization sets to accomplish its mission, vision, values, and purpose.	CERT-RMM
strategic planning	The process of developing strategic objectives and plans for meeting these objectives.	CERT-RMM

Term	Definition	Source
Supply Chain Management (SUPPLY)	The domain with the purpose to establish and manage relationships with key suppliers to ensure resilience and security in the supply chain, including evaluation, performance oversight, and backup arrangements.	Sol-ReMM
supply chain risk	Supply chain risk is measured by the likelihood and severity of damage if an IT or OT system is compromised by a supply chain attack and considers the importance of the system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation. Supply chain attacks may involve manipulating computing system hardware, software, or services at any point during the lifecycle. Supply chain attacks are typically conducted or facilitated by individuals or organizations that have access through commercial ties, leading to stolen critical data and technology, corruption of the system or infrastructure, or disabling of mission-critical operations. See also *risk* and *supply chain*.	Adapted from NIST 7622, p. 7 & p. 10
susceptibility	The probability that an event, once initiated or attempted, will succeed and lead to the realization of a risk. Susceptibility is a component of the overall probability of a risk and is the component of probability that the organization has the most control over.	C2M2
threat	Any actor 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, or denial of service. This includes actors without intention to cause adverse impact (e.g., insider mistakes).	Adapted from DOE RMP
Threat and Vulnerability Management (THREAT)	The domain with the purpose to establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to resilience and cybersecurity threats and vulnerabilities	Sol-ReMM
threat objective	Threat objectives are the potential outcomes of threat actor activities that are of concern because they would have negative impacts on the organization. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage. Threat actors may leverage multiple tactics or techniques, like those defined in the MITRE ATT&CK frameworks (for Enterprise or Industrial Control Systems) to achieve their goals. Threat objective examples include data manipulation, intellectual property theft, damage to property, denial of control, loss of safety, and operational outage.	C2M2

Term	Definition	Source
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, OT, and information assets of an organization and to the organization itself, identifying feasible threats, describing the nature of the threats, and evaluating their severity.	C2M2
triggers	Events (such as a change to IT infrastructure) and time intervals (such as monthly or yearly) that are used to indicate when an activity should occur, such as a review and possible update of the risk management strategy.	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.	Adapted from NISTIR 7628 Vol. 1, pp. 8
vulnerability assessment	Systematic examination of IT or OT assets or systems 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. This may include several types of assessments, such as a paper-based assessment, tool-based vulnerability scanning, and penetration tests.	DOE RMP
Workforce Management (WORKFORCE)	The Sol-ReMM domain with the purpose to develop and manage plans and procedures to allow the workforce to be well-prepared and competent in handling resilience and cybersecurity events.	Sol-ReMM

APPENDIX C: ACRONYMS

Acronym	Definition
C2M2	Cybersecurity Capability Maturity Model
C2M2-Nuclear	Cybersecurity Capability Maturity Model - Nuclear
CCPA	California Consumer Privacy Act
CERT®-RMM	CERT® Resilience Management Model
CISA	Cybersecurity and Infrastructure Security Center
CMMC	Cybersecurity Maturity Model Certification
COP	Common operating picture
COTS	commercial off-the-shelf
CSF	NIST Framework for Improving Critical Infrastructure Cybersecurity
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
FIRST	Forum of Incident Response and Security Teams
FERC	Federal Energy Regulatory Commission
HR	human resources
IAM	identity and access management
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	information technology

MIL	maturity indicator level
NERC	North American Electric Reliability Corporation
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
OT	operations technology
PCI DSS	Payment Card Industry Data Security Standards
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RMP	Electricity Subsector Cybersecurity Risk Management Process Guideline
SCADA	supervisory control and data acquisition
SEI	Software Engineering Institute
SLA	service level agreement
Sol-ReMM	Solar Cybersecurity Resilience Maturity Model
TTP	tactics, techniques, and procedures
US-CERT	United States Computer Emergency Readiness Team