PNNL-30545

ELECTRICITY SUBSECTOR TRANSMISSION RESILIENCE MATURITY MODEL (TRMM) User Guide

Draft Version 1.0

October 2020

North American Transmission FORUM

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Pacific Northwest NATIONAL LABORATORY

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The U.S. Department of Energy (DOE), Electric Power Research Institute (EPRI) and North American Transmission Forum (NATF), and Pacific Northwest National Laboratory (PNNL) acknowledge the dedication and technical expertise of the organizations and individuals who have provided the critiques, evaluations, and modifications to enable the development of this first release of the Transmission Resilience Maturity Model (TRMM) Guide.

Department of Energy	PNNL	NATF/EPRI Members	
David Meyer	Cliff Glantz	Jeff Schraufnagel	ATC
EPRI	Paul Skare	Dave McRee	Duke Energy
Kevin Berent	Sri Nikhil Gourisetti	Tom Pruitt	Duke Energy
Laura Fischer	Grace Mcnally	Steve Ladd	Duke Energy
NATF	Devan Farrell	Floyd Galvan	Entergy
Ed Ernst	Easton Gervais	Mark Peterson	Great River Energy
Lynna Estep		Gordie Halt	ITC
Ken Keels		Dennis Snook	OPPD
		Todd Lucas	Southern Company
		Grant Smedley	Salt River Project
		Mark Wehlage	Xcel Energy
		Brian Long	Xcel Energy

CAUTIONARY NOTE

Intended Scope and Use of This Publication

The guidance provided in this publication is intended to address the implementation and management of resilience practices, most specifically the practices of transmission business units (TBU). This guidance is not intended to replace or subsume other resilience-related activities, programs, processes, or approaches that electricity subsector organizations have implemented or intend to implement. 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 resilience program.

1. INTRODUCTION

The electric transmission sector is facing a range of threats to its functionality that are either new, more severe than experienced in earlier years, or more well understood. Such threats include more frequent and more severe extreme weather events, wildfires, droughts, and human-caused physical and cyberattacks. They also include geological, electromagnetic, and biological events. The novelty or increasing severity of these threats creates a significant need for transmission owners to implement programs to prevent, prepare for, respond to, and recover from such incidents. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats, and the transmission networks are essential components of that infrastructure.

The Electricity Subsector Transmission Resilience Maturity Model (TRMM) is a tool that a transmission organization can use to objectively evaluate and benchmark its currently established transmission resilience strategies, programs, policies, and investments, in order to target and prioritize enhancements where needed.

The TRMM was developed to address the unique characteristics of the transmission system. The model can enable users to:

- evaluate and benchmark their organization's resilience capabilities, effectively and consistently
- prioritize actions and investments to improve the resilience of their systems
- share transmission-related knowledge, best practices, and relevant references within their organization and with business partners as a means to improve resilience capabilities
- contribute to increasing the overall resilience of the Nation's transmission systems.

The TRMM provides descriptive rather than prescriptive industry-focused guidance. The model content is presented at a high level of abstraction so that it can be interpreted by transmission organizations of various types, structures, and sizes. The model is designed to an be easy-to-use, self-assessment tool.

1.1 Definition and Scope of Resilience in the Model

In general, resilience is the ability to endure different kinds of shocks and survive or readily bounce back. Of particular interest to TRMM users is the resilience of the transmission system. While there are several definitions of resilience related to the electric subsector, North American Transmission Forum's (NATF) public document, "Transmission System Resiliency – An Overview," provides a good construct of transmission system resilience:

> "the ability of the system and its components (i.e., both the equipment and human components) to minimize damage and improve recovery from **non-routine** disruptions, including **high impact, low frequency** (HILF) events, in a reasonable amount of time"[1]

The key points of the definition have been highlighted with bold text for emphasis as it relates to three key elements of resilience events: (1) large impacts, (2) long duration, and (3) non-routine. The delineation between reliability and resilience is not a bright line; there is some overlap between the two. In addition, the delineation is not uniform across organizations and geographic locations and depends on things such as an organization's inherent threats, its vulnerabilities due to system design, and societal concerns (e.g., different priorities in urban and rural areas).

Many events will have aspects of both reliability and resilience. Generally, as we move into more resilience-weighted events, these events will include longer durations and higher impacts to a widespread area. Impacts can be in the form of degraded assets and tools, as well as other grid and societal impacts.

Figure 1.1 augments the definition of resilience by providing contrasting examples on the reliability-resilience continuum. For example, having one Bulk Electric System (BES) transformer vandalized is most clearly on the reliability end of the spectrum. The 2013 Metcalf event[2], with multiple transformers targeted in conjunction with communications channels, falls somewhere in the middle of the spectrum. In comparison, we can hypothesize a high-impact resilience event where 20 critical BES stations are simultaneously targeted.

Another example from Figure 1.1 is a Category 3 hurricane in Florida, which likely falls more on the reliability side of the diagram. This is due to the unfortunate reality that Florida utilities have to frequently deal with those strong storms. In response, Florida utilities have taken steps to harden their systems to perform better by withstanding hurricane-force winds. Contrast that scenario with Hurricane Sandy's impact on the Northeast in 2012. At its peak, Sandy was a Category 3 storm. However, it was not even classified as a hurricane when it reached the Northeast. The combination of winds and flooding were unprecedented (non-routine). The impacts were devastating to not only the electric system, but all infrastructure in the affected areas which spanned a large area in the northeastern United States with large population centers (large impacts). Because of the significant impacts, restoration was more on the order of weeks rather than days (long duration). Had the storm maintained more of its original strength, the impacts and, therefore, duration could have been even more significant.

[1] https://www.natf.net/docs/natf/documents/resources/resiliency/transmission-system-resiliency-an-overview.pdf
[2] https://en.wikipedia.org/wiki/Metcalf_sniper_attack

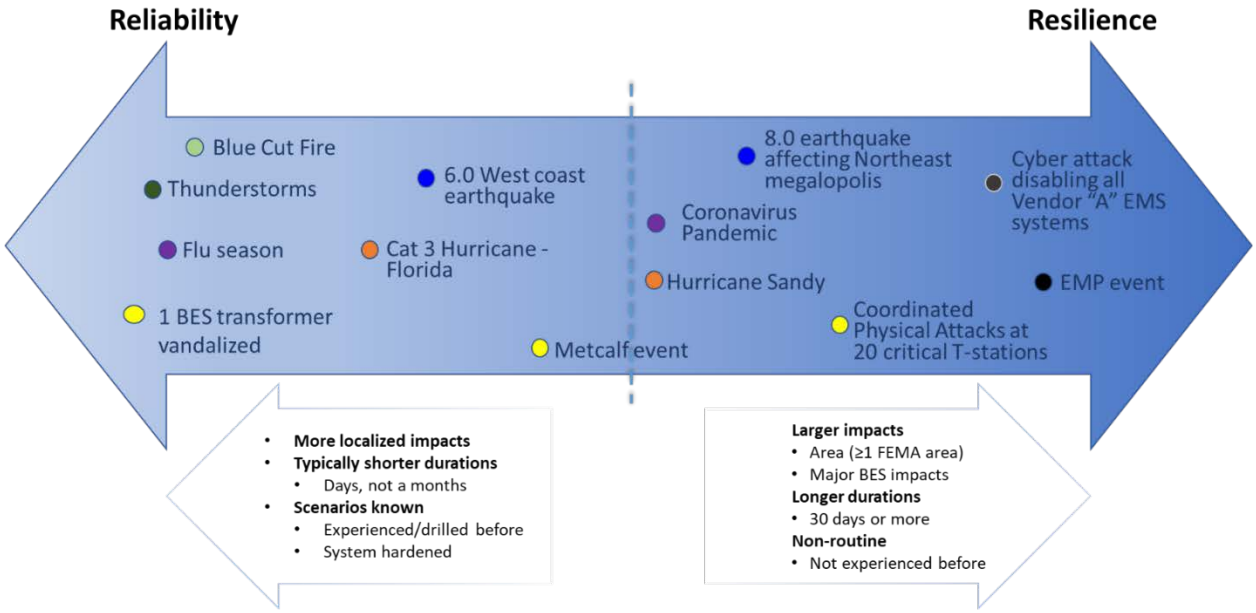

Figure 1.1: Reliability-Resilience Continuum Diagram

The scope of the TRMM was designed to cover all stages of a resilience event including: (1) preparation (longer-term and shorter-term), (2) operations during a resilience event, and (3) recovery after an event. This is illustrated in Figure 1.2.

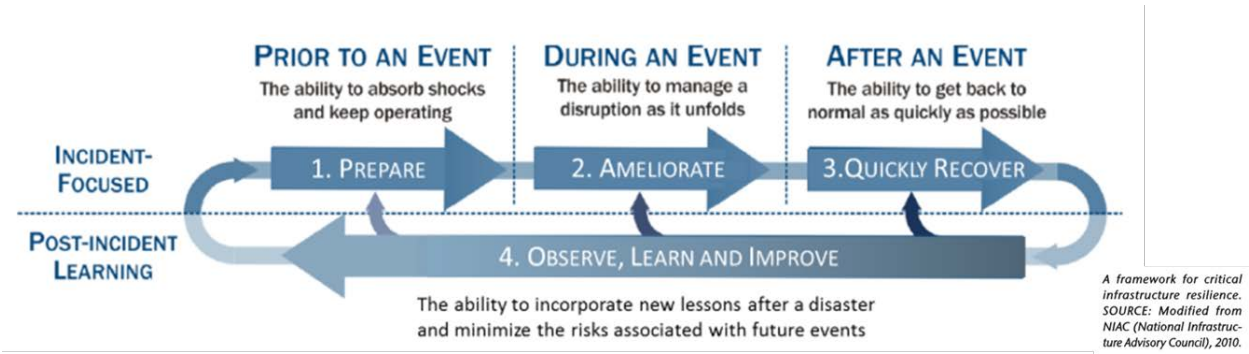

Figure 1.2: Sequence of the NIAC Resilience Construct3

Prior to an event, there is long-term preparation for potential events. That allows time for investments in hardening, redesign, acquisition of spare parts, workforce training, etc. Shorter-term preparations involve using the resources you have or can engage quickly in the limited time available to prepare for potential impacts. All stages rely heavily on robust response and

[3] National Infrastructure Advisory Council's "A Framework for Establishing Critical Infrastructure Resilience Goals", October 19, 2010 https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf

recovery plans. Flexibility and scalability of those plans are key in managing the range of resilience event impacts.

In addition, the model includes aspects to ensure experience from near misses and events are incorporated as lessons learned into the resilience program and strategies.

1.2 Intended Audience

The TRMM enables transmission organizations to evaluate resilience capabilities consistently, communicate capability levels in meaningful terms, and prioritize resilience investments. The model can be used by any transmission organization, regardless of ownership, structure, or size. Within the organization, various stakeholders may benefit from familiarity with the model. This document is intended to be relevant to people in the following organizational roles[4]:

- **Decision-makers** (executives) who control the allocation of resources and the management of risk in their organizations; these are typically senior leaders. This includes the organization's TRMM sponsor.
- **Leaders** with responsibility for managing organizational resources and operations associated with the domains of this model. (See section 7. MODEL DOMAINS for more information on the content of each TRMM domain.)
- **Practitioners** with responsibility for supporting the organization in the use of this model (including planning and managing changes in the organization after application of the model). This includes the organization's TRMM subject matter experts (SMEs).
- **Facilitators** with responsibility for leading a self-assessment of an organization based on this model and the associated toolkit and analyzing the self-assessment results.

1.3 Benefits

The TRMM was designed by industry SMEs and provides many benefits to users in a confidential and secure manner. The tool is conveniently internet accessible[5], but all inputs and results remain on the user's local computer, i.e., no central database or repository is maintained.

The TRMM supports sharing of resilience-related knowledge and best practices internally. In addition, TRMM results can be voluntarily shared by organizations performing self-assessments with industry associations in order to share best practices. Benefits include:

- consistent evaluation, trending, and benchmarking of resilience capabilities
- identification of strengths and weaknesses in existing programs
- reduction of liability risks and pressure for regulatory oversight.

[4] For more information about roles, please refer to the TRMM Facilitator Guide. The Facilitator Guide may be downloaded from https://trmm.labworks.org/resources

[5] Access the TRMM tool at: https://trmm.labworks.org/trmmtool

In addition, the TRMM provides a roadmap for managing risks and challenges, implementation of risk-based, cost-effective programs, and overall program improvements. Ultimately, this can help alleviate some resilience-related customer and stakeholder concerns.

1.4 Document Organization and Additional Resources

This document introduces the model and presents the TRMM's main structure and content.

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

Table 1.1: Target Audiences for Document Sections

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

Chapter 2 presents background information on the model and its development. Chapter 3 provides an overview of the U.S. transmission sector. Chapter 4 describes several core concepts that are important to the content and structure of the TRMM. Chapter 5 describes the architecture of the TRMM. Chapter 6 provides guidance on how to use the model. Chapter 7 contains the model itself - the model's objectives and practices, organized into nine domains. Chapter 7 also includes examples for each domain. Appendix A includes references that were either used in the development of this document or provide further information about the practices identified within the model. Appendix B is a glossary of relevant terms. Appendix C defines the acronyms used in this document. Appendix D provides the revision history of this document.

Other TRMM information products are also available on the TRMM webpage [https://trmm.labworks.org/trmmtool]. Click the Resource button and links to several informational products will be displayed. These include, but are not limited to the following documents:

- The TRMM Facilitator Guide – This provides instructions to internal or external personnel who are facilitating the TRMM self-assessment. It includes information on meeting logistics and helpful hints on how to conduct and schedule an assessment.
- TRMM Supplementary Explanations – This document provides a short, supplementary explanation for each practice in the TRMM. This can help clarify the meaning and intent of a practice.

- TRMM Instructional Videos – These instructional videos show how to access and enter assessment data into the tool, save and load assessment data, and generate and interpret the informational products in the TRMM Core Assessment Report.

2. BACKGROUND

The TRMM was developed by a diverse group of transmission resilience experts and maturity model developers. This group included:

- leaders and transmission experts from a range of transmission-owning utilities who are members of the Electric Power Research Institute (EPRI), the North American Transmission Forum (NATF), or both
- senior technical representatives from the NATF
- transmission system experts from EPRI
- maturity modeling and electric sector researchers from Pacific Northwest National Laboratory (PNNL)
- leadership and support from the U.S. Department of Energy (DOE) Office of Electricity.

Wherever possible, the TRMM initiative leveraged and built upon existing efforts, models, and best practices to enhance transmission resilience.

In particular, the TRMM was designed to use the framework from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), a model that has been in widespread use within the energy sector since 2014. The ES-C2M2 was developed as a result of a White House initiative, led by the DOE in partnership with the U.S. Department of Homeland Security (DHS) and in collaboration with private- and public-sector experts, and representatives of asset owners and operators within the electricity subsector. The ES-C2M2 used the National Infrastructure Protection Plan framework[6] as a public–private partnership mechanism to support the development of the model. In its basic architecture, the TRMM is similar to the ES-C2M2, but it focuses on the topic of transmission resilience rather than cybersecurity.

Further, TRMM is designed to be applied in parallel with ES-C2M2, not to encompass it. Transmission owners who have cybersecurity concerns are strongly advised to address them through ES-C2M2, not TRMM. Organizations that apply both models may find it helpful to coordinate the implementation of their cybersecurity program and their transmission resilience program.

2.1 Model Development Approach

The initial version of this model was developed during 2019. The following themes characterized the development approach:

- **Public–private partnership**: Numerous industry and government organizations participated in the development of this model, bringing a broad range of knowledge, skills, and experience to the team. The model was developed collaboratively with an industry

[6] https://www.cisa.gov/national-infrastructure-protection-plan

advisory group through a series of working sessions and was revised based on feedback from more than 20 industry experts.

- **Best practices and sector alignment**: The model builds upon and ties together a number of existing transmission resilience resources and initiatives and was informed by a review of threats to the transmission system. Leveraging related work by NATF and its members shortened the development schedule and helped to ensure that the model would be relevant and beneficial to the transmission entities.
- **Descriptive, not prescriptive**: This model was developed to provide descriptive, not prescriptive, guidance to help transmission organizations develop and improve their resilience capabilities. As a result, the model's practices can tend to be abstract so that they can be interpreted by utilities of various structures, functions, and sizes.
- **Pilot to test, validate, and improve**: A draft of this model was piloted with five utilities to test, evaluate, and improve it.
- **Focus:** The TRMM focuses on higher-level, business or organizational practices related to resilience. Opportunities for continuous improvements will be monitored, including opportunities for addressing more technical topics either through improvements to the model or other initiatives.

3. ABOUT THE ELECTRIC TRANSMISSION SECTOR

The electricity portion of the energy sector includes the generation, transmission, distribution, and marketing of electricity. The use of electricity is ubiquitous, spanning all sectors of the U.S. economy. The electricity subsector accounts for 40 percent of all energy consumed in the United States. Electricity system facilities are dispersed throughout the North American continent. Although most assets are privately owned, no single organization represents the interests of the entire subsector.

The electric transmission network is the backbone of the Nation's energy grid and consists of more than 600,000 circuit miles of lines, 240,000 of which are considered high-voltage lines (230 Kilovolts and greater). These lines link the generators of electricity to the distributors, transporting electricity to local electric companies, which in turn deliver it to customers.

The transmission network provides a range of benefits that ultimately accrue to customers in the form of reliable service and a reduction in costs, by: improving power flow and relieving congestion, facilitating robust wholesale market competition, enabling a diverse and changing energy portfolio, and mitigating damage and limiting customer outages during severe weather events and other major disruptions to the system.[7]

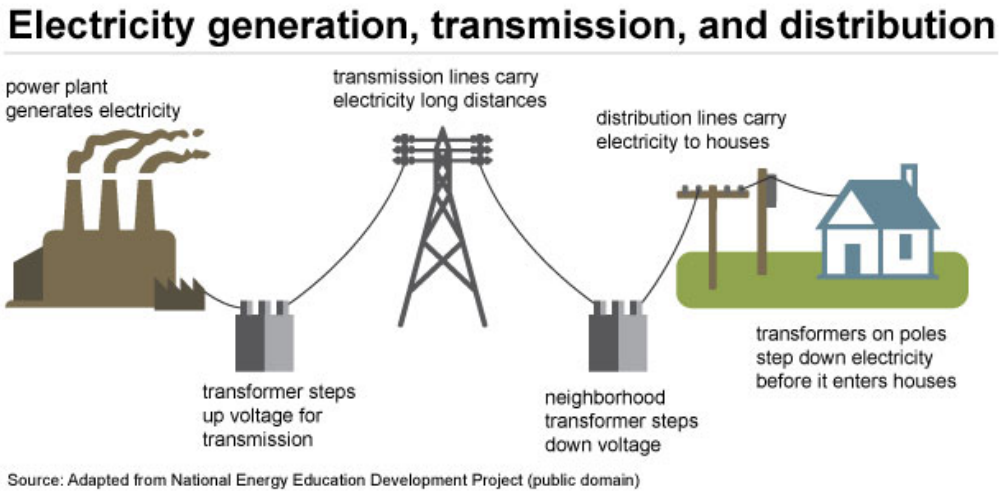

Figure 3.1: Electric Grid Energy Delivery System

To apply this model to the electricity subsector, the advisory group focused on the transmission business unit (TBU). However, the model is adaptable and can be customized to support other business units (e.g., generation, distribution) or the entire enterprise.

[7] https://www.eei.org/issuesandpolicy/transmission/Pages/default.aspx

4. CORE CONCEPTS

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

4.1 Maturity Model

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

A maturity model thus enables identification of a benchmark against which an organization can evaluate the level of capability represented by its current practices, processes, and methods, and set its own goals and priorities for improvement. When a model is widely used in a particular industry (and assessment results are shared, perhaps with anonymity), organizations can benchmark their performance against other similar organizations. In the case of the TRMM, the model must be flexible enough to accommodate the diversity within the transmission industry, including the reality that different entities face widely different combinations of threats to their resilience.

To measure progression, maturity models typically have "levels" along a scale — TRMM uses a scale of maturity indicator levels (MIL) 0–3, which are described in Section 5.2. A set of attributes defines each level. If an organization demonstrates all 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 what a future, more mature state would look like
- identify the specific capabilities it must attain to reach that future state.

To ensure the accuracy and legitimacy of the model as a self-assessment tool, the MIL attributes that are the heart of the model must be developed and validated by recognized experts in the relevant technical field.

4.2 Transmission Assets

Many TRMM attributes, or practices, refer to transmission *assets*. When evaluating how completely a practice is performed, be sure to consider its applicability to the full range of such assets, including:

- transmission equipment, such as transmission lines, transmission substations

- transmission support equipment, such as tools for repairing transmission system equipment, vehicles for transporting materials and personnel, tools for system analyses, monitoring, and managing restoration processes
- essential operating information such as weather conditions, forecast, and status of key equipment and IT systems
- others, such as energy control centers.

4.3 Relationship to the Risk Management Process

The TRMM is designed to support the enterprise's risk management process, as depicted in Figure 4.1. Risk management is the "identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities."[8]

Figure 4.1: Risk Management Process

4.3.1 Risk Framing

The top-most box in Figure 4.1 is "Risk Framing." It involves the identification and characterization of threats and vulnerabilities. Threats may come either in the form of a natural event or a human-caused event. Many threats are external to the organization, but there are important internal threats to consider.

4.3.2 Risk Assessment

Moving clockwise around Figure 4.1, the next stage in the process is "Risk Assessment." It involves characterizing the consequences of adverse events and the likelihood or susceptibility

[8] https://en.wikipedia.org/wiki/Risk_management

to the events that could trigger those consequences. Figure 4.2 illustrates the role risk framing plays in risk assessment. Specifically, threat and vulnerability information are two key inputs in the estimation of consequences, along with an understanding of how the electric power systems, the utility, its customers, and stakeholders will react to adverse events.

The assessment of relative risk involves a consideration of consequences, threats, and vulnerabilities – where threats and vulnerabilities help estimate the likelihood that the transmission system will experience the predicted consequences. This approach serves as a proxy for the more traditional risk framework that uses the probability of an outcome and the consequences of that outcome to estimate risk (i.e., risk = probability × consequence.) This approach is necessary since severe resilience events are, by definition, low frequency with little or no historical data to derive quantitative estimates of likelihood for use in risk assessments. Because of that, risk estimates for transmission resilience events are often qualitative or are based on the relative susceptibility of the transmission system to a threat exploiting system vulnerabilities.

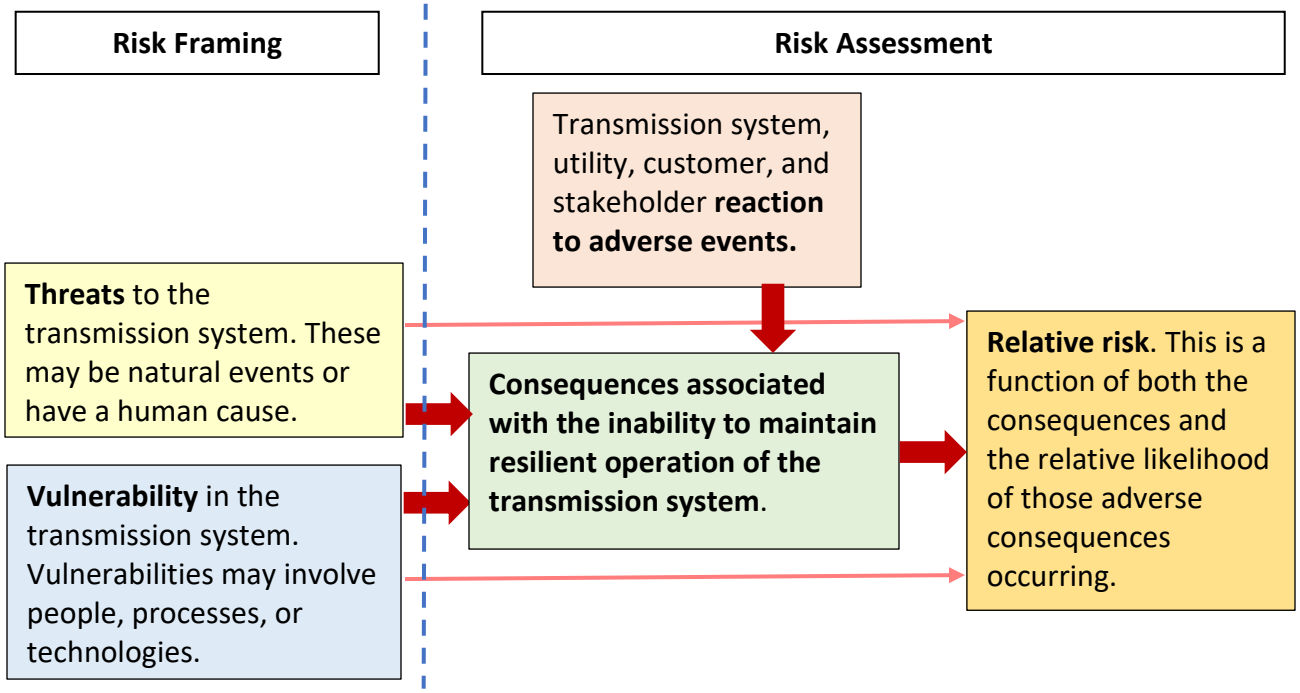

Figure 4.2. Risk Assessment Components

4.3.3 Risk Response

The "Risk Response" step in Figure 4.1 involves identifying and characterization ways to mitigate risks and then selecting and implementing the selected approach to achieve risk reduction.

4.3.4 Risk Monitoring

The "Risk Monitoring" step in Figure 4.1 involves assessing the actual change in risk status after implementing risk reduction measures and monitoring how risk factors evolve over time.

The TRMM identifies the establishment of a resilience risk management strategy that aligns with the enterprise's broader risk management strategy as an indicator of a mature risk management program. Resilience risk is an important component of the overall business risk environment. When resilience risk management activities feed into the enterprise risk management strategy and program, transmission resilience risks can be factored into broader enterprise decisions that consider a wide array of risks, tolerance for risk, and risk response approaches.

4.4 Design Basis Resilience Events

Design basis resilience events for the TRMM are defined as postulated, reasonable, worst-case resilience events used to establish the parameters to which a TBU will design and plan its system resilience capabilities. Designs and plans will include capabilities to withstand events, continue transmission system operations or quickly bounce back from events, and minimize the risk to the health and safety of society at large.

Typically, organizations have some kind of design basis events that govern their designs and plans. However, these have been traditionally based mainly upon reliability. The design basis resilience events go a step beyond those traditional design basis events and consider more extreme scenarios that the organization should be cognizant of and able to address. The intent is to use a combination of strategic and targeted mitigations, along with scalable and flexible plans, to address the design basis resilience events and meet the organization's resilience goals.

Defining a suite of design basis resilience events that address credible high impact/low frequency events can be the foundation for implementing a robust resilience program. Design basis resilience events are intended to be threshold events against which capabilities of absorbing, responding to, and recovering from a challenging blow are tested. Therefore, these design basis resilience events should be of sufficient magnitude regarding duration, geographical area impacts, and impacts to key equipment. In addition to magnitudes, the types of impacts, especially to key equipment should be considered.

For example, the following magnitudes may be considered when developing design basis resilience events:

- Significant transmission system impacts may persist for a duration of weeks or months.
- There is significant geographic area of impact. For many portions of the U.S., this might involve an area with a radius of 500 miles or more.

  - Impacts in this radius would affect utilities, other critical entities, and society at large.
  - Utilities and critical entities within this radius would experience a substantial initial reduction in operability – perhaps a drop in operability to 25% or less.

Also consider the need for various kinds of design basis resilience events. For example, impacts of cyber-related events can be very different from weather or physical attacks and pandemics imply another type of impact. Therefore, it is important to consider applicable kinds of design basis resilience events in order to cover equipment, personnel, and other impacts.

The design basis resilience events provide a measuring stick for resilience capabilities in areas represented by the various TRMM domains. For example:

- Event and response plans could be developed to be scalable and flexible in order to address the design basis resilience events.
- Special communications capabilities could be secured considering the impact to primary communications that are possible for the design basis resilience events.
- Backup capabilities and spare plans could consider the size and duration of the design basis resilience events.
- Alternate suppliers and transportation capabilities could be planned for considering the impacts implied by the design basis resilience events.
- Training plans, exercises, and drills could be based on design basis resilience events.
- Support plans for the workforce and their families could be developed based on the impacts and durations implied by the design basis resilience events.

4.5 Transmission Operations

In this model, the term *transmission operations* refers to all activities of the transmission organization or TBU.

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

4.6 Hierarchy of Terms for Formal Documentation

The TRMM uses several terms whose definitions are important to understand when using the model. These terms are defined in APPENDIX B: GLOSSARY at the end of this document. Figure 4.3 highlights for comparison and understanding a few terms regarding the hierarchy of organizational directives regarding transmission resilience activities.

Figure 4.3 indicates that "strategy," the high-level game plan, is at the top level of the hierarchy. Coming out of the strategy are a more detailed set of "plans" that specify broad courses of action. Coming out of plans are the "processes" that details the specifics of what needs to be done. Coming out of processes are the "procedures" that inform personnel of how processes are to be carried out.

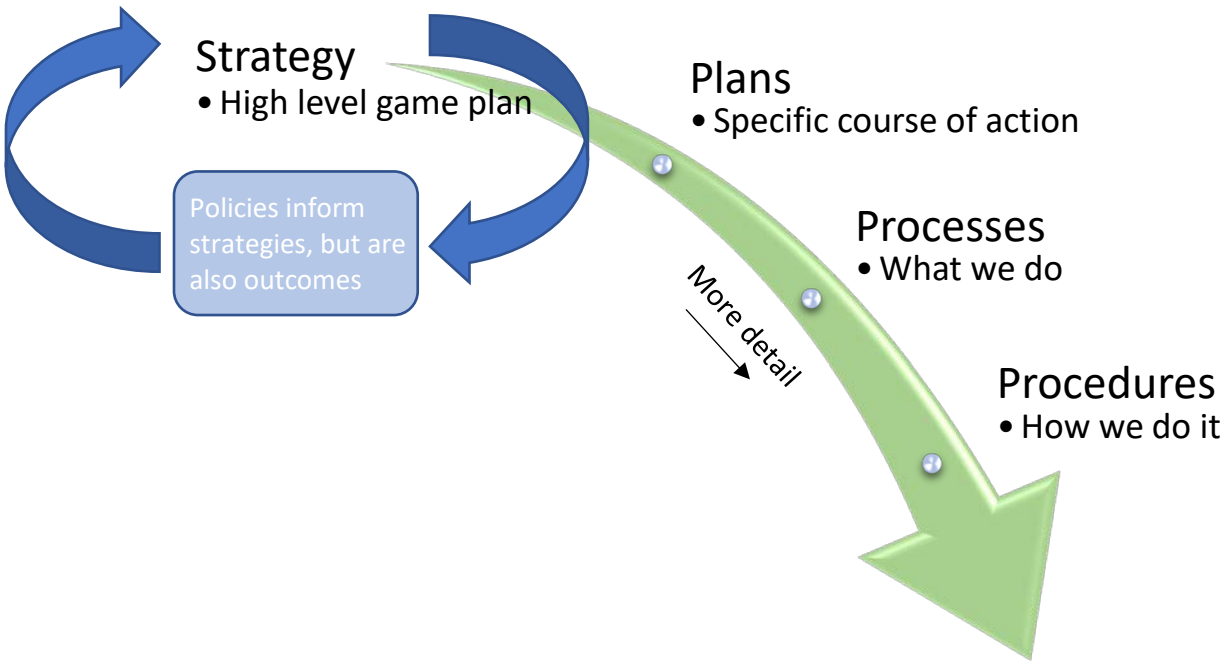

Figure 4.3: Hierarchy of Terms used in the TRMM

5. MODEL ARCHITECTURE

The TRMM builds upon a combination of existing transmission-related standards, frameworks, programs, and initiatives. The model provides flexible guidance to help transmission organizations develop and improve their resilience-related capabilities. As a result, the model's practices tend to be highly abstracted, so that they can be interpreted for organizations of various structures and sizes.

The following sections provide additional information about the terms used to describe the TRMM: domains, objectives, practices, and maturity indicator levels (MILs).

5.1 Domains

Domains are the key topical areas of the model. Each of the model's domains contains a structured set of transmission resilience-related practices. Each set of practices represents the activities an organization can perform to establish or achieve greater capability in the domain.

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

The practices within each domain are organized under objectives, which represent achievements that support the domain. Each of the objectives in a domain has a set of pertinent practices, which are ordered by MIL.

Figure 5.1 summarizes this relationship of the elements in the model.

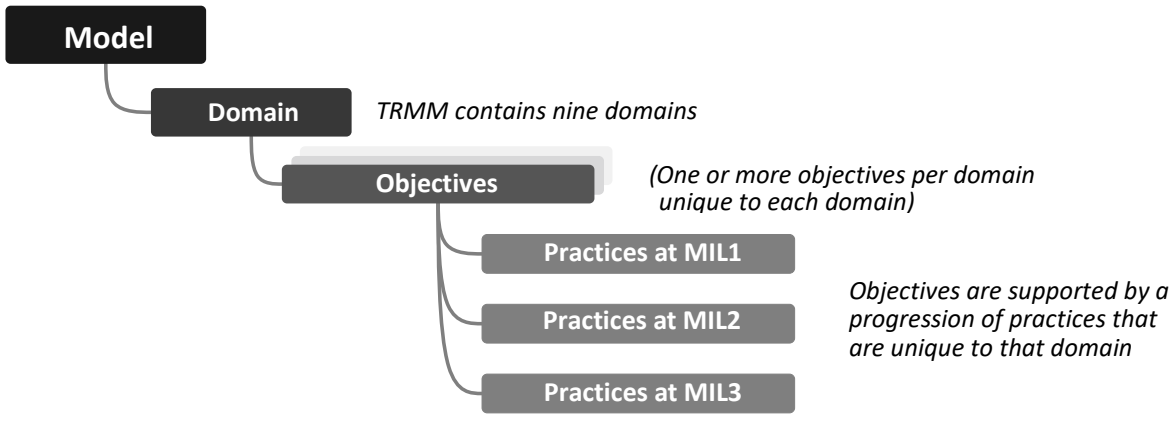

Figure 5.1: The Relationship Between Model Elements

Section 7. MODEL DOMAINS contains specific information about all nine of the TRMM domains, with descriptions, examples, and complete verbiage of all objectives and practices.

5.2 TRMM Domains

The TRMM is organized into nine domains. They are logically ordered to indicate the hierarchy shown in Figure 5.2 below.

The top tier is an overall program dedicated to resilience. This would be analogous to Compliance Program Management where there is an individual/group that has overall responsibility for and visibility to all things related to compliance. There may be dispersed individuals/groups that also have transmission resilience responsibilities (as is often the case in the compliance program), but their work is aligned with the overall program.

The following two tiers are planning and preparation for responding to and recovering from events. As introduced in Figure 1.2, longer-term preparation includes identifying and mitigation of risks. In this timeframe, there is time for investments in hardening and redesign. Shorter-term preparations involve using readily available resources . In this timeframe, there is limited time to position the grid for the impact. Therefore, the effective implementation of shorter-term planning relies heavily on the effectiveness of longer-term planning.

Finally, the base of the triangle in Figure 5.2 represents the supporting areas important to resilience. The topics covered by these domains cut across multiple areas and timeframes but are integral to an organization's resilience posture.

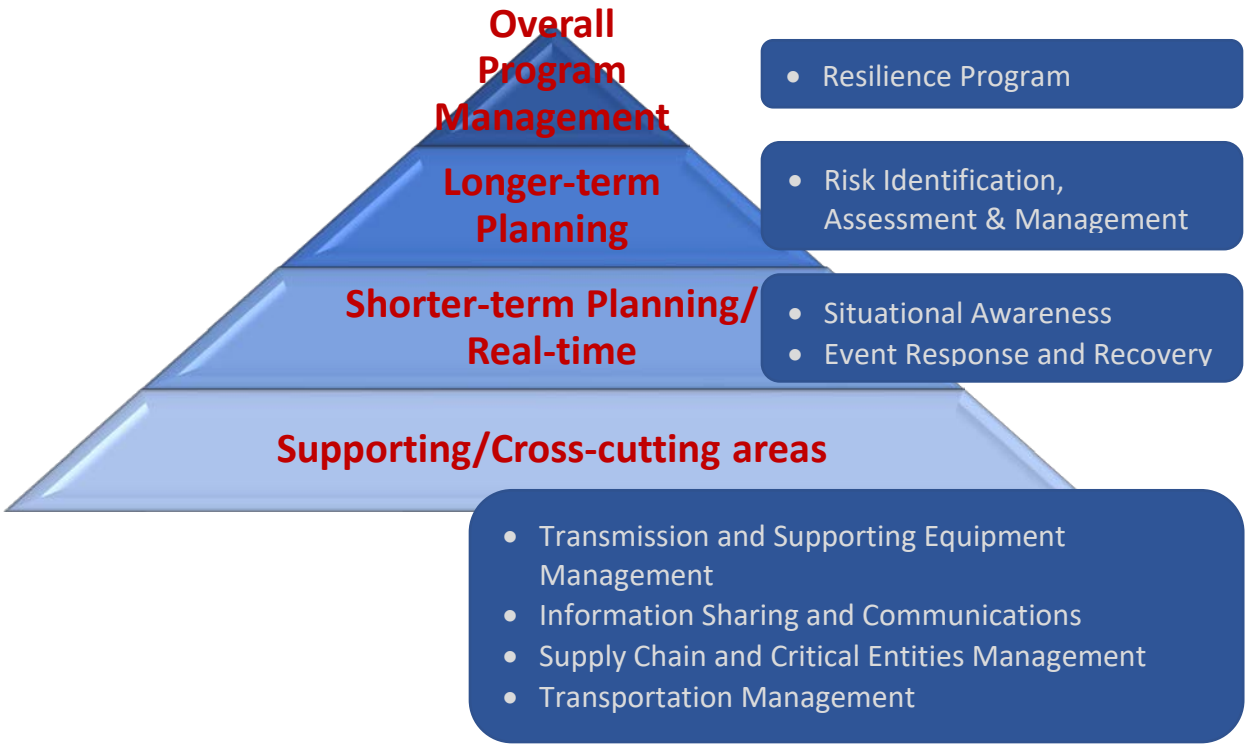

Figure 5.2: TRMM Hierarchy of Domains

5.3 Maturity Indicator Levels

The model defines four MILs, MIL0 through MIL3, which apply independently to each domain in the model. The MILs evaluate serve two purposes related to maturity: 1) the completeness, thoroughness, or level of development of resilience activities and 2) organization performance.

The more deeply ingrained an activity, the more likely it is that the organization will continue to perform it over time, that it will be retained under times of stress, and that outcomes will be consistent, repeatable, and of high quality. As an organization progresses from one maturity level to the next higher level, it will have more complete or more advanced implementations of the core activities in the model.

TRMM practices are designed to represent implementation at a specific MIL that capture the progression of transmission resilience maturity. The same activity may be covered by multiple practices, but at the various MILs, to indicate the level of rigor at which the activity is performed. For example, the Event Response and Recovery domain has a set of practices related to response capabilities. There are related practices at MIL1, MIL2, and MIL3:

- MIL1: Response capabilities are available to reduce the consequences of resilience events, even if only organized in an ad hoc manner
- MIl2: The TBU has documented plans to respond and recover from resilience events that are reviewed and updated on an organization-defined frequency
- MIL3: The TBU's documented response and recovery plans are coordinated across the enterprise

The implementation of each practice in the TRMM is evaluated with a four-point scale, as shown in Table 6.1.

Table 6.1. The Implementation Scale for Evaluating TRMM Practices

4-point answer scale	The organization's performance of the practice described in the model is…
Fully implemented (FI)	Complete – the practice is performed as described in the model
Largely implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially implemented (PI)	Incomplete – there are multiple opportunities for improvement
Not implemented (NI)	Absent – the practice is not performed in the organization

This four-point scoring system is referred to using the acronym "FILIPINI." This is shorthand for "fully implemented, largely implemented, partially implemented, and not implemented."[9]

[9] The authors and developers of other C2M2-based maturity models pronounce this acronym as "fill-uh-PEE-nee."

For an objective to achieve a given maturity level, all the practices in that objective defined for that given maturity level, and all the practices in that objective at lower maturity levels, must be "largely" or "fully" implemented. To achieve a given maturity level for a domain, all the practices in a domain must also meet or exceed that given maturity level.

The general performance characteristics for each MIL are provided below.

Maturity Indicator Level 0 (MIL0)

Performance at MIL0 simply means that the practice has not achieved MIL1.

Maturity Indicator Level 1 (MIL1)

To achieve MIL1 performance, MIL1 activities are performed in at least in an informal or ad hoc manner. "Ad hoc" refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. Documentation is not required. A more formalized implementation that covers the scope of the practice immediately qualifies as largely or fully implemented at MIL1 and may jump to MIL2 or MIL3 depending on the performance for practices that evaluate those higher levels of maturity.

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

If an organization were just starting work in a particular area, it should focus initially on implementing the MIL1 practices.

Maturity Indicator Level 2 (MIL2)

MIL2 performance is the result of formal processes and procedures that are kept current. A MIL2 organization is no longer performing activities irregularly or in an ad hoc manner. As a result, the organization's performance of the practices is more stable. At MIL2, the organization can be more confident that the performance of the domain practices will be sustained over time.

Maturity Indicator Level 3 (MIL3)

MIL3 is the highest achievable MIL in the TRMM. Organizations performing at MIL3 are actively managing resilience activities. MIL3 performance is further stabilized and guided by high-level organizational directives, such as policy. Where applicable, performance at MIL3 includes coordination across the enterprise and not just within the TBU. Overall, a MIL3 organization

should have additional confidence in its ability to sustain the performance of the TRMM practices over time and across the organization.

Understanding MIL Results in the Model

The TRMM highlights which domains and their objectives are operating at a high maturity level and which are at lower maturity levels. Items 1-3 are important in understanding the TRMM scoring:

1. The MIL score is independent for each objective and domain. That is, an organization using the model is likely to score at different MILs in different objectives and different domains. For example, an organization could be operating at MIL1 in one objective, MIL2 in another objective, and MIL3 in a third objective. Similarly, the organizations may operate at different MILs across the nine domains. Some domains may be at MIL1, MIL2, or MIL3 levels. Note, there are no practices assigned for MIL0; therefore, if an organization is not operating at least at MIL1 for all practices at the objective or domain level, they would score at a MIL0 for that respective objective or domain.
2. The MIL scores are cumulative within each objective and domain. To earn a specified MIL for a given objective, an organization must largely or fully implement all the objective's practices at that MIL and any lower MIL. For example, an organization must perform all the objective's MIL1 and MIL2 practices to achieve MIL2 in the objective. The organization would have to largely or fully implement all the practices in MIL1, MIL2, and MIL3 to achieve MIL3 for an objective. Just a single practice performed at partially or not implemented can keep a MIL from being achieved. Similarly, to earn a specified MIL for a given domain, an organization must largely or fully implement all the domain's practices at that MIL and each lower MIL. This scoring approach aligns with the concept that the chain is only as strong as the weakest link. Even one practice that is partially or not implemented, will keep an organization from achieving a MIL level.
3. Progress toward reaching the next MIL. Given the above rules for achieving MIL, an organization can, for example, have the same MIL for:

    - an objective or domain if only one practice is partially or not implemented, and all the other practices are largely of fully implemented.
    - an objective or domain where all the practices are partially or not implemented.

    This might accurately reflect the resilience capabilities of the organization in that objective or domain, but it does not indicate how close the organization may be to achieving that MIL. To capture that information, the TRMM provides a bar chart that offers a "MIL Progression Rating." This rating indicates the MIL level achieved and progress toward the next MIL. For example, an organization with a MIL1 rating and half of the additional MIL2 practices being largely or fully implemented, would have a MIL Progression Rating of 1.5. The integer value indicates the MIL level achieved and the decimal value indicates the fraction of practices at the next level that are largely or fully implemented. The decimal value can range from 0 to a value just under 1.

Items 4 and 5 are important points of consideration for organizations using the TRMM. More information on strategies for applying the TRMM are provided in the TRMM Facilitator Guide.[10]

4. Establishing a target MIL for each domain is an effective strategy for entities using the model to guide transmission resilience program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.
5. Resilience practice performance and MIL achievement goals need to align with business objectives and the organization's transmission resilience strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the model was developed with the intent that all companies, regardless of size, should be able to achieve MIL1 across all domains.

[10] https://trmm.labworks.org/resources

6. USING THE MODEL

The TRMM is meant to be used by an organization to evaluate its transmission resilience capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its transmission resilience investments. Figure 6.1 below summarizes the recommended approach for using the model. An organization performs an assessment with the model, uses that assessment to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements the plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated. This section covers preparation activities, step-by-step instructions for using the model and interpreting its report, and various follow-up activities,

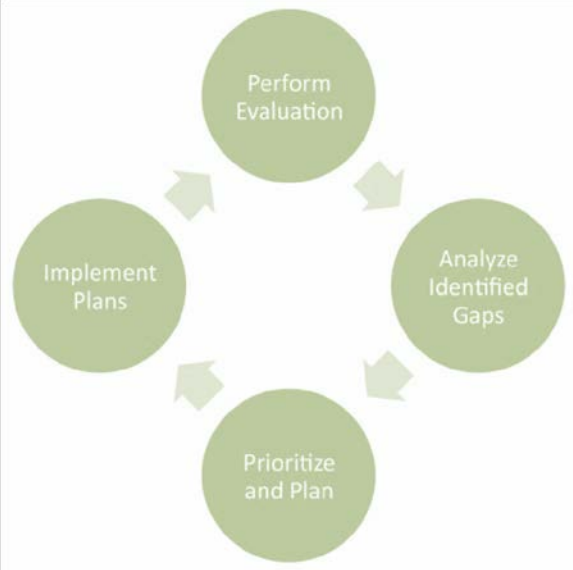

Figure 6.1: Recommended Approach for Using the Model

6.1 Prepare to Use the Model

The model is designed to enable organizations to complete a self-assessment in a short period of time without extensive study or preparation. This goal is achieved in part because the model is supported by a user-friendly assessment tool with a scoring mechanism and automated report generator. The assessment can be performed in a manner and at a pace that best suits the organization.

More thorough guidance on selecting facilitator(s), identifying the appropriate SMEs, and conducting the assessment program can be found in the supporting *TRMM Facilitator Guide*.[11]

[11] The TRMM Facilitator Guide may be downloaded from https://trmm.labworks.org/resources

6.2 Perform an Assessment

The organization should select the appropriate personnel to evaluate its performance capabilities against the model domains. Participation by a broad representation across the parts of the organization being assessed yields the best results and enables internal information sharing about the model practices. Personnel selected to contribute to the assessment should include operational personnel, management stakeholders, and any others who could provide useful information on the organization's performance of the resilience practices in the model.

Please note that not all personnel need to participate in completion of each domain. To ensure time and resources are used effectively, the organization should determine ahead of time which personnel are most relevant to each domain. Flexibility in scheduling personnel's time is encouraged in order to accomplish the best assessment in the most efficient manner. See the *TRMM Facilitator Guide* for more information.

Starting the TRMM

To begin using the model from the TRMM website, click "TRMM Tool" on the navigation menu. After logging into the tool, the starting page for the TRMM tool is displayed (Figure 6.2). The navigation menu at the top of the page provides access to TRMM webpages where the user can learn more about the tool, access TRMM resources, examine frequently asked questions, and more.

Below the navigation bar is introductory text. Below this text are two buttons. The leftmost button, "Get Started", provides the option to begin a fresh evaluation. To its right is the "Load" button which is used to load data from an existing evaluation . If the "Load" button is clicked, Figure 6.3 is displayed, prompting the user to either upload an existing TRMM data file or copy and paste the formatted data from an existing TRMM data file into the indicated window on the screen.

Once the user either starts a fresh assessment or loads the data for an existing assessment, a standard disclaimer screen is displayed. The user clicks "Okay" to acknowledge reading the disclaimer and proceed.

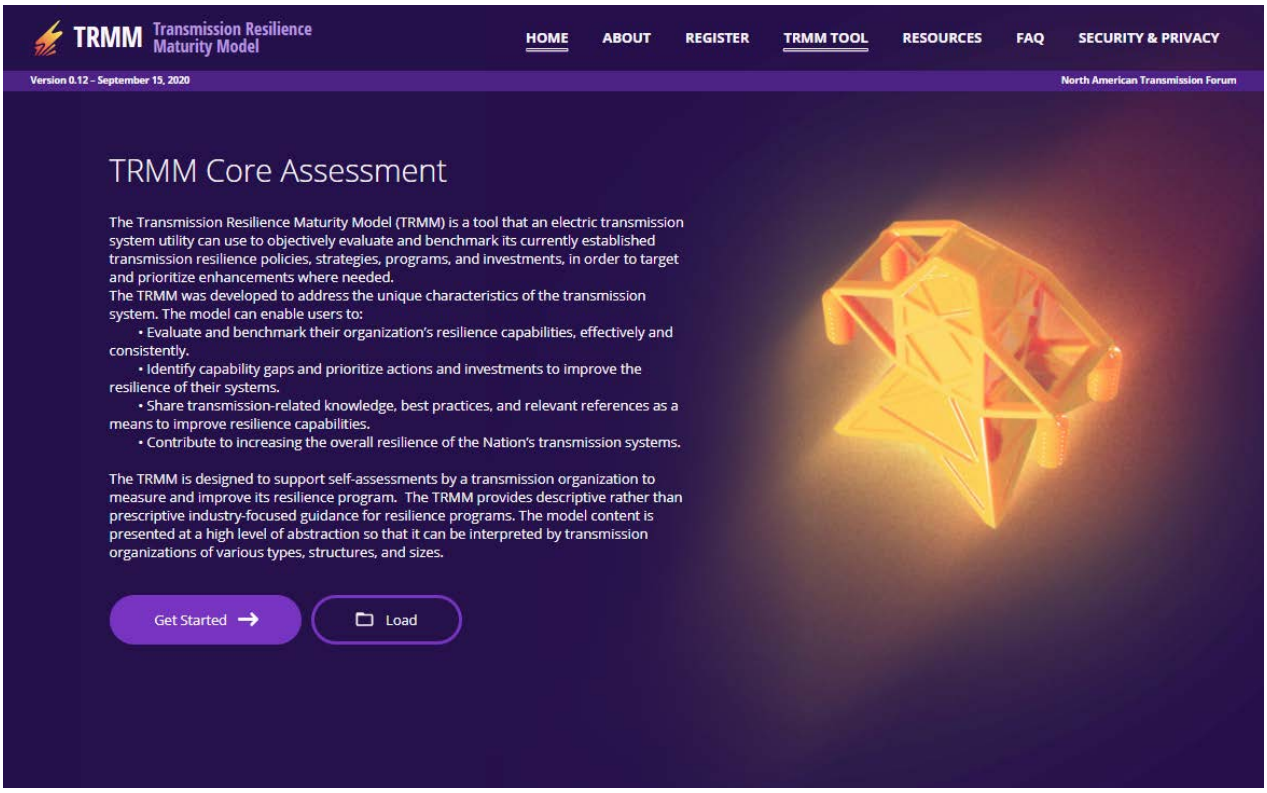

Figure 6.2: The TRMM Tool Homepage

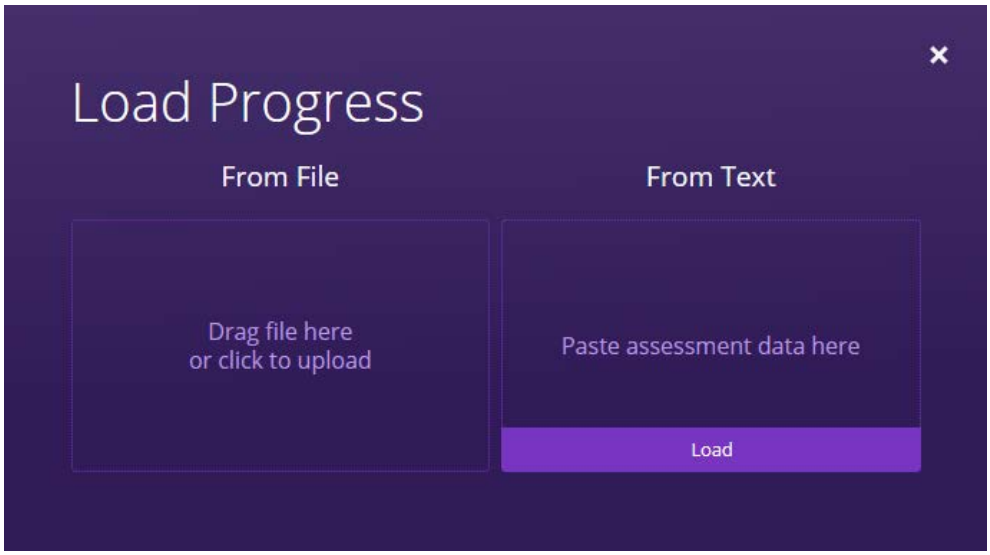

Figure 6.3: Select Whether to Start Fresh or Load an Existing Assessment.

Assessing Resilience

Figure 6.4 shows the starting screen for a new assessment. A brief introduction to the first domain is presented. Clicking "Begin" below the introductory text takes the user to the first practice in the first objective of the first domain. However, the user does not have to start there. The user can instead use the left navigation menu to navigate to whichever domain or objective the user wants to assess. (Reference a close-up of the left navigation menu in Figure 6.5 for an example, partially completed assessment.) The left navigation menu is active throughout the assessment allowing the user to set their own order for conducting the assessment.

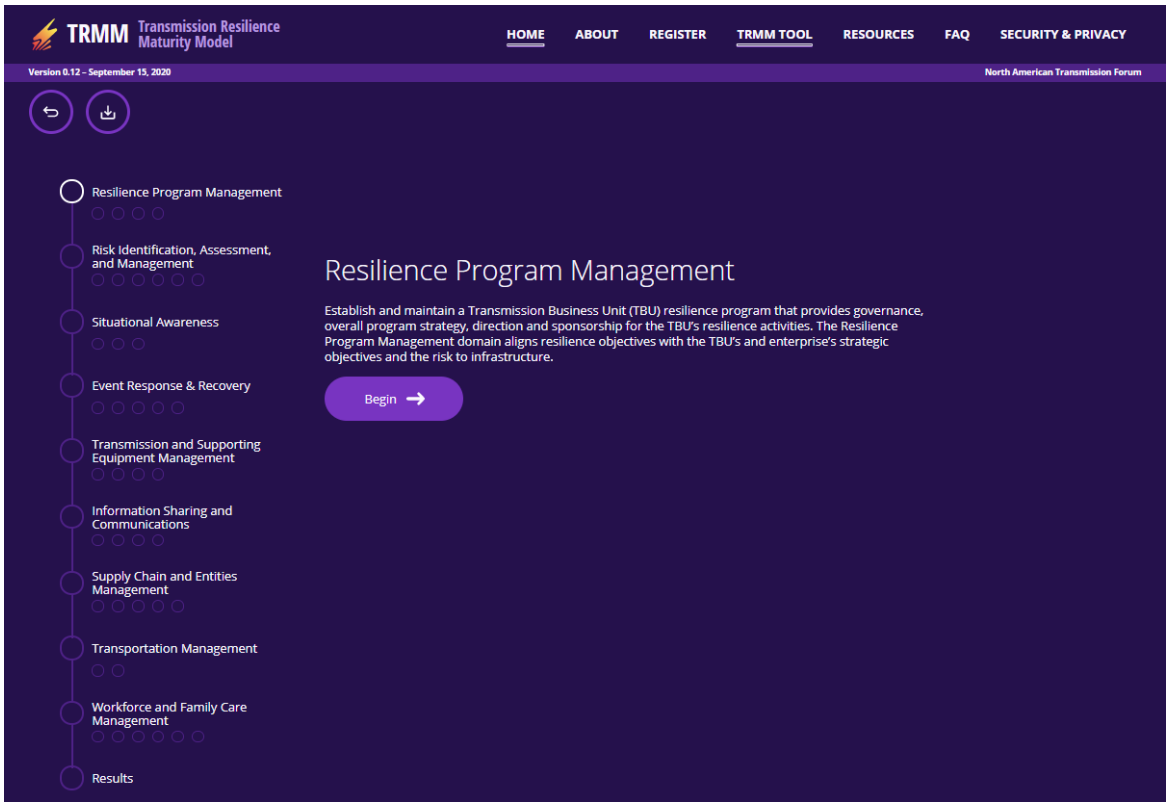

Figure 6.4: Starting Point for a New Evaluation

The icon in the top left of the left navigation pane, labeled as #1, allows the user to "Start Over." Clicking it gives the user the option to save their work and start a new assessment or start over without saving their current work.

The icon next to "Start Over" is the "Save Assessment" button, labeled as #2. It allows the user to download their current assessment data to their computer. Data are saved to a file in a JavaScript Object Notation (JSON) format (the format used to input data to the TRMM) or to text (a less commonly used option).

Below these two icons follow the nine model domains. Clicking the circle to the left of a domain name (examples marked as #3 and 4), takes the user to the corresponding domain. Domains for which all the practices are assessed are denoted with a green check mark (see example labeled as #3). A bolded circle indicates the current domain. If a circle is unchecked, all the practices in the domain are not yet assessed. The circle labeled as #4 is an example of both.

Below the domain names are smaller circles. These represent each of the objectives in the domain. Clicking an objective circle takes the user to that objective. A check mark in an objective circle indicates all the practices in the objective are scored (see example labeled as #5). A slightly bolded circle indicates the current objective being assessed (#6).

Below the last of the domains is a circle for "Results". Clicking "Results" takes the user to a screen from which they can automatically generate an assessment report.

Figure 6.5: TRMM Navigation

Figure 6.6 presents the introductory screen for the first objective of the first domain. Clicking "Begin Section" takes the user to first practice in this objective. Alternatively, the user can click any of the numbered practices in the middle of the screen to display that practice. The name of the domain and its summary description are provided. The name of the objective is provided using a yellow font.

Figure 6.7 presents an example practice that has been scored as "Partially Implemented" with comments entered in the Notes field. To change the scoring level, the user can select a different implementation value by clicking the appropriate large circle. Previously evaluated practices for the current objective are indicated by the color-coded circles on the line above the text describing the current practices.

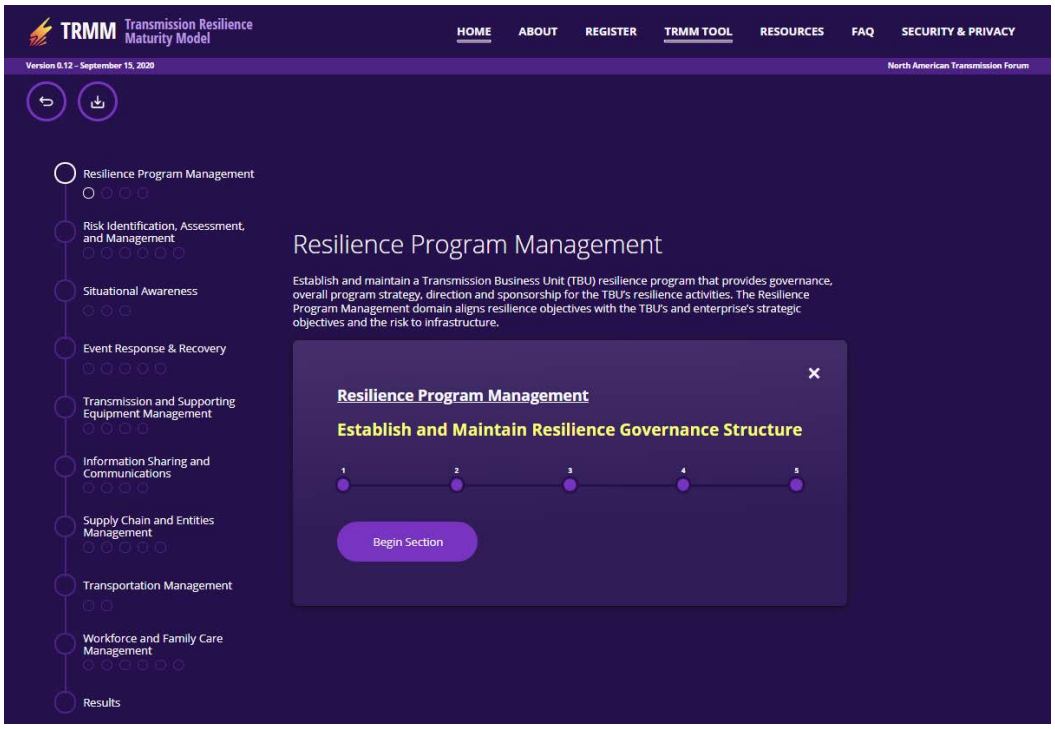

Figure 6.6: Starting Display for the First Objective in the First Domain

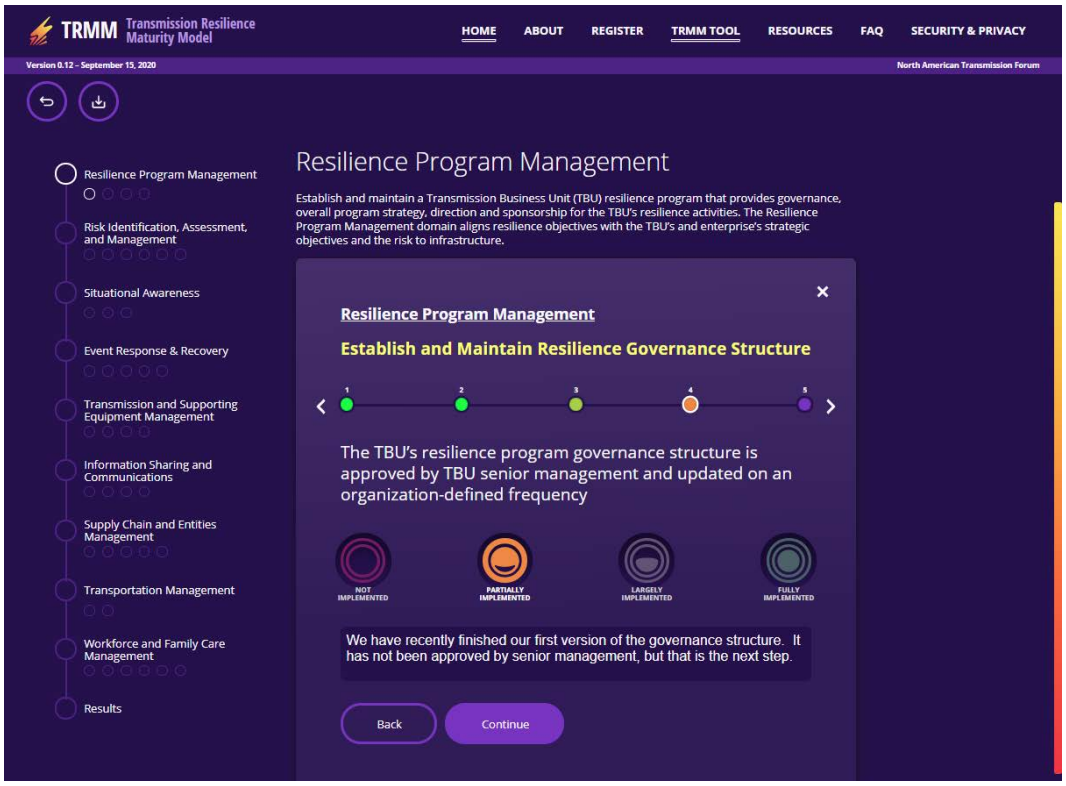

Figure 6.7: A Practice is Displayed That Has Been Scored.

After evaluating each of the practices for the current objective, a summary of the practices and their scores is displayed in Figure 6.8. To continue to the next objective, the user scrolls down and clicks “Continue to the Next Screen”. To return to the current objective (e.g., to change a score or add notes) the user clicks **inside the text box of the practice they wish to revisit.**

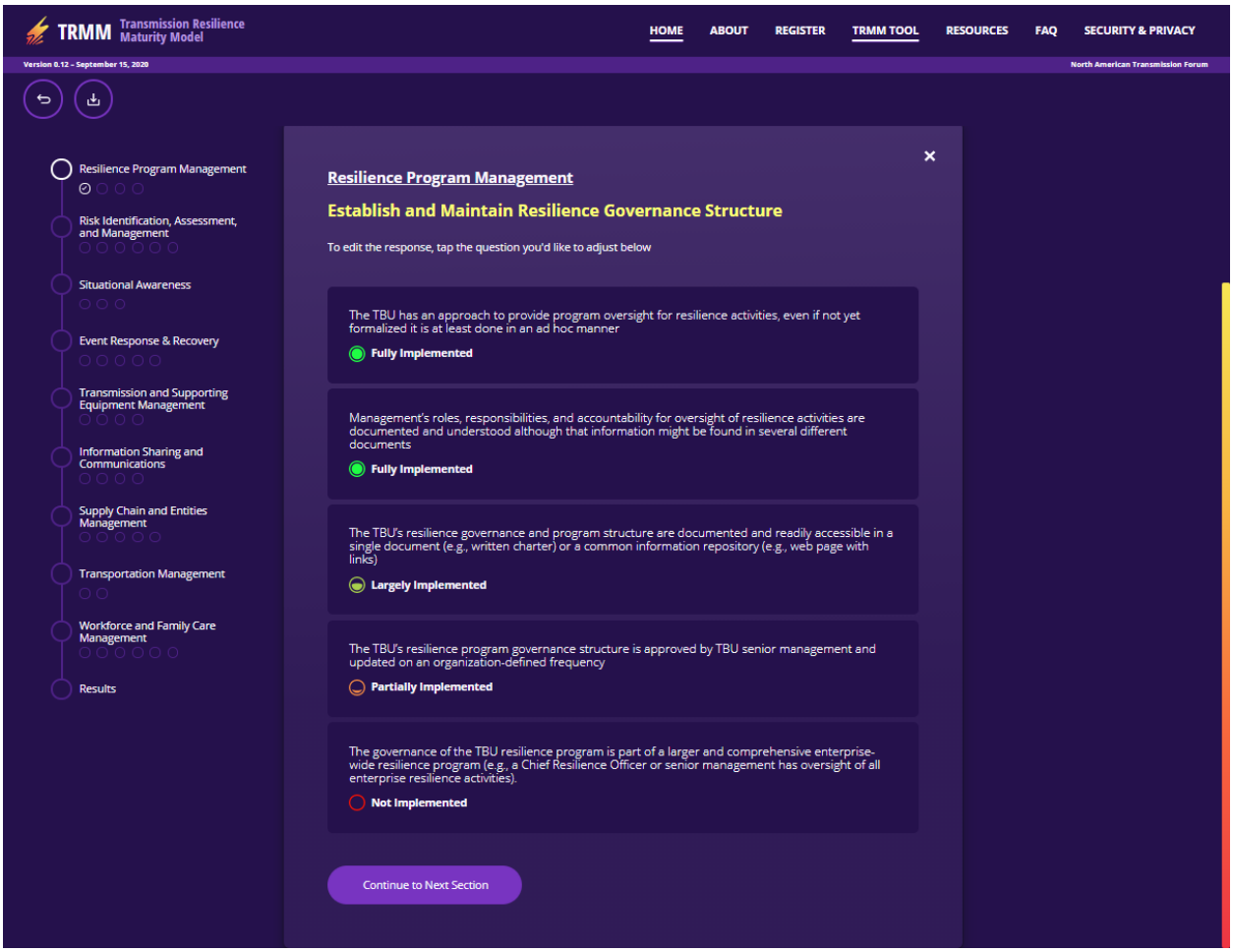

Figure 6.8: After All the Practices for a Given Objective are Entered, a Summary Screen of the Scoring for the Objective is Displayed

Skipping ahead to when data have been entered for each domain and each objective, Figure 6.9 displays the screen after the last objective in the final domain has been completed. When each objective is completed its circle in the left navigation pane is checked. In Figure 6.9, all the objectives and all the domains are checked – indicating the analysis is complete. The user would click the “Complete Assessment” button to proceed to the report creation. At any point, the User can also click “Results” in the left navigation window to proceed to create a report for an incomplete or a completed assessment.

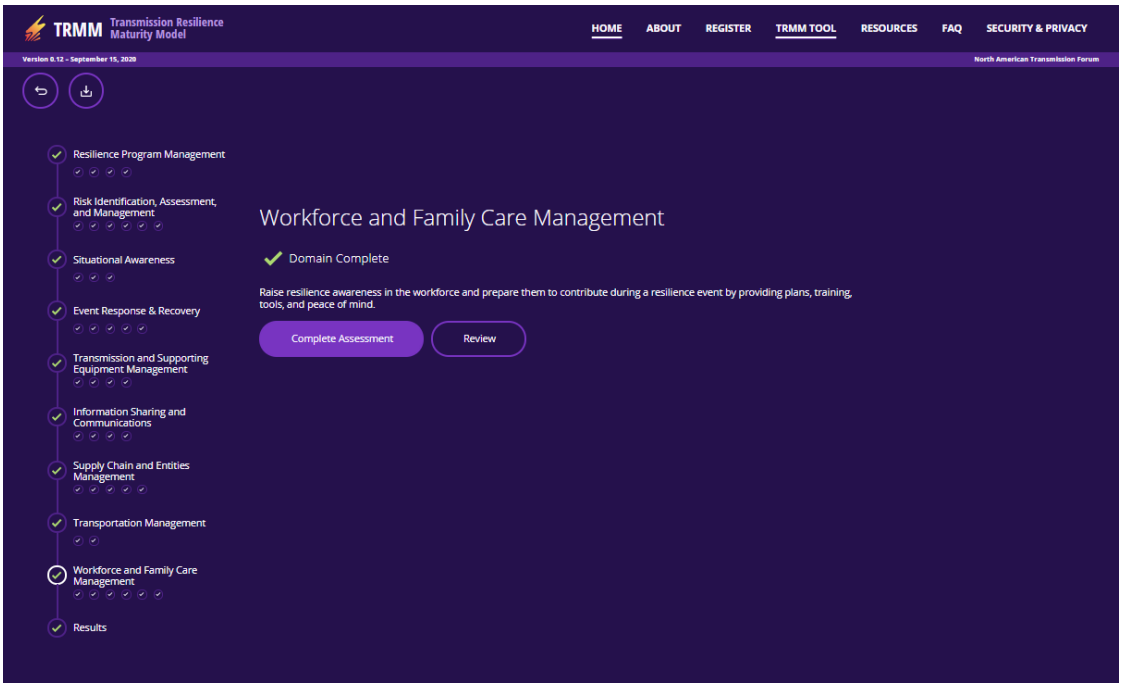

Figure 6.9: The Last Objective Has Been Completed

When the assessment is complete, Figure 6.10 will be displayed with its "Assessment Complete" message. If the assessment is not yet complete, a similar screen will be displayed with the message "Assessment Incomplete."

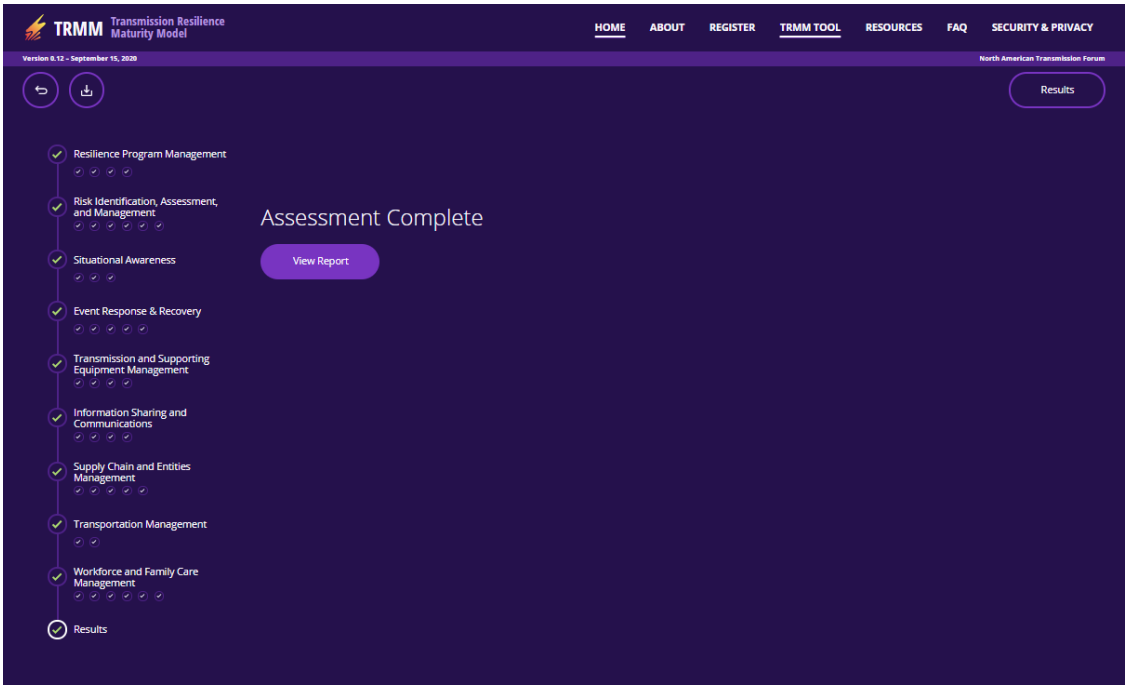

Figure 6.10: The "Assessment Complete" Screen

Clicking “View Report” on the “Assessment Complete” screen (or “View Partial Report” on the “Assessment Incomplete” screen) will trigger the automatic production and display of the TRMM Core Assessment Report. There may be short delay (e.g., 30 seconds or less) for the report to be generated and displayed on the computer screen.

The Core Assessment Report – Introduction and Summary

After the Core Assessment Report is generated, a display similar to what is shown in Figure 6.11 will appear on the user’s screen.

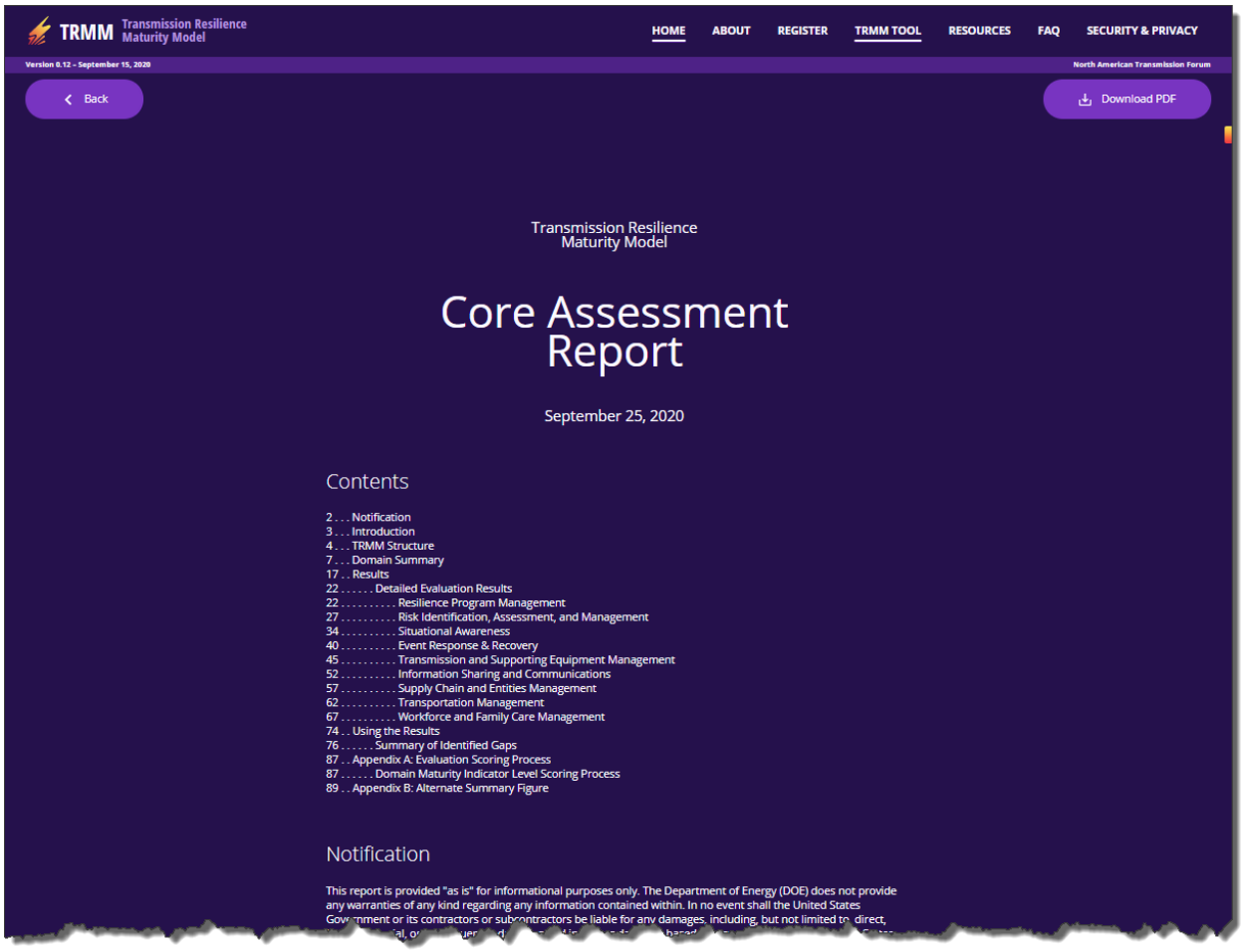

Figure 6.11: Top of “Core Assessment Report” Presents TRMM Assessment Results

The report begins with its title and the date and is followed by a Table of contents. The complete report will typically be about 100 pages in length – perhaps longer for organizations with a relatively low maturity level. The report can be viewed interactively within the tool, or it can be downloaded and stored as a PDF file. To download the PDF file, click “Download PDF” in

the upper right-hand corner of the screen. This option is displayed when the Core Assessment Report is on the screen.

The key sections of the Core Assessment Report are:

- The Table of Contents
- Notification about the limitations of the assessments
- Introduction to the TRMM
- Description of the TRMM Structure
- Summary results of the TRMM that focused on cumulative results from the nine TRMM domains
- Detailed Evaluation Results for each domain
  - Resiliency Program Management
  - Risk Identification, Assessment, and Management
  - Situational Awareness
  - Event Response & Recovery
  - Resiliency Asset Management
  - Information Sharing and Communications
  - Supply Chain and Critical Entities Management
  - Transportation Management
  - Workforce Management
- Guidance on Using the Results
- Summary of Identified Gaps in programmatic maturity for transmission resilience
- Appendix A: A Description of the Evaluation Scoring Process
- Appendix B: An Alternate Summary Figure

Figure 6.12 displays the beginning of the summary TRMM results. It displays the current MIL level with the addition of the progression toward the next MIL. Figure 6.13 displays a close-up of Figure 6.12. The solid blue bar, brightening in color as it increases in height, presents the achieved MIL. The shaded or darkened portion of the bar above the top of the achieved MIL indicates the status of the progression toward the next MIL (i.e., the percentage of the practices that evaluate the next MIL level that are fully or largely implemented). If for a given domain, none of the practices at the maturity level beyond what has been achieved are largely or fully implemented, the progression MIL level will be the same as the actual MIL level. If 60% of the practices for the next MIL level are largely or fully implemented (as indicated in Figure

6.13 for the *Resilience Program Management* domain), it will show 60% progress toward the next MIL level. If MIL1 is not achieved, only the progression bar toward MIL1 is displayed (as indicated in Figure 6.13 for the *Risk Identification, Assessment, and Management* domain where only one of the 13 MIL1 practices is not achieved). For the *Event Response and Recovery* domain, Figure 6.13 indicates 80% progress from the achieved MIL2 to MIL3.

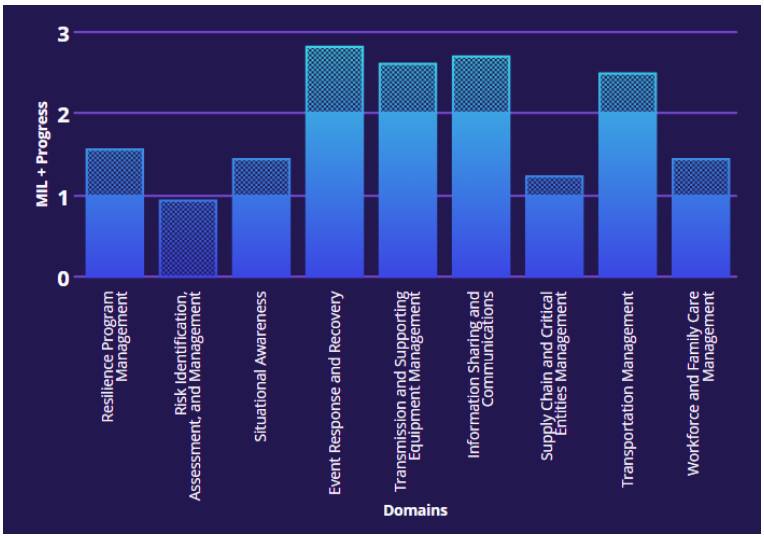

Figure 6.12: Bar Chart Presenting MIL + progression toward the next MIL.

MIL 1 is achieved for the Resilience Program Management domain, and there is 60% progress toward MIL2.

MIL 1 is not achieved for the Risk Identification, Assessment, and Management; only the over 90% progress toward MIL2 is shown.

MIL2 is achieved for the Event Response and Recovery domain, and there is over 80% progress toward MIL3.

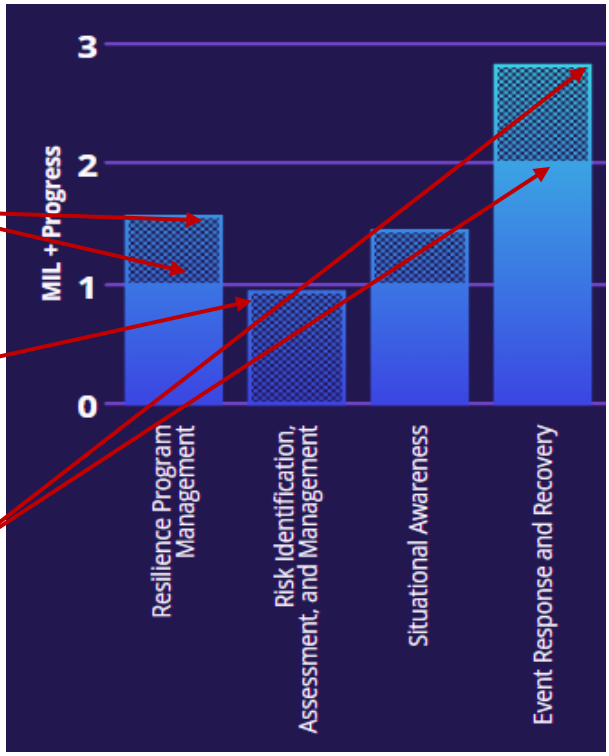

Figure 6.13: Closeup of the MIL + Progression Bar Chart.

Figure 6.14 displays a pie chart that presents more detailed results for each domain. It shows the breakdown of the implementation scores for the all the practices for MIL1-3 for each domain. Looking at the Resilience Program Management (PM) domain (found in the midnight to 1 AM slot on the circular chart), we see six practices in the first slice for MIL1. Three of these are fully implemented and other three are largely implemented. In the second slice of the PM domain, we see results presented for 20 practices (these are the MIL1 plus MIL2 practices). Six are fully implemented, eight are largely implemented, four are partially implemented, and two are not implemented. In the third slice of the PM domain, we see results presented for 28 practices (these are the MIL1, MIL2, and MIL3 practices). Six are fully implemented, nine are largely implemented, six are partially implemented, and seven are not implemented.

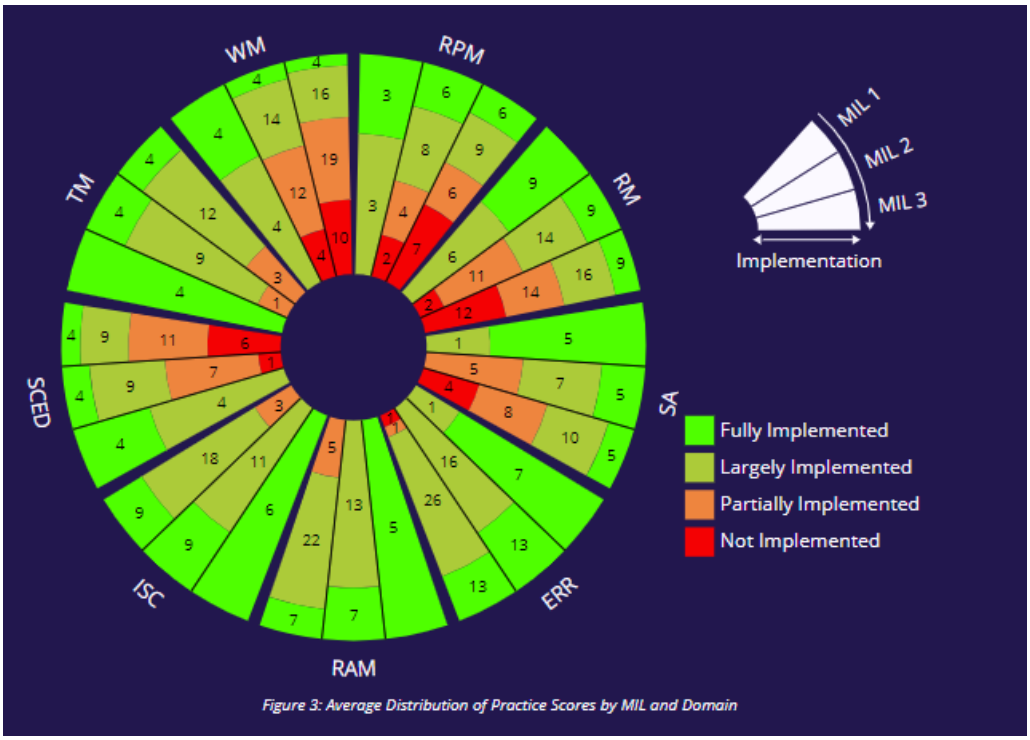

Figure 6.14: The Third Display in the Summary. This is a pie chart that summarizes the results by domain and MIL, over all practices.

The pie chart can be interrogated to provide more detailed information by clicking a segment in any slice. In Figure 6.15, the visualization details are presented for the MIL3 data for the Resilience Program Management domain. The image that is displayed shows the results for all the MIL1-3 practices that need to be fully or largely implemented to achieve MIL3. This displays the same results as presented in the last paragraph. To the right of the pie chart, the text of the practices that are fully implemented are displayed. The user can choose additional displays by

selecting the domain to assess, the objectives to assess, and the MIL(s) of interest. Clicking on the pie chart or using a drop-down menu can determine which practices are displayed in the text window – for all results or for only a specific implementation score.

Figure 6.15: The Visualization Data Display

Figure 6.16 shows the traditional C2M2 donut chart that displays the pie chart results in a more traditional and less dense format as compared to figure 6.14.

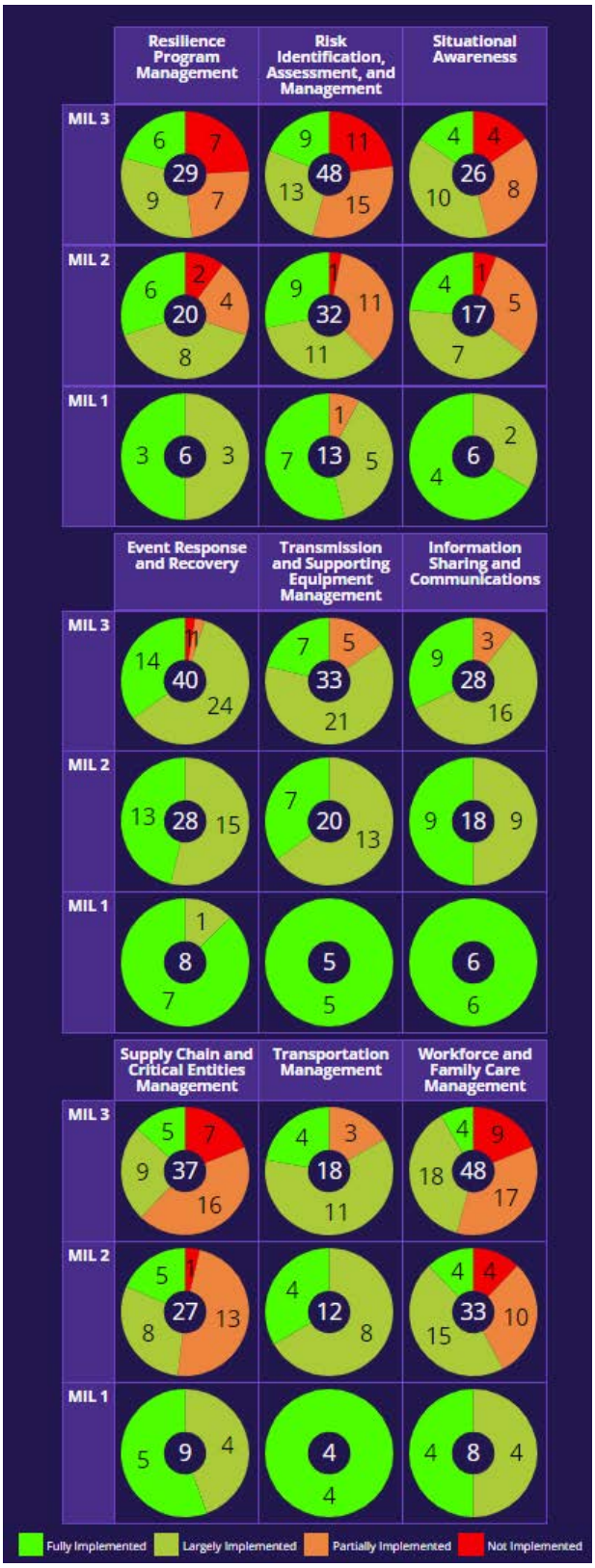

Figure 6.16: Traditional TRMM Donut Diagram Displaying Results by Domain and MIL

To understand how to interpret the chart, lets focus on the left most column in Figure 6.17 that displays the results at each MIL for the Resiliency Program Management domain:

- Starting with the bottom, "MIL1" donut for this domain, there are six practices that evaluate MIL 1 performance, as indicated by the number "6" in the middle of the donut (i.e., within the donut hole). Three of these practices scored at the fully implement level (the bright green segment of the donut) and three practices as largely implemented (the olive-green segment of the donut).

- At the next level up, MIL 2, there are 20 practices at MIL1 and MIL2 that have to be scored as fully or largely implemented for MIL 2 to be achieved, as indicated by the number "20" in the middle of the donut. This consists of the six practices from MIL1 and 14 additional practices at the MIL2 level. Considered together, there are six practices that are fully implemented, eight that are largely implemented, four that are partially implemented and two that are not implemented. Achieving MIL2 is prevented by the presence of partially and not implemented practices. By subtracting the MIL1 donut results from the MIL2 donut results, the performance of the MIL2 practices can be determined.

Figure 6.17: Donut Diagram

- For MIL 3, there are 28 total practices at MIL1–3 that have to be scored as fully or largely implemented for MIL 3 to be achieved, as indicated by the number in the middle of the donut. In total, there are six practices that are fully implemented (though those are all "inherited" from MIL 1 and MIL2), nine practices are largely implemented (eight of which are inherited from MIL1 and MIL2), six practices that are partially implemented, and seven practices that are not implemented.

As with Figure 6.14, the individual pie charts in Figure 6.16 can be clicked to display detailed visualization data like that shown in Figure 6.15.

The Core Assessment Report – Detailed Evaluation Results

The Core Assessment Report continues by presenting "detailed evaluation results" for each domain. The bar charts and donut diagrams described above are presented again, focusing on the individual domains in the TRMM, with results presented for each objective within the

domain. After presenting its bar charts and donut diagrams, each domain section includes additional products, as described below.

For each objective in the given domain, the top two thirds of Figure 6.18 present the count of practice scores for each implementation score category. This approach allows the insertion of a blue symbol to indicate the effective MIL for the objective. The bottom portion of this figure indicates the scores for each MIL1, MIL2, and MIL3 practice in the domain using a concise display.

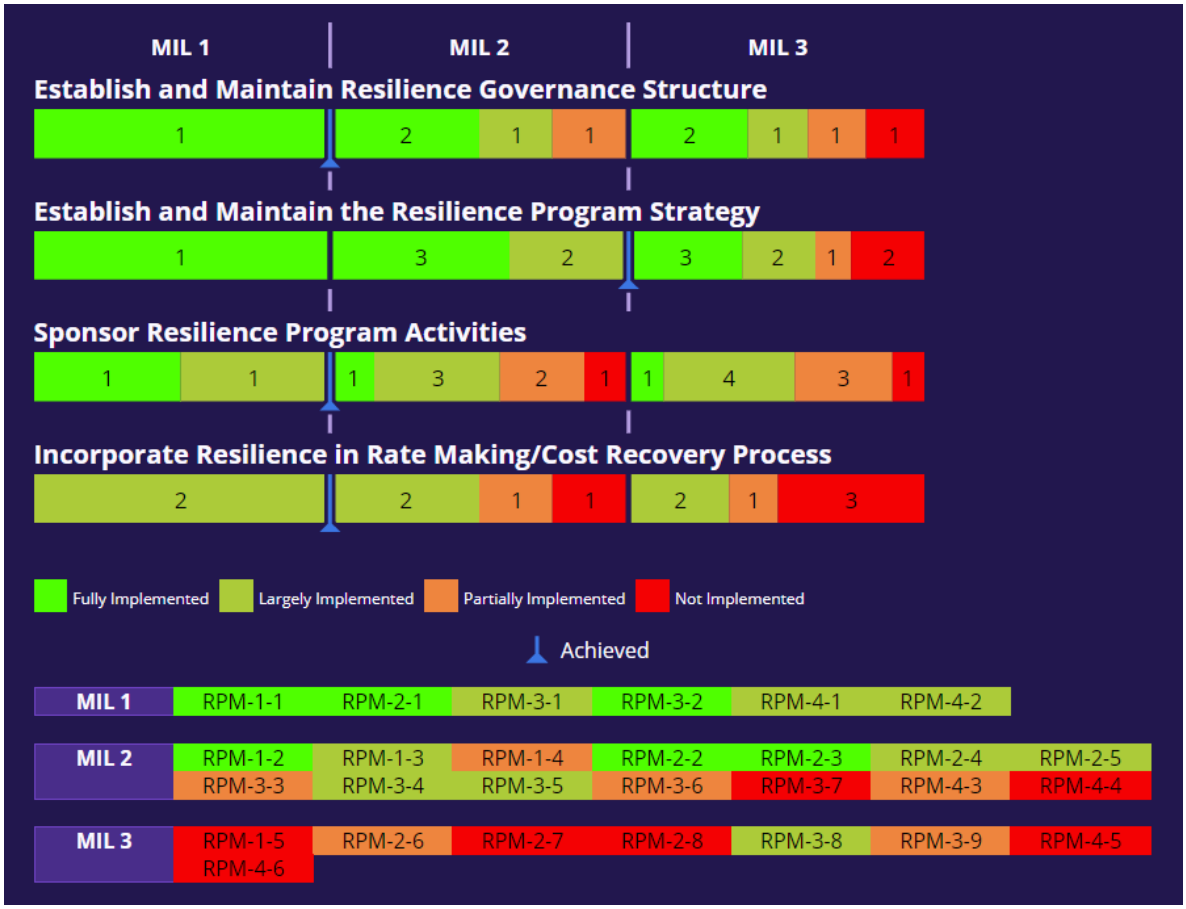

Figure 6.18: Alternate Domain Summary Graphics

Figure 6.19 presents more detailed information about the practices. It presents each practice in the domain, listed in order within their objectives, provides the practice's MIL level, and implementation score. This is a concise presentation of the data entered into the TRMM tool.

(1) Establish and Maintain Resilience Governance Structure

Control	Question	MIL	Status
RPM-1-1	The TBU has an approach to provide program oversight for resilience activities, even if not yet formalized it is at least done in an ad hoc manner	1	FI
RPM-1-2	Management's roles, responsibilities, and accountability for oversight of resilience activities are documented and understood although that information might be found in several different documents	2	FI
RPM-1-3	The TBU's resilience governance and program structure are documented and readily accessible in a single document (e.g., written charter) or a common information repository (e.g., web page with links)	2	LI
RPM-1-4	The TBU's resilience program governance structure is approved by TBU senior management and updated on an organization-defined frequency	2	PI
RPM-1-5	The governance of the TBU resilience program is part of a larger and comprehensive enterprise-wide resilience program (e.g., a Chief Resilience Officer or senior management has oversight of all enterprise resilience activities)	3	NI

(2) Establish and Maintain the Resilience Program Strategy

Control	Question	MIL	Status
RPM-2-1	The TBU has a resilience program strategy (i.e., resilience objectives and an approach to achieve them), even if only in an ad hoc manner	1	FI
RPM-2-2	There is a documented TBU resilience program strategy that defines objectives for the TBU's resilience activities	2	FI
RPM-2-3	The documented TBU resilience program strategy includes preparation (longer-term and shorter-term), operating, and recovery components as well as mechanisms for incorporating lessons learned	2	FI
RPM-2-4	Engagement with external entities and resilience-related activities (e.g., regulators, scientists, electric and other industry groups, and community groups and leaders) is leveraged to define objectives, goals, and areas for collaboration in the documented TBU resilience strategy	2	LI
RPM-2-5	The documented TBU resilience program strategy is regularly reviewed and updated on an organization-defined frequency to account for changes (e.g., changes in industry standards or best practices, the threat environment, operations, technological innovations, stakeholder concerns.)	2	LI
RPM-2-6	The documented TBU resilience strategy includes provisions for tracking the performance of the resilience program and adjusting the resilience strategy as needed	3	PI
RPM-2-7	The TBU resilience strategy is independently reviewed and evaluated for its adequacy (i.e., by reviewers who are not involved in the strategy such as an internal audit group, technical peer review group, or third-party consultant; this is not intended to be the regulators)	3	NI
RPM-2-8	The documented TBU resilience program strategy is aligned with the TBU's and enterprise's strategic objectives and is approved by TBU's senior management.	3	NI

Figure 6.19: Restatement of TRMM Input Data in the Core Assessment Report

Figure 6.20 provides a focused summary of partially and not implemented practices. This portion of the Core Assessment Report provides a quick overview of the practices that need improvement to reach the next maturity level.

Summary of Identified Gaps

This section provides a summary of what gaps were found as a result of the survey. Gaps are defined as answers marked as either "Not Implemented" or "Partially Implemented". This section is meant to provide with a quick overview of what needs to be improved and to assess the threat level.

(RPM) Resilience Program Management

Status	MIL	Control	Question
Partially Implemented	2	RPM-1-4	The TBU's resilience program governance structure is approved by TBU senior management and updated on an organization-defined frequency
		RPM-3-3	Adequate resources (people, tools, training, and funding) are provided to support resilience activities
		RPM-3-6	Resilience stakeholders (TBU, enterprise, and external) are identified, documented, and engaged
		RPM-4-3	Specific responsibility is assigned within the enterprise or TBU to support the TBU in monitoring rate making and cost recovery issues (including industry trends) that may affect resilience objectives
	3	RPM-2-6	The documented TBU resilience strategy includes provisions for tracking the performance of the resilience program and adjusting the resilience strategy as needed
		RPM-3-9	The application of new resilience program processes, tools, and technologies (from internal or external research and development activities) is supported by senior management
Not Implemented	2	RPM-3-7	TBU senior management support for resilience activities is evident via clear messaging of its benefits, external sharing and collaboration, and the TBU's related goals
		RPM-4-4	The formal enterprise rate making and cost recovery process specifically addresses the need for funding resilience program activities
	3	RPM-1-5	The governance of the TBU resilience program is part of a larger and comprehensive enterprise-wide resilience program (e.g., a Chief Resilience Officer or senior management has oversight of all enterprise resilience activities)
		RPM-2-7	The TBU resilience strategy is independently reviewed and evaluated for its adequacy (i.e., by reviewers who are not involved in the strategy such as an internal audit group, technical peer review group, or third-party consultant; this is not intended to be the regulators)
		RPM-2-8	The documented TBU resilience program strategy is aligned with the TBU's and enterprise's strategic objectives and is approved by TBU's senior management.
		RPM-4-5	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
		RPM-4-6	Approved rates support adequate funding for key resilience program activities and objectives

(RM) Risk Identification, Assessment, and Management

Status	MIL	Control	Question
Partially Implemented	2	RM-1-4	The identification, prioritization, and assessment of threats is guided by documented procedures which are updated on an organization-defined frequency
		RM-1-5	Threat information is obtained from a documented set of sources to support threat management activities (e.g., key internal sources, various critical infrastructure sector ISACs, industry associations, vendors, federal briefings)
		RM-1-6	Identified threats are prioritized and documented for more detailed assessment as input to the risk assessment process
		RM-2-7	Vulnerability assessments are reviewed and updated at an organization-defined frequency

Figure 6.20: Summary of Identified Gaps

Saving and Loading Assessment Files

Figure 6.21 illustrates the TRMM "save" function. When a user clicks the "Save" icon displayed in the upper left-hand corner of a TRMM screen when entering assessment information, the user will be guided in storing their TRMM input file to their computer. Options are provided to save the file by downloading it in JSON format or copying the data to a text file. JSON is a standard data interchange format that is used to transmit data between a web application and a server.[12] It is the format used by the TRMM to save and load assessment data.

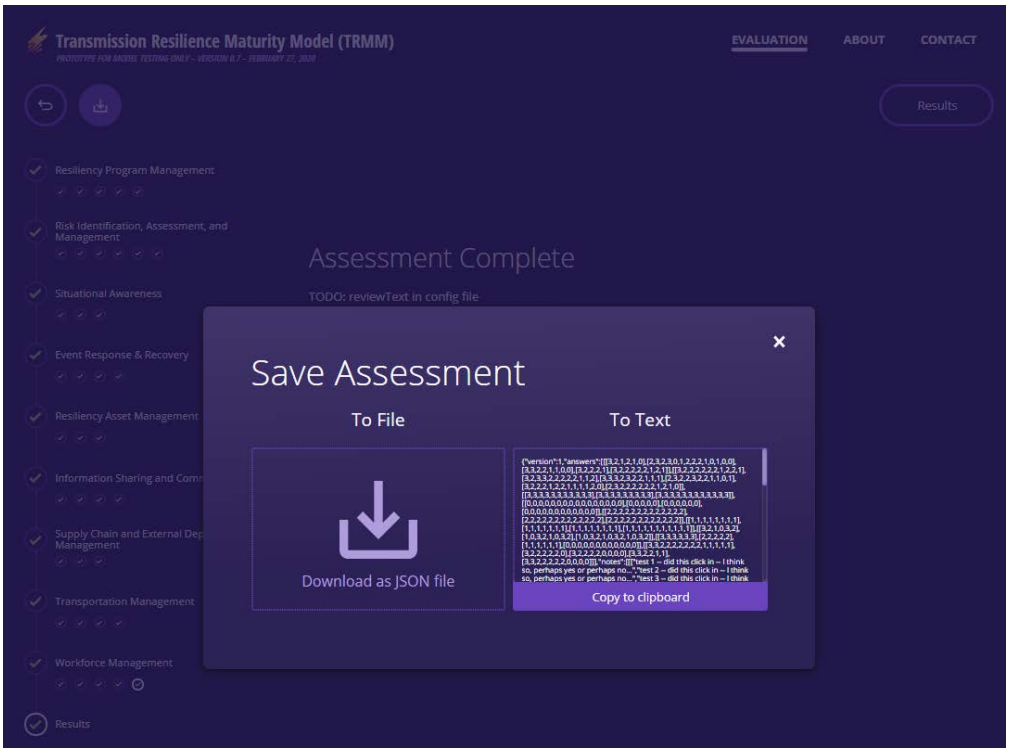

Figure 6.21: The Screen for Saving Assessment Data Files

Figure 6.22 illustrates the TRMM "load" function. When a user clicks the "Load" icon displayed in the upper left-hand corner of a TRMM screen, or the Load option when displayed when beginning to use the tool, the user will be guided in accessing an existing TRMM input file and uploading it into the tool. The TRMM input file directly loaded into the tool must be a JSON file previously saved by the tool. Alternatively, data saved to text using the Save feature can be pasted into the From Text field. This loading of data allows the user to access and work with existing data files, including modifying and adding information to the files.

[12] https://fileinfo.com/extension/json

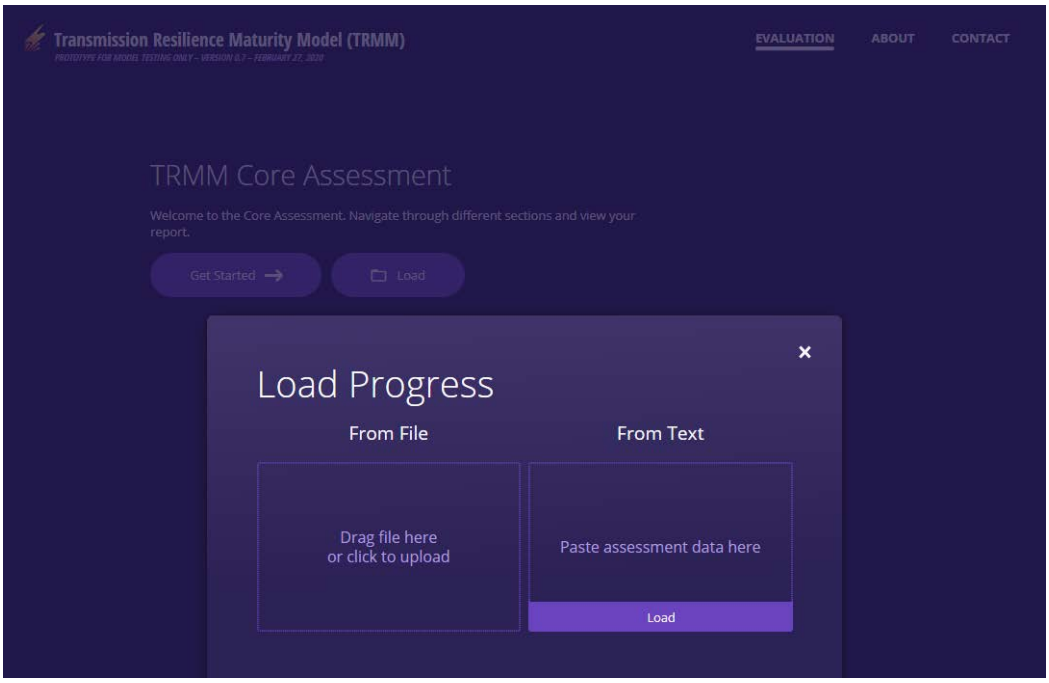

Figure 6.22: The "Load Progress" Window.

6.3 Analyze Identified Gaps

The scoring report from the assessment 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 objectives and resilience strategy. 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 capability profile is best identified after an initial baseline assessment. This gives the organization an opportunity to develop more familiarity with the model. The appropriate organizational stakeholders should select the desired target profile. This could be a single individual with expertise in the organization's operations and management, but it is more likely to be a collection of individuals.

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

6.4 Prioritize and Plan

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

Next, a plan should be developed to address the selected gaps. 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.

6.5 Implement Plans and Periodically Reevaluate

Plans developed in the previous step should be implemented to address the identified gaps. Model assessments are particularly useful in tracking implementations and should be conducted periodically to ensure that desired progress is achieved. Reassessments should also be considered in response to major changes in the business, technology, market, or threat environments to ensure that the current profile matches the organization's desired state.

7. MODEL DOMAINS

7.1 Resilience Program Management (PM)

Purpose: Establish and maintain a transmission business unit (TBU) resilience program that provides governance, overall program strategy, direction and sponsorship for the TBU's resilience activities. The PM aligns resilience objectives with the TBU's and enterprise's strategic objectives and the risk to infrastructure.

A transmission resilience program is an integrated group of activities designed and managed to meet resilience objectives for the TBU.

The Transmission Resilience Program Management (PM) domain has four objectives:

1. Establish and maintain resilience governance structure
2. Establish and maintain the resilience program strategy
3. Sponsor resilience program activities
4. Incorporate resilience in rate making/cost recovery process

For resilience program success, a plan for oversight and governance of resilience-related activities is established, with clear responsibilities outlined. As the foundation for the program, a transmission resilience program strategy is established. In its simplest form, the program strategy should include a list of transmission resilience objectives and a plan to meet them. A more comprehensive program strategy will include priorities, a governance approach, and structure and organization for the program. Senior management should be involved in the development and approval of the resilience program, possibly including support for a dedicate resilience group. Implementation of a resilience group is most effective at the enterprise level so resilience goals and objectives across the enterprise are aligned. This approach provides visibility and oversight for all resilience activities, creating efficiencies and transparency for the entire enterprise.

Senior management involvement is key to the program's success. As such, sponsorship is important for implementing the program in accordance with the strategy. The fundamentals of sponsorship include providing resources (people, tools, and funding). More advanced sponsorship includes 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.

Funding of resilience activities is key to the program's success. Because resilience is a relatively new aspect to regulatory actions, it is important to monitor and respond to regulatory and cost recovery issues that may affect resilience objectives. Therefore, more advanced programs include a deliberate process for incorporating resilience activities into the rate making/cost recovery process.

Example Transmission Resilience Program Management

The Anywhere Utility Inc. (AUI) management prioritizes having an effective resilience program. A few years ago, the resilience program lacked the structure and management oversight that AUI wanted to achieve. To address this, management roles, responsibilities, and accountability for governing the resilience activities are now defined and documented. Senior managers have approved AUI's transmission business unit (TBU) resilience governance and program structure and specific managers are assigned the responsibility for ensuring appropriate management of the transmission resilience program.

The Senior Vice President of Transmission and her leadership team (i.e., the leaders of each TBU department) have overseen the development and implementation of the transmission resilience strategy. Plans call for reviewing and updating the strategy every three years. The strategy covers such topics as event preparation, operations, event recovery, redundancy, training, and drills/exercises. In addition, the strategy calls for the alignment of the TBU resilience program with other AUI TBU programs, other AUI goals, and the AUI's larger enterprise resilience program.

The Senior Vice President for Transmission is responsible for providing sponsorship for resilience activities and ensuring adequate resources are provided to support resilience program activities. She assigns implementation responsibilities and associated authorities for resilience activities to TBU staff. Transmission resilience stakeholders from other AUI departments and external stakeholders (e.g., other companies, state and local governments, key customers) are identified, documented, and engaged.

In addition, AUI is considering the addition of a new position, Chief Resilience Officer, to oversee all resilience activities for the enterprise. The Chief Resilience Officer's roles and responsibilities would be modeled after those of AUI's current Chief Compliance Officer. The Chief Resilience Officer will have some critical direct reports within the TBU and a working relationship with other groups across the enterprise to support efficient action on resilience issues.

An administrative element of the resilience program involves addressing regulatory and cost recovery issues. The resilience management program has a documented plan for covering the incorporation of resilience activities into the enterprise's rate making decision process. Specific enterprise personnel acquire and assess resilience-related costs, take actions to support cost recovery, and monitor regulatory actions associated with transmission resilience. Also, a TBU Director has responsibility for monitoring rate making and cost recovery activities as it affects Transmission and serves as a liaison to the enterprise group responsible for the overall rate making and cost recovery process.

Objectives and Practices

1. Establish and Maintain Resilience Governance Structure

ID	Practice	MIL
1.1.1	The TBU has an approach to provide program oversight for resilience activities, even if not yet formalized it is at least done in an ad hoc manner.	1
1.1.2	Management's roles, responsibilities, and accountability for oversight of resilience activities are documented and understood although that information might be found in several different documents.	2
1.1.3	The TBU's resilience governance and program structure are documented and readily accessible in a single document (e.g., written charter) or a common information repository (e.g., web page with links).	2
1.1.4	The TBU's resilience program governance structure is approved by TBU senior management and updated on an organization-defined frequency.	3
1.1.5	The governance of the TBU resilience program is part of a larger and comprehensive enterprise-wide resilience program (e.g., a Chief Resilience Officer or senior management has oversight of all enterprise resilience activities).	3

2. Establish and Maintain the Resilience Program Strategy

ID	Practice	MIL
1.2.1	The TBU has a resilience program strategy (i.e., resilience objectives and an approach to achieve them), even if only in an ad hoc manner.	1
1.2.2	There is a documented TBU resilience program strategy that defines goals for the TBU's resilience activities.	2
1.2.3	The TBU's resilience program strategy should consider both traditional and nontraditional events that challenge resilience.	
1.2.4	The documented TBU resilience program strategy includes preparation (longer-term and shorter-term), operating, and recovery components as well as formal mechanisms for incorporating lessons learned.	2
1.2.5	Engagement with external entities and resilience-related activities (e.g., regulators, scientists, electric and other industry groups, and community groups and leaders) is leveraged to define goals and areas for collaboration in the documented TBU resilience strategy.	2
1.2.6	The documented TBU resilience program strategy is regularly reviewed and updated on an organization-defined frequency to account for changes (e.g., changes in industry standards or best practices, the threat environment, operations, technological innovations, stakeholder concerns.)	2
1.2.7	The documented TBU resilience strategy includes provisions for tracking the performance of the resilience program and adjusting the resilience strategy as needed.	3
1.2.8	The documented TBU resilience strategy is independently reviewed and evaluated for its adequacy (i.e., by reviewers who are not involved in the strategy such as an internal audit group, technical peer review group, or third-party consultant; this is not intended to be the regulators).	3
1.2.9	The documented TBU resilience program strategy is aligned with the TBU's and enterprise's strategic objectives and is approved by TBU's senior management.	3

3. Sponsor Resilience Program Activities

ID	Practice	MIL
1.3.1	TBU and appropriate enterprise stakeholders (e.g., Corporate Communications, Human Resources) are identified for resilience activities, even if only in an ad hoc manner.	1
1.3.2	Resource needs (people, tools, training, and funding) are identified (although not necessarily allocated) to support resilience activities, even if only in an ad hoc manner or as part of other programs.	1
1.3.3	Adequate resources (people, tools, training, and funding) are provided to support resilience activities.	2
1.3.4	TBU senior management sponsors the specific resilience activities to implement the resilience program strategy.	2
1.3.5	Implementation responsibilities for resilience activities are assigned to specific personnel with appropriate authority and knowledge.	2
1.3.6	Resilience stakeholders (TBU, enterprise, and external) are identified, documented, and engaged.	2
1.3.7	TBU senior management support for resilience activities is evident via management actions and communications. (e.g., via setting of specific TBU resilience related goals, clear messaging of resilience activities' benefits, and support of external sharing and collaboration on resilience).	2
1.3.8	Processes are in place to secure emergency funds for longer duration, larger impact events.	3
1.3.9	The application of new resilience program processes, tools, and technologies (from internal or external research and development activities) is supported by senior management.	3

4. Incorporate Resilience in Rate Making/Cost Recovery Process

ID	Practice	MIL
1.4.1	The enterprise rate making and cost recovery process addresses resilience needs (in addition to reliability needs), even if only in an ad hoc manner.	1
1.4.2	There is someone supporting the TBU who monitors rate making and cost recovery issues that may affect resilience objectives, even if only in an ad hoc manner.	1
1.4.3	Specific responsibility is assigned within the enterprise or TBU to support the TBU in monitoring rate making and cost recovery issues (including industry trends) that may affect resilience objectives.	2
1.4.4	The formal enterprise rate making and cost recovery process specifically addresses the need for funding resilience program activities.	2
1.4.5	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.	3
1.4.6	Approved rates support adequate funding for key resilience program activities and objectives.	3

7.2 Risk Identification, Assessment, and Management (RM)

Purpose: Establish, operate, and maintain a resilience risk management program to identify, analyze, prioritize, select, develop, and implement actions to address resilience risks.

Transmission system resilience is defined as the ability of the system and its components (i.e., both the equipment and human components) to minimize damage and improve recovery from non-routine disruptions, including high impact, low frequency (HILF) events, in a reasonable amount of time. Resilience includes a diverse range of topics, such as flexibility, hardening, security, and recovery.

A resilience threat will adversely impact an organization's facilities and operations. These threats include actions by malicious actors (e.g., terrorist groups, criminal organizations), non-routine weather events (e.g., hurricanes, major ice storms), earthquakes, solar storms, and others.

A resilience vulnerability is a weakness or flaw in transmission infrastructure, site security, communications systems, IT systems, internal controls, etc. that could be exploited by a non-routine threat and result in a disruption of transmission capabilities that cannot be promptly restored (e.g., an outage lasting many days, weeks, or months). Vulnerability discovery may be performed using internal and external sources of information (e.g., announcements by industry associations or vendors, exercise findings, self-assessment results, and audits.)

Transmission resilience risk is determined by characterizing the consequences of adverse events and the likelihood or susceptibility to the events that could trigger those consequences. Consequences of concern for resilience programs are those that could impact transmission operations (including mission, goals, image, and reputation), resources, and other organizations over an extended period of time. Transmission resilience risk is one component of the overall business risk environment and it feeds into an organization's enterprise risk management program. Transmission resilience risk cannot be completely eliminated, but it can be managed and mitigated through informed decision-making processes.

Further information about risk, as used in this model, is provided in Section 4.3 Relationship to the Risk Management Process.

The Risk Identification, Assessment, and Management (RM) domain comprises six objectives:

1. Identify threats to transmission resilience
2. Identify vulnerabilities to transmission resilience
3. Identify the consequences of transmission resilience threats and vulnerabilities
4. Assess transmission resilience risks
5. Perform risk mitigation activities
6. Management support activities

A transmission resilience risk management program provides direction for analyzing and prioritizing resilience risks, determining risk tolerance, and defining actions that will be taken to manage risks. The program should include a risk assessment methodology and a risk monitoring component. As new risks are identified and existing risks are revisited, the program should be updated to ensure that the organization is prepared to prevent, respond to, and recover from a resilience event. As not every organization faces the same threats or possesses the same vulnerabilities, resilience risk will differ across organizations. The approach to transmission resilience risk management should align with the enterprise risk management approach to ensure that transmission resilience risk is managed in a manner that is consistent with both the TBU's and enterprise's overall mission and business objectives.

Managing transmission resilience risk involves framing, identifying and assessing risks, responding to them (e.g., accepting, avoiding, mitigating, transferring), and monitoring them in a manner that aligns with the needs of the organization. With defined risk criteria, organizations can consistently monitor and respond to identified risks. Defining design basis resilience events can be an integral part of managing resilience risks. Design basis resilience events outline the circumstances for which the resilience program should be designed, implemented, and tested to address in a manner that meets resilience goals. The design basis resilience events can serve as the foundation upon which the resilience program is built. For more information, reference section 4.4 Design Basis Resilience Events.

Example: Management of Transmission Resilience Risks

Anywhere Utility Inc. (AUI) has developed a comprehensive program to manage resilience risks that affect its transmission business unit (TBU). This replaces the former and largely ad hoc program that lacked documentation and consistency. The current transmission resilience risk management program is one aspect of AUI's larger corporate effort to identify and manage key risks. The driver for the transmission resilience risk management effort is a growing awareness that not only must the traditional risks from extreme weather and weather-related events be managed but other threats such as geomagnetic disturbances, electromagnetic pulses, and cyberattacks are expanding the resilience risk landscape and must be addressed.

Foundational to AUI's determination of risk is the identification of the significant resilience-related threats and vulnerabilities that may affect AUI's transmission capabilities. Threat and vulnerability information is obtained from internal and selected external information sources, including national and industry sources, and regularly assessed by designated TBU staff members. Following AUI's risk assessment procedures, designated and trained TBU staff develop detailed characterization of threats and vulnerabilities whose combinations that could pose significant risks to transmission resilience. Using this information design basis resilience events are identified and documented.

After assessing threats and vulnerabilities the resulting range of consequences are assessed. This includes health and safety, business, regulatory, and stakeholder

perception consequences. AUI is developing plans for also including societal impacts, including the interaction of societal impacts and transmission resilience impacts. Because of the difficulty in quantifying probabilities of some events (particularly those associated with emerging threats, technology changes and high impact, low frequency events), AUI implements a relative ranking system (i.e., high, medium, low) to estimate the probability of events that cannot be accurately quantified. Threat, vulnerability, consequence, and likelihood estimates are used to estimate the relative risks to transmission system resilience. Risk information, including supporting information is documented and stored in a risk register. Information on threats, vulnerabilities, and consequences and risk assessments are reviewed and updated at least once every two years.

Potential resilience enhancement activities are identified, assessed, cost-estimated, and documented as part of the risk management program. TBU staff follow procedures to make risk management recommendations for transmission resilience. Procedures allow for expedited decisions to address the most significant risks to transmission resilience. Emphasis is placed on maintaining acceptable risk levels for the TBU's design basis resilience events.

The status of risk management action plans is monitored and documented. Activities to manage the risk include not only programs to harden targeted transmission assets, but also recovery capabilities such as Incident Command Response, mutual aid and assistance, and relationships with key vendors, government agencies, and community organizations.

Objectives and Practices

1. Identify Threats to Transmission Resilience

ID	Practice	MIL
2.1.1	Threat information is obtained from selected information sources, even if only in an ad hoc manner.	1
2.1.2	Threats are identified and characterized as input to further analysis, even if only in an ad hoc manner.	1
2.1.3	Threats and their relevant characterization information are documented.	2
2.1.4	The identification, characterization, and documentation of threats is guided by documented procedures which are updated on an organization-defined frequency.	2
2.1.5	Threat information is obtained from a documented set of sources to support threat management activities (e.g., key internal sources, various critical infrastructure sector ISACs, industry associations, vendors, federal briefings).	2
2.1.6	Documented threat information is independently reviewed by individuals or groups not involved in the collection and characterization of that threat information (such as an internal audit group or third-party consultant but not the regulator).	3

ID	Practice	MIL
2.1.7	Active monitoring of internal and external sources of **threat** information is conducted to provide timely updates of new or evolving threats.	3
2.1.8	**Threat** information is consolidated and maintained in a **risk register** or risk information database.	3

2. Identify Vulnerabilities to Transmission Resilience

ID	Practice	MIL
2.2.1	**Vulnerability** information is obtained from selected information sources, even if only in an ad hoc manner.	1
2.2.2	**Vulnerabilities** are identified and characterized as input to further analysis, even if only in an ad hoc manner.	1
2.2.3	**Vulnerabilities** and their relevant characterization information are documented.	2
2.2.4	The identification, characterization, and documentation of **vulnerabilities** is guided by documented procedures which are updated on an organization-defined frequency.	2
2.2.5	**Vulnerability** information is obtained from a documented set of sources to support vulnerability management activities (e.g., various critical infrastructure sector ISACs, industry associations, vendors, federal briefings).	2
2.2.6	**Documented vulnerability** information (including their relevant characterization information) is independently reviewed by individuals or groups not involved in the original collection and characterization of vulnerabilities (such as an internal audit group or third-party consultant but not the regulator)	3
2.2.7	There is secure two-way information sharing on transmission vulnerabilities with appropriate external stakeholders (e.g., vendors, government agencies, research organizations and consultants, sector organizations, other utilities).	3
2.2.8	**Vulnerability** information is consolidated and maintained in a **risk register** or risk information database.	3

3. Identify the Consequences of Transmission Resilience Threats and Vulnerabilities

ID	Practice	MIL
2.3.1	**Consequences** based upon the TBU's **threats** and **vulnerabilities** are identified, even if only in an ad hoc manner.	1
2.3.2	Identified **consequences** are characterized by level of impact (e.g., minor, moderate, severe), even if only in an ad hoc manner	1
2.3.3	The likelihood of the **consequence** occurring is characterized (e.g., negligible, unlikely, credible) even if only in an ad hoc manner.	1
2.3.4	**Consequence** impact and likelihood information are documented and updated on an organization-defined frequency.	2
2.3.5	**Consequence** impact and likelihood information are collected in accordance with documented procedures.	2

ID	Practice	MIL
2.3.6	Consequence information is independently reviewed by individuals or groups not involved in the original collection and characterization (such as an internal audit group or third-party consultant but not the regulator).	3
2.3.7	Consequence information is consolidated and maintained in a risk register or risk information database.	3

4. Assess Transmission Resilience Risks

ID	Practice	MIL
2.4.1	Risks to transmission resilience are assessed, even if only in an ad hoc manner, using available information on threats, vulnerabilities, and consequences.	1
2.4.2	Risks to transmission resilience are characterized, prioritized, and documented on an organization-defined frequency.	2
2.4.3	There is a documented risk assessment procedure for characterizing and prioritizing risk that is updated on an organization-defined frequency.	2
2.4.4	Based on risk assessments, design basis resilience events are developed and updated on an organization-defined frequency and are used to assist in making risk mitigation decisions.	2
2.4.5	Design basis resilience events are vetted with peer organizations to ensure they cover both traditional and nontraditional events that represent credible, extreme resilience events.	3
2.4.6	Quantitative methods (e.g., tools, models, analyses) are used to assess those resilience risks for which simple qualitative assessments may not provide enough information to support risk management decisions.	3
2.4.7	Risk assessments are independently reviewed by individuals or groups not involved in the original assessment (such as an internal audit group or third-party consultant but not the regulator).	3
2.4.8	Risk information is consolidated and maintained in a risk register or risk information database.	3

5. Perform Risk Mitigation Activities

ID	Practice	MIL
2.5.1	Risk mitigation activities to enhance resilience are identified, even if only in an ad hoc manner.	1
2.5.2	Costs to implement and maintain risk mitigation activities (e.g., hardening of assets, acquisition of spare parts) are estimated, even if only in an ad hoc manner.	1
2.5.3	Risk mitigation activities are prioritized based upon both the costs and risk reductions that could result, even if only in an ad hoc manner.	1
2.5.4	Equipment, systems, and mitigation/recovery plans are designed to support resilience goals (e.g., meeting design basis resilience events).	2
2.5.5	Documented procedures are used for prioritizing risk mitigation activities to enhance transmission resilience.	2
2.5.6	The documented procedure for prioritizing risk mitigation activities is periodically updated to reflect evolving risks and changes in the operational environment.	2

ID	Practice	MIL
2.5.7	Risk mitigation activities to enhance resilience are characterized, prioritized, and documented (e.g., estimating initial and ongoing costs, estimating potential risk reductions).	2
2.5.8	Project management principles (e.g., development of a timeline; logistics planning for resources and personnel; tracking progress, status, and budget) are applied to risk mitigation activities.	2
2.5.9	Transmission resilience risk mitigation activities are aligned with enterprise risk management activities.	3

6. Management Support Activities

ID	Practice	MIL
2.5.1	Risk mitigation activities to enhance resilience are identified, even if only in an ad hoc manner.	1
2.5.2	Costs to implement and maintain risk mitigation activities (e.g., hardening of assets, acquisition of spare parts) are estimated, even if only in an ad hoc manner.	1
2.5.3	Risk mitigation activities are prioritized based upon both the costs and risk reductions that could result, even if only in an ad hoc manner.	1
2.5.4	Equipment, systems, and mitigation/recovery plans are designed to support resilience goals (e.g., meeting design basis resilience events).	2
2.5.5	Documented procedures are used for prioritizing risk mitigation activities to enhance transmission resilience.	2
2.5.6	The documented procedure for prioritizing risk mitigation activities is periodically updated to reflect evolving risks and changes in the operational environment.	2
2.5.7	Risk mitigation activities to enhance resilience are characterized, prioritized, and documented (e.g., estimating initial and ongoing costs, estimating potential risk reductions).	2
2.5.8	Project management principles (e.g., development of a timeline; logistics planning for resources and personnel; tracking progress, status, and budget) are applied to risk mitigation activities.	2
2.5.9	Transmission resilience risk mitigation activities are aligned with enterprise risk management activities.	3

7.3 Situational Awareness (SA)

Purpose: Establish and maintain activities to monitor, analyze, and communicate information in a common operating picture (COP), commensurate with the resilience objectives and risks to the transmission infrastructure. The Time Horizon[13] covered by this domain is Operations Planning and Real-time Operations (i.e., the timeframe where the transmission business unit (TBU) must be aware of threats in order to adjust and implement mitigating strategies, but not far enough in advance to build or harden). Those Long-term Planning actions are covered under the Risk Identification, Assessment, and Management domain.

[13] Time Horizons, as defined by NERC and used in the NERC Reliability Standards (https://www.nerc.com/pa/Stand/Resources/Documents/Time_Horizons.pdf, April 15, 2014).

Situational Awareness provides an understanding of the current resilience landscape, based on knowledge and analysis of both real-time and near real-time knowledge. This is accomplished, in part, through monitoring key aspects of potential threats, vulnerabilities, and risk. It also includes the monitoring the inventory and status of assets and equipment – including spare transmission assets and equipment needed to support resilience program activities (e.g., light vehicles, service vehicles, communication equipment). It further includes information on workforce resources (e.g., available primary response staff and backup staff, available contractor support).

It is important to note that events external to an enterprise can represent imminent or emerging operational threats to the enterprise. Therefore, a broad awareness of relevant external events is necessary to develop and maintain a robust COP. COP is defined as a single identical display of relevant information shared by all affected groups. A COP facilitates collaborative planning and assists all groups to achieve situational awareness. The COP aggregates information from multiple topical areas such as cyber, physical, telecommunications, and system operations. The COP leverages various technologies to collect, analyze, alarm, present, and use the aggregated information for timely, effective TBU decision-making and actions.

The COP serves as a key input to the Event Response and Recovery domain activities (reference section *7.4 Event Response and Recovery (ERR)*).

The Situational Awareness (SA) Domain comprises three objectives.

1. Perform monitoring
2. Establish, maintain, and communicate a Common Operating Picture (COP)
3. Management support activities

Monitoring activities should be prioritized based on the potential magnitude and likelihood of the defined threat's negative impact to operations. Higher probability events with more severe impacts should garner more monitoring activity.

Effectively communicating the current state and potential future states to decision-makers is the essence of an effective COP.

Example: Situational Awareness

Staff members in the Anywhere Utility Inc. (AUI) transmission business unit (TBU) are tasked with performing monitoring of internal and external sources of information to support Situational Awareness and a common operating picture (COP). This starts with detecting and monitoring operational threats that may negatively impact transmission operations. Threats of interest include, but are not limited to, meteorological events, geological phenomenon, space weather, and physical and cybersecurity attacks. Situational analysis also includes monitoring of vulnerabilities and transmission resilience resources and capabilities.

A few years ago, AUI's TBU conducted Situational Awareness activities related to

transmission resilience in a mostly ad hoc manner, without formal procedures or documentation requirements. Currently, threat communication procedures are documented for obtaining and analyzing information from both internal and external sources for use in transmission operations. Information on the status of the assets, equipment, and resources (including the workforce) used to support resilience events are assessed to support the Situation Analysis.

AUI's TBU hosts a daily briefing to develop the COP. This includes the participation of representatives from groups outside the TBU (e.g., cybersecurity, physical security, communications) that provide input to the COP. Experts report on potential threats, TBU status, and any change in status of resilience resources and capabilities. At the conclusion of each briefing, a designated TBU staffer aggregates the information into a concise COP for dissemination to all interested parties. The COP also includes a stoplight (red/yellow/green) designator to easily convey the day's status. AUI is considering further improvements to this process, including the possibility of a dedicated control center to aggregate and analyze inputs from the various areas on a 24/7/365 basis.

As feedback to the longer-range resilience activities, threats identified during day-to-day operations are provided to personnel handling risk analyses to determine likelihood and potential impacts in accordance with the TBU risk assessment program.

Objectives and Practices

1. Perform Monitoring

ID	Practice	MIL
3.1.1	TBU performs monitoring of internal sources of information for detecting emerging threats that may negatively impact the transmission system or the TBU, even if only in an ad hoc manner.	1
3.1.2	TBU performs monitoring of external sources of information (e.g., external sources such as space weather reports, severe weather forecasts, ShotSpotter, energy-Information Sharing and Analysis Center [E-ISAC]) for detecting emerging threats that may negatively impact the transmission system or the TBU, even if only in an ad hoc manner.	1
3.1.3	Documented processes provide guidance on how internal and external sources of information are leveraged to detect threats that are currently impacting or forecast to affect the transmission system and its supporting systems (e.g., IT systems, OT systems, telecommunications).	2
3.1.4	Monitoring information is correlated from multiple sources to identify threat patterns and trends.	2
3.1.5	Given the risk of simultaneous attacks (e.g., cyberattack occurring at the same time as a pandemic, coordinated physical and cyberattack), documented processes are established for information exchange among all potentially affected parts of the TBU and support an appropriate response.	2
3.1.6	Results of monitoring activities are provided as input to resilience risk assessments.	2
3.1.7	Predictive methods and models are used to augment monitoring activities and advise proactive responses.	3

3.1.8	Specific individuals or a designated group are responsible for monitoring activities to integrate situational awareness information across all potential impacted areas of the enterprise (e.g., physical security, cybersecurity, operations, communications).	3
3.1.9	Automated mechanisms are used to scan, analyze, prioritize, and report key situational awareness information to provide timely notification of active events.	3

2. Establish, Maintain, and Communicate a Common Operating Picture (COP)

ID	Practice	MIL
3.2.1	The TBU aggregates information from multiple topical areas such as cyber, physical, telecommunications, and operations to provide situational awareness, even if only in an ad hoc manner.	1
3.2.2	Methods of communicating the aggregated information exist, even if only in an ad hoc manner.	1
3.2.3	The TBU routinely creates a Common Operating Picture (COP) to provide a clear understanding of current status and existing or potential threats and consequences.	2
3.2.4	Parameters of the COP have been defined and include inputs from resilience-related monitoring activities to cover all relevant areas (operating, physical, cyber, telecommunications).	2
3.2.5	Methods of communicating the COP are established and maintained to support situational awareness at all levels of the TBU.	2
3.2.6	Documented processes exist for using the COP as input/feedback to resilience risk assessments.	2
3.2.7	The COP includes visualizations (e.g., dashboard, red/yellow/green status, graphics) to facilitate understanding of the state of defined threats and risks, including both IT/OT, cyber/physical, and operational areas.	3
3.2.8	Predetermined actions are defined and invoked (in a manual or automated process) based on the COP.	3
3.2.9	Methods of communicating the COP are established and maintained to support situational awareness at all levels of the enterprise.	3

3. Management Support Activities

ID	Practice	MIL
3.3.1	Internal stakeholders for situational awareness activities are identified and involved, even if only in an ad hoc manner.	1
3.3.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support situational awareness activities, even if only in an ad hoc manner.	1
3.3.3	Adequate resources (people, funding, training, and tools) are provided for resilience-related situational awareness activities.	2
3.3.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development of resilience-related policies and procedures for situational awareness activities.	2
3.3.5	Responsibility and authority for the performance of resilience activities related to this domain are assigned to specific personnel.	2
3.3.6	Formal processes are used to incorporate resilience lessons learned into future plans for situational awareness activities.	3

ID	Practice	MIL
3.3.7	Leveraging research and development activities to deploy new processes, tools, and technologies for resilience activities related to this domain are supported by senior management.	3
3.3.8	Metrics exist to monitor, measure, and trend situational awareness activities in order to track and improve resilience capabilities.	3

7.4 Event Response and Recovery (ERR)

Purpose: Establish, maintain, and exercise plans, procedures, and technologies to respond to and recover from events affecting transmission business unit (TBU) resilience, commensurate with the resilience objectives and risks to the transmission infrastructure.

A key element of resilience is the TBU's ability to respond to and recover from an actual resilience event. To achieve a good outcome the TBU must have defined plans and capabilities for restoration and recovery as well as be able to satisfactorily execute these capabilities. Integral to those capabilities is implementation of an incident command structure (e.g., based on Federal Emergency Management Agency (FEMA) Incident Command System (ICS)). Given that employees are integral to the restoration and recovery process, the TBU must pay special attention to addressing employee needs so that they can perform their defined tasks.

The Response and Recovery (ERR) domain comprises five objectives:

1. Develop and maintain response and recovery capabilities
2. Exercise/drill response and recovery capabilities
3. Communicate and share pertinent information during an event
4. Provide support for personnel participating in response and recovery
5. Management support activities

This domain covers the creation and management of the necessary plans and actions to respond to an actual resilience event. Trends from historical COPs, as well as lessons learned from events or drills/exercises, are an important input for this domain's activities by providing beneficial information for continuous improvement of response and recovery capabilities. However, going beyond historical events and contemplating non-routine, extreme resilience events are critical for the TBU to integrate flexibility and scalability into their plans for responding to the wide range of potential resilience events and their impacts. Drills and exercises are an important tool in identifying improvement opportunities in responding to these notable, but infrequent scenarios.

Example: Event Response and Recovery

The transmission business unit (TBU) for Anywhere Utility Inc. (AUI) prioritizes its ability to respond and recover from an event that could potentially challenge its transmission resilience capabilities. Historically, response and recovery has always been a priority, but the program lacked documented procedures and responsibilities. In addition, response and recovery processes were built to manage the traditional weather risks of ice storms, hurricanes, and tornadoes in AUI's service area, with little consideration of newer threats such as geomagnetic disturbances, electromagnetic pulses (EMP), and cyberattacks. Industry peers were consulted to identify good and best practices for responding and recovering from an event that challenged transmission resilience.

As a result, AUI's response and recovery program is now formalized. The TBU has documented plans that are flexible and scalable in order to respond to and recover from credible events. Management roles and responsibilities are clearly defined in the plans. Response and recovery plans address recovery to both a (near-term) stable state and (longer-term) normal state. Plans are coordinated with multiple AUI business units, government agencies, and mutual assistance partners. Procedures cover the secure sharing of sensitive information.

Incident response drills/exercises are conducted with internal and external partners at least once every two years. AUI's drills include broad participation with external entities such as neighboring electric utilities, natural gas utilities, government entities, and law enforcement. Procedures govern assessing, confirming, and de-conflicting information received from partners. In conjunction with lessons learned from exercises/drills, response and recovery plans are reviewed and updated every two years. To augment the current drills/exercises, AUI is planning to implement an annual tabletop exercise to engage their enterprise executives in response and recovery activities.

A relatively new element in the response and recovery plans involves employee support during a resilience event. The plans incorporate provisions for food, water, housing, and medical support for employees during longer duration events (i.e., weeks not days).

Objectives and Practices

1. Develop and Maintain Response and Recovery Capabilities

ID	Practice	MIL
4.1.1	Response capabilities are available to reduce the consequences of resilience events, even if only organized in an ad hoc manner.	1
4.1.2	Plans are in place to prepare for and execute recovery, even if only in an ad hoc manner.	1
4.1.3	The TBU has implemented an incident command structure, (e.g., based on the FEMA Incident Command System), even if it is informal and is not documented.	1

ID	Practice	MIL
4.1.4	The TBU has documented plans to respond and recover from resilience events that are reviewed and updated on an organization-defined frequency.	2
4.1.5	The TBU has documented response and recovery plans that lay out a formal structure for the Incident Command System.	2
4.1.6	The TBU's documented response and recovery plans include provisions for mutual assistance.	2
4.1.7	The TBU's documented response and recovery plans address recovery to both a near-term stable state and longer-term normal state.	2
4.1.8	The TBU's documented response and recovery plans are coordinated with local/state/federal law enforcement as appropriate, including support for evidence collection and preservation.	2
4.1.9	The TBU's documented response and recovery plans address information sharing with government entities (e.g., DOE, CDC, state/local governments) during an event.	2
4.1.10	The TBU's documented response and recovery plans address longer duration events (i.e., weeks to months) resulting in 1) loss of equipment or supporting infrastructure (e.g., due to natural or physical threats) and 2) unavailability of expert personnel (e.g., due to pandemic threats).	2
4.1.11	The TBU's documented response and recovery plans address temporary lines of succession for scenarios where primary responsible personnel are not able to get to critical locations or are incapacitated.	2
4.1.12	The TBU's documented response and recovery plans are coordinated across the enterprise.	3
4.1.13	The TBU's documented response and recovery plans address simultaneous attacks (e.g., cyberattack occurring at the same time as a pandemic, coordinated physical and cyberattack).	3
4.1.14	The TBU's documented response and recovery plans are agile, flexible, and able to scale up response resources to deal with longer duration/larger geographical impacts (e.g., as should be covered in the TBU's design basis resilience events).	3

2. Exercise/Drill Response and Recovery Capabilities

ID	Practice	MIL
4.2.1	The TBU's response and recovery drills/exercises are conducted, at least in an ad hoc manner.	1
4.2.2	The TBU's response and recovery drills/exercises are conducted at an organization-defined frequency.	2
4.2.3	The TBU's response and recovery drills/exercises are designed to simulate impacts to a larger geographical area, beyond just impacts to the organization's service territory (e.g., as considered in the TBU's design basis resilience events.)	2
4.2.4	Agility, flexibility, and scalability of response and recovery plans are tested via drills/exercises on an organization-defined frequency.	3
4.2.5	Drills/exercises are conducted routinely with broad and active participation by groups within the company, chief executive officers, and external agencies (e.g., state and local government agencies, national guard, Red Cross, trade groups).	3

3. Communicate and Share Pertinent Information During an Event

ID	Practice	MIL
4.3.1	Information is available from identified internal and external communications partners and shared with them as appropriate before, during and after an event, even if the communication is conducted in an ad hoc manner.	1
4.3.2	Documented processes provide for accurate and up-to-date information to affected personnel and prevent misinformation.	2
4.3.3	Documented processes enable secure sharing of sensitive information, both internally and externally during an event.	2
4.3.4	Documented processes address methods for validating the authenticity of directives (e.g., from control center, Reliability Coordinator, state or government agencies).	2
4.3.5	Communications that support effective decision-making flow consistently up and down the enterprise chain of command.	3
4.3.6	Documented processes provide for secure sharing of all information, both internally and externally during an event.	3

4. Provide Support for Personnel Participating in Response and Recovery

ID	Practice	MIL
4.4.1	Provisions are made for the physical safety and security of response and recovery personnel (e.g., employees, contractors, mutual assistance crews), even if only in an ad hoc manner.	1
4.4.2	The plans to support personnel participating in response and recovery are documented and reviewed and updated on an organization-defined frequency.	2
4.4.3	The documented plan considers the need for the acquisition, storage, and distribution of food and water for use by response and recovery personnel during longer duration events (i.e., weeks to months).	2
4.4.4	The documented plan incorporates provisions for secure, temporary or alternative housing for response and recovery personnel during longer duration events (i.e., weeks to months).	2
4.4.5	The documented plan provides for medical and psychological support to response and recovery personnel during longer duration events (i.e., weeks to months). Medical support includes providing for prescription medicines, timely access to medical care, etc.	2
4.4.6	The documented plan addresses the need for regular and timely communication between response and recovery personnel and their families during a resilience event. (Supports psychological well-being/peace of mind for the deployed employees that their families are safe and secure).	3
4.4.7	The documented plan includes a consideration of the safety, security, and well-being of employees not currently involved in the response and recovery activities but who could be called in to provide support during later stages of an event.	3

5. Management Support Activities

ID	Practice	MIL
4.5.1	Internal stakeholders for event response & recovery activities are identified and involved, even if only in an ad hoc manner.	1
4.5.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support event response & recovery activities, even if only in an ad hoc manner.	1
4.5.3	Adequate resources (people, funding, training, and tools) are provided for resilience-related event response & recovery activities.	2
4.5.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development of resilience-related policies and procedures for event response & recovery activities.	2
4.5.5	Responsibility and authority for the performance of resilience activities related to this domain are assigned to specific personnel.	2
4.5.6	Formal processes are used to incorporate lessons learned into future plans for event response & recovery activities.	3
4.5.7	Leveraging research and development activities to deploy new processes, tools, and technologies for resilience activities related to this Domain are supported by senior management.	3
4.5.8	Metrics exist to monitor, measure, and trend event response & recovery activities in order to track and improve resilience capabilities.	3

7.5 Transmission and Supporting Equipment Management (EqM)

Purpose: Identify and manage assets used to detect, identify, analyze, prepare for, respond to, and recover from resilience threats and events. For the purposes of this model, assets to be considered include things such as transmission equipment, tools, databases, software, computer hardware, vehicles.

In order to effectively manage resilience challenges, the transmission business unit (TBU) needs a variety of assets to be able to detect, identify, analyze, respond to, and recover from resilience threats and events.

These assets include:

- transmission system equipment (e.g., transformers, poles, relays)
- transmission support equipment (e.g., tools for repairing transmission system equipment, vehicles for transporting materials and personnel, tools for system analyses, monitoring, and managing restoration processes).

The Transmission and Supporting Equipment Management (EqM) domain comprises four objectives:

1. Identify and manage transmission equipment
2. Develop and coordinate transmission equipment spare program

3. Identify and manage supporting equipment
4. Management support activities

As the TBU develops its transmission and supporting equipment management approach, the starting point is to identify the assets that are already in place that the TBU has historically used to mitigate and respond to events. This asset suite would then need to be reviewed and assessed relative to its resilience risk profile in order to make appropriate enhancements. Ongoing maintenance of the assets due to changes in availability, risks, threats, etc. is imperative to the overall management of assets.

A key element of managing resilience events is a robust spare equipment program which considers things such as the number, types, and locations of equipment as well as the ability to move spare equipment to needed locations during a resilience event.

Example: Transmission and Supporting Equipment Management

The transmission business unit for Anywhere Utility Inc. (AUI) has an Asset Management department that manages the transmission equipment (e.g., transformers, poles, relays) needed to provide and deliver an adequate level of transmission resilience per the TBU's resilience program. Historically, transmission equipment were managed with support tools that only addressed assets designed to deal with events that have occurred in the past (e.g., severe weather) and did not explicitly address different types of high impact, low frequency (HILF) events. Other aspects of the resilience asset management program lacked formal documentation.

To implement a more comprehensive asset management system for resilience events, the TBU has developed and implemented new procedures and tools to effectively manage all resilience assets, including both transmission equipment and supporting equipment. Plans and procedures are now instituted to support the timely procurement of assets needed to support the resilience program. Procedures call for the prompt identification and tracking of resilience assets. Critical resilience assets are identified and staged for rapid deployment. Critical assets are also maintained and tested on a periodic basis (which varies depending on the type of asset) according to documented procedures.

Enterprise-level policies call for the spare transmission equipment program to address both reliability and resilience issues. TBU senior leadership is assigned the responsibility of assuring the acquisition and maintenance of adequate spare parts. Key aspects of the program consider:

- Staging of spare equipment at strategic locations
- Transportation plans for spares
- Shielding provisions for certain types of spare equipment
- Rotation of spares to ensure efficient use of equipment life

- Exploration of participation in spare sharing programs
- Plug-and-play capabilities (standardization for efficient use of spares across AUI and with neighbors).

Senior leadership is also responsible for explicitly addressing spare equipment needs in the enterprise's long-term investment planning. The spare equipment program is reviewed and updated at least once every two years.

Objectives and Practices

1. Identify and Manage Transmission Equipment

ID	Practice	MIL
5.1.1	Key types of transmission equipment (e.g., transformers, breakers, relays, poles) important to maintaining resilience of the transmission system and responding to a resilience event have been identified, even if only in an ad hoc manner.	1
5.1.2	A listing of key types of transmission equipment important to maintaining resilience and responding to a resilience event is documented and updated on an organization-defined frequency.	2
5.1.3	Detailed and specific inventory information (e.g., location, asset owner, type of asset/tool, equipment number, vendor/manufacturer, operational or staged for backup) is documented using an asset management or tracking tool for assets categorized as key types of transmission equipment for resilience.	2
5.1.4	Changes to inventoried transmission equipment are identified and documented using an asset management or tracking tool.	2
5.1.5	The transmission business unit (TBU) has an ongoing maintenance and testing program that addresses the unique needs of transmission equipment important for resilience.	2
5.1.6	The TBU actively works to identify and acquire technological advances that could enhance the resilience of transmission equipment (e.g., new tools, approaches).	3
5.1.7	The TBU uses risk-based assessments to evaluate the resilience capabilities of its transmission equipment.	3

2. Develop and Coordinate Transmission Equipment Spare Program

ID	Practice	MIL
5.2.1	The TBU has a transmission equipment spare program, even if only in an ad hoc manner.	1
5.2.2	The transmission equipment spare program is guided by documented policies and procedures that are updated at an organization-defined frequency.	2
5.2.3	The documented transmission equipment spare 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 timeliness of restoration.	2
5.2.4	The documented transmission equipment spare program prioritizes classes of critical components (e.g., certain types or voltage classes of transformers) based on the need for this equipment during events that challenge resilience.	2

ID	Practice	MIL
5.2.5	The documented transmission equipment spare program covers requirements for spare equipment maintenance and operability (e.g., periodic testing and maintenance of warehouse stock, deployment of warehouse stock to field with replenishment by new purchases).	2
5.2.6	The documented transmission equipment spare program is coordinated with spare equipment programs of other business units (e.g., distribution, generation).	3
5.2.7	The TBU performs and documents risk-based assessments to determine the acceptable number and location of spare transmission equipment.	3
5.2.8	The documented transmission equipment spare program is coordinated with neighboring utilities, as well as through industry partnerships (e.g., EEI STEP, RESTORE).	3
5.2.9	The documented transmission equipment spare program is coordinated with vendors to ensure availability during times of high demand by many organizations (e.g., during a resilience event impacting a large area).	3
5.2.10	The documented transmission equipment spare program adopts standard designs to facilitate the efficient use of spares, including replacement and sharing of assets when needed (e.g., plug-n-play).	3

3. Identify and Manage Supporting Resources

ID	Practice	MIL
5.3.1	Key types of supporting equipment and components (e.g., tools, software, telecommunications, vehicles, non-transmission equipment) important to maintaining resilience of the transmission system and responding to a resilience event have been identified, even if only in an ad hoc manner.	1
5.3.2	A listing of key types of supporting equipment important to maintaining resilience and responding to a resilience event is documented and updated on an organization-defined frequency.	2
5.3.3	Detailed and specific inventory information (e.g., location, asset owner, type of asset/tool, equipment number, vendor/manufacturer, operational or staged for backup) is documented using an asset management or tracking tool for assets categorized as key types of supporting equipment for resilience.	2
5.3.4	Changes to inventoried supporting equipment are identified and documented using an asset management or tracking tool.	2
5.3.5	The transmission business unit (TBU) has a maintenance and testing program to evaluate and maintain the health of resilience supporting equipment (both in-service as well as spares waiting in inventory).	2
5.3.6	The TBU actively works to identify and acquire technological advances that could enhance the resilience of supporting equipment (e.g., new tools, approaches).	3
5.3.7	The TBU performs risk-based assessments to determine the acceptable number and location of resilience supporting equipment (both in-service as well as spares waiting in inventory)	3
5.3.8	The documented supporting equipment spare program is analogous to and has the same level of detail as the transmission equipment spare program.	3

4. Management Support Activities

ID	Practice	MIL
5.4.1	Internal stakeholders for transmission and supporting equipment management activities are identified and involved, even if only in an ad hoc manner.	1
5.4.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support transmission and supporting equipment management activities, even if only in an ad hoc manner.	1
5.4.3	Adequate resources (people, funding, training, and tools) are provided for resilience-related transmission and supporting equipment management activities.	2
5.4.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development of resilience-related policies and procedures for transmission and supporting equipment management activities.	2
5.4.5	Responsibility and authority for the performance of resilience activities related to this domain are assigned to specific personnel.	2
5.4.6	Formal processes are used to incorporate resilience lessons learned into future plans for transmission and supporting equipment management activities.	3
5.4.7	Leveraging research and development activities to support the deployment of new processes, tools, and technologies for resilience activities related to this Domain are supported by senior management.	3
5.4.8	Metrics exist to monitor, measure, and trend transmission and supporting equipment management activities in order to track and improve resilience capabilities.	3

7.6 Information Sharing and Communications (ISC)

Purpose: Establish and maintain relationships, procedures, and capabilities (both voice and data) with internal and external entities to collect and provide resilience information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with resilience objectives and risks to transmission infrastructure.

The objective of information sharing is to strengthen resilience that supports transmission capabilities and the interconnected critical infrastructure, by establishing and maintaining a framework for interaction, communication, and information sharing. This includes communication within an organization or enterprise, with external partners, and with government agencies.

The Information Sharing and Communications (ISC) domain comprises four objectives:

1. Identify internal and external communication partners
2. Build information sharing and communication relationships
3. Manage/maintain communications tools
4. Management support activities

Sharing resilience information begins with identifying the communication partners relevant to the TBU and the enterprise. This information is available from many internal and external sources. External partners may include electric, gas, telecommunications, water utilities, and critical end users; vendors; local, state, and federal governments (including both elected officials and first responders); meteorological organizations; the news media; and the general public. While identification is the first step, using that information and building relationships with communication partners before an event is integral to successful restoration and recovery. Drills/exercises are important vehicles for building those relationships and building expertise for the TBU and their communication partners. Drills/exercises also provide verifications of communication tools' capabilities.

Essential to the resilience posture of any entity is the sharing of different types of risk-related information both within the organization and with external partners. A sound internal communications plan in many cases is an important precursor to facilitating coordinated communications with external partners. Consequently, the secure distribution of information both internally and externally is vital. As threats and vulnerabilities are discovered, organizations should ensure that relevant data is effectively and appropriately shared before, during, and after events so that peers may also reduce their risk and improve resilience. Forums, such as the Electricity Information Sharing and Analysis Center (E-ISAC)[14] for the electricity subsector, can facilitate this sharing among critical infrastructure sectors and subsectors.

Example: Information Sharing and Communications

The Anywhere Utility Inc. (AUI) has historically managed relationships with several external agencies to deal with severe weather events. These agencies include local and state government, law enforcement, neighboring utilities, and mutual aid arrangements through trade associations. However, given the changing threat landscape (e.g., physical security, cybersecurity, electromagnetic pulse (EMP)) AUI reviewed its communication plan and determined increased rigor was needed. This increased rigor included the identification of additional communications partners as well as the development of relations and communication tools/processes with these partners. By contemplating more severe, nontraditional threats, AUI identified the potential for primary communications tools to be unavailable for certain scenarios. Therefore, AUI has joined a research and development project exploring resilient, alternate communication tools.

Procedures were developed and implemented to identify and document a comprehensive list of internal and external partners. Roles and responsibilities for maintaining up-to-date information on communication partners are assigned to personnel. Procedures to contact the identified partners are documented and contact procedures and information are updated annually. Contact information is verified at least twice a year via exercises.

[14] For more information, please visit the E-ISAC website: https://www.eisac.com/

The TBU implements and maintains tools for communicating with its communication partners, including redundant methods for high priority partners. Communication tools are reviewed and tested to identify deficiencies and opportunities for improvement. Personnel performing testing and maintenance of communications tools have the skills, knowledge, and resources needed to perform their assigned responsibilities.

Objectives and Practices

1. Identify Internal and External Communication Partners

ID	Practice	MIL
6.1.1	Enterprise (internal) communication partners are identified, even if only in an ad hoc manner.	1
6.1.2	External communication partners are identified, even if only in an ad hoc manner. External partners may include other utilities that provide infrastructure services, critical users of electrical power vendors, governments, law enforcement, broadcast media, regulatory agencies, etc.	1
6.1.3	Internal and external communication partners are identified and documented.	2
6.1.4	Internal and external communication partners' contact information is reviewed, verified with them, and updated on an organization-defined frequency.	2
6.1.5	Responsibilities for maintaining a current list of internal and external communication partners are assigned to personnel.	2
6.1.6	Procedures and methods to contact the internal and external identified partners are documented and updated on an organization-defined frequency.	2
6.1.7	The TBU, working with Human Resources, has processes to obtain listings of contact information for TBU employees and their families for use by authorized communicators during a resilience event.	3
6.1.8	Internal and external communication partner contact information is prioritized by relevance to continued operations or recovery (i.e., risk and shared interest).	3

2. Build Information Sharing and Communication Relationships

ID	Practice	MIL
6.2.1	Outreach is periodically conducted with internal and external communications partners (i.e., outreach occurs even when there is no pending event) for relationship building, even if only in an ad hoc manner.	1
6.2.2	Outreach responsibilities are documented and updated on an organization-defined frequency.	2
6.2.3	Outreach with internal and external communications partners is conducted at the organization-defined frequency.	2
6.2.4	Drills/exercises with internal and external communications partners are conducted to test two-way communications/coordination and build relationships.	3
6.2.5	Information-sharing requirements have been jointly defined and documented with internal and external partners and address timely dissemination or exchange of pertinent information.	3

3. Manage/Maintain Communications Tools

ID	Practice	MIL
6.3.1	The TBU tests and maintains tools for communications with internal and external communication partners, even if only in an ad hoc manner.	1
6.3.2	Redundancy (e.g., backup tools, alternate paths/tunnels) exists for communication resources used with high priority partners.	2
6.3.3	Communication tools are reviewed, tested, and updated on an organization-defined frequency to consider any gaps, necessary changes, and the latest technological advances.	2
6.3.4	Drills/exercises are conducted using primary and redundant communication resources on an organization-defined frequency.	2
6.3.5	Alternative, resilient communications resources are available for communications with internal and external partners (e.g., portable radios, satellites, fiber optics).	3
6.3.6	Communication tools consider the need for continued operability during longer duration (i.e., weeks to months) resilience events.	3
6.3.7	Tools are used to facilitate and automate, effective communications to internal and external partners (e.g., using methods like direct dialing or messaging) during events and drills/exercises.	3

4. Management Support Activities

ID	Practice	MIL
6.4.1	Internal stakeholders for information sharing and communications activities are identified and involved, even if only in an ad hoc manner.	1
6.4.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support information sharing and communications activities, even if only in an ad hoc manner.	1
6.4.3	Adequate resources (people, funding, training and tools) are provided for resilience-related information sharing and communications activities.	2
6.4.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development of resilience-related policies and procedures for information sharing and communications activities.	2
6.4.5	Responsibility and authority for the performance of resilience activities related to this domain are assigned to specific personnel.	2
6.4.6	Formal processes are used to incorporate resilience lessons learned into future plans for information sharing and communications activities.	3
6.4.7	Leveraging research and development activities to support the deployment of new processes, tools, and technologies for resilience activities related to this Domain are supported by senior management.	3
6.4.8	Metrics exist to monitor, measure, and trend information sharing and communications activities in order to track and improve resilience capabilities.	3

7.7 Supply Chain and Critical Entities Management (SCE)

Purpose: Establish and maintain relationships with suppliers and other key resources needed to respond to a transmission resilience event commensurate with resilience objectives and the risk to the transmission infrastructure (e.g., establishing mutual aid agreements, managing key vendor and customer relations, establishing spare equipment sharing arrangements)

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

Supply chain risk is a noteworthy example of a supplier dependency. The characteristics of products and services vary widely. Without proper supply chain management, new threats can be introduced, including software of unknown provenance and counterfeit hardware. Requests for proposals often give suppliers of high-technology systems, devices, and services only rough specifications, which may lack adequate requirements for security and quality assurance. Therefore, it is important to consider transmission resilience requirements in managing procurement activities (e.g., via agreements, acceptance testing, mitigation strategies).

A key element in supply chain and critical entities management is the identification of the TBU's "critical entities" (see the definition of *critical entities* in APPENDIX B: GLOSSARY). These critical entities can impact the TBU, the Bulk Electric System (BES), or society at large.

When identifying critical entities, it is important to remember that it is more than just traditional supply chain partners (i.e., supply chain critical entities) with which the TBU typically has strong, contractual relationships, such as breaker manufacturers and internet service providers. Critical entities also include:

- Entities that do not have the formal contracts or agreements of supply chain entities and provide essential products or services to the electricity subsector and are dependent upon the TBU for their electricity needs (either directly or indirectly), such as natural gas compressor stations and generators. These are considered electricity subsector critical entities.
- Entities that do not fall into the previous two categories (supply chain or electricity subsector critical entities) and provide essential products or services to the society at large and are dependent upon the TBU for their electricity needs (either directly or indirectly), such as telecommunication nodes, defense and military facilities, water pumping stations, hospitals and medical centers. These are considered society critical entities.

The Supply Chain and Critical Entities Management (SCE) domain comprises five objectives:

1. Identify critical entities
2. Manage the supply chain to support resilience
3. Manage the needs of electricity subsector critical entities to support resilience

4. Manage the needs of society critical entities to support resilience
5. Management support activities

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

Managing dependency risk involves an array of potential activities. One example involves implementing supplier/customer agreements that contain resilience requirements. Supplier agreements are of even greater importance when there are a limited number of suppliers providing critical products/services for multiple, simultaneous requests. Holistically, the TBU's suppliers should be adequately diverse in both their capabilities and geographical locations. Another example involves the sharing of resilience-related threat information with other critical infrastructure entities.

Example: Supply Chain and Critical Entities Management

The transmission business unit (TBU) for Anywhere Utility Inc. (AUI) requires well-established relationships with a diverse set of key suppliers and vendors to meet its routine needs as well as potential needs that could arise during resilience events. Historically, while AUI's supply chain and critical entities management adequately addressed routine operations, resilience needs (i.e., needs resulting from long duration, widespread events impacting not just AUI, but a number of utilities) were not as well covered by policies and procedures. The TBU recognized that the broad multi-company/wide geographic scope of some resilience events would put great strain on the traditional supply chains, as there would be simultaneous demands on suppliers from multiple companies during these resilience events. As a result, enhancements were made to the supply chain and critical entities management program and AUI has started conversations with other utilities to discuss competing demands during extreme events.

The TBU now has procedures in place directing the identification, documentation, prioritization, and annual review of supply chain and critical entities management information involving its critical entities for resilience. Critical entities include those that the TBU is dependent on (e.g., equipment vendors, fuel suppliers) and those that depend on the TBU for their electricity needs. Since AUI does not directly serve all these critical entities, but instead delivers to Distribution Providers (DPs) who, in turn, serves some of the critical entities, AUI has implemented outreach to the DPs in order to more comprehensively identify and manage all critical entities. Also, since a subset of the critical entities could impact society at large, and not just AUI or the BES, AUI has planned outreach to water, telecommunications, government, and other entities critical to key society needs.

Per AUI's procedures, all critical entities are periodically contacted to gather information on interdependencies, associated risks, and potential mitigation steps. Resilience requirements are included in new procurement contracts with suppliers and vendors. Agreements also require notification by suppliers and vendors of vulnerabilities in their products (e.g., security vulnerabilities, product defects) and services throughout the intended life cycle of delivered products and contracts. Information sources are monitored to provide timely identification of

potential supply chain threats. Procedures covering acceptance testing of procured assets are required to include testing for stresses that may be present during resilience events. Key suppliers and other critical entities are reviewed at an organization-defined frequency for their ability to continually meet resilience requirements and their potential impact during resilience events.

Objectives and Practices

1. Identify Critical Entities

ID	Practice	MIL
7.1.1	The transmission business unit's (TBU) key supply chain critical entities (both product and service providers) are identified, even if only in an ad hoc manner.	1
7.1.2	Key electricity subsector critical entities are identified, even if only in an ad hoc manner. (Examples include natural gas compressor stations, telecommunication nodes).	1
7.1.3	Key society critical entities are identified, even if only in an ad hoc manner. (Examples include telecommunication nodes, defense and military facilities, water pumping stations, hospitals and medical centers).	1
7.1.4	The TBU's supply chain critical entities are identified, documented (e.g., company names, contact information, nature of the TBU's dependency on their services), and updated on an organization-defined frequency.	2
7.1.5	Electricity subsector critical entities are identified, documented (e.g., company names, contact information, nature of their dependency on the TBU's services) and updated on an organization-defined frequency.	2
7.1.6	Society critical entities are identified, documented (e.g., company names, contact information, nature of their dependency on the TBU's services) and updated on an organization-defined frequency.	2
7.1.7	The TBU has a documented prioritization of supply chain critical entities whose support may be needed to restart or maintain power transmission during a resilience event.	2
7.1.8	The TBU has a documented prioritization of electricity subsector critical entities whose support may be needed to 1) provide essential products or services to the electric utility industry or 2) restart or maintain power transmission during a resilience event.	2
7.1.9	The TBU has a documented prioritization of society critical entities whose support may be needed to provide essential products or services to society at large.	2
7.1.10	The TBU has a documented and prioritized list of alternative or backup suppliers and service providers who could be solicited to meet the critical needs of the TBU during a severe events (e.g., as considered in the TBU's design basis resilience events) when scarce resources might be in high demand.	3

2. Manage the Supply Chain to Support Resilience

ID	Practice	MIL
7.2.1	Supply chain critical entities (both product and service providers) are contacted to discuss supply chain risks and potential mitigation steps, even if only in an ad hoc manner.	1

ID	Practice	MIL
7.2.2	Cybersecurity requirements are considered when establishing relationships with **supply chain critical entities**, even if only in an ad hoc manner.	1
7.2.3	Diversification and redundancy (e.g., numbers, capabilities, and location) requirements are considered when choosing **supply chain critical entities**.	2
7.2.4	Evaluation and selection of **supply chain critical entities** includes a documented consideration of their ability to meet cybersecurity requirements.	2
7.2.5	Following a documented process, **supply chain critical entities** are engaged at an organization-defined frequency to assess their abilities to meet the TBU's resilience requirements.	2
7.2.6	Agreements with **supply chain critical entities** require prompt notification to the TBU of newly identified equipment vulnerabilities (e.g., security vulnerabilities, product defects) throughout the intended life cycle of delivered products.	2
7.2.7	Information received from **supply chain critical entities** that may impact resilience capabilities, planning, or status are promptly assessed, documented, and addressed (e.g., supplier's capability to provide enough support during a major event).	2
7.2.8	Identified supply chain risks are entered into the **risk register** or risk information database.	3
7.2.9	Selective acceptance testing evaluates the ability of key types of transmission and supporting equipment (e.g., bulk power transformers, EMS SCADA, protective relays, telecommunication equipment) to perform under the stress of a simulated range of resilience events (e.g., as considered in the TBU's design basis resilience events.)	3
7.2.10	The TBU has procedures in place for evaluating and engaging backup suppliers, as needed, to support a range of resilience events (e.g., as considered in the TBU's design basis resilience events.)	3

3. Manage the Needs of Electricity Subsector Critical Entities to Support Resilience

ID	Practice	MIL
7.3.1	The TBU is aware of the potential impacts it faces if **electricity subsector critical entities** (e.g., natural gas pipeline compressor stations, generating units) are unable to provide functions that the TBU relies upon during a resilience event, even if only in an ad hoc manner.	1
7.3.2	There is a documented process for the TBU to identify risk information that captures the impacts it faces if **electricity subsector critical entities** are unable to provide functions that the TBU relies upon during a resilience event.	2
7.3.3	Updated (on an organization-defined frequency) and documented policies or processes are implemented to address resilience risks to the TBU if **electricity subsector critical entities** are unable to provide functions that the TBU relies upon during a resilience event.	2
7.3.4	There is a documented process for the TBU to discuss interdependency risks and explore potential mitigations with entities that provide functions that meet the critical needs of the broader electricity subsector during a resilience event.	3
7.3.5	Identified risks from **electricity subsector critical entities** are entered into the **risk register** or risk information database.	3

4. Manage the Needs of Society Critical Entities to Support Resilience

ID	Practice	MIL

7.4.1	The TBU is aware of the potential impacts faced by society critical entities (e.g., medical services, defense facilities) in their service area if the resilient operation of the transmission system cannot be maintained, even if only in an ad hoc manner.	1
7.4.2	There is a documented process for the TBU to identify risk information that captures the impacts to society critical entities if the TBU's ability to transmit power is degraded during a resilience event.	2
7.4.3	Updated (on and organization-defined frequency) and documented policies or processes are implemented to address resilience risks to society critical entities.	2
7.4.4	Identified risks from society external entities are entered into the risk register or risk information database.	3

5. Management Support Activities

ID	Practice	MIL
7.5.1	Internal stakeholders for the TBU's supply chain and critical entities management activities are identified and involved, even if only in an ad hoc manner.	1
7.5.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support supply chain and critical entities management activities, even if only in an ad hoc manner.	1
7.5.3	Adequate resources (people, funding, training, and tools) are provided for resilience-related supply chain and critical entities management activities.	2
7.5.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development of resilience-related policies and procedures for risk identification, assessment, and management activities.	2
7.5.5	Responsibility and authority for the performance of resilience activities related to this domain are assigned to specific personnel.	2
7.5.6	Formal processes are used to incorporate resilience lessons learned into future plans for supply chain and critical entities management activities.	3
7.5.7	Leveraging research and development activities to support the deployment of new processes, tools, and technologies for resilience activities are supported by senior management.	3
7.5.8	Metrics exist to monitor, measure, and trend supply chain and critical entities management activities in order to track and improve resilience capabilities.	3

7.8 Transportation Management (TM)

Purpose: Establish and maintain transportation plans and capabilities for the timely delivery of personnel, assets, and fuel to where they are needed to both prepare for and respond to a transmission resilience event.

During an event that challenges transmission resilience, a key resilience activity involves the transportation of physical assets (e.g., transformers, transmission tower equipment, cranes, power lines, portable generators), personnel (e.g., lineman, drivers, crane operators), fuel (e.g.,

diesel, gasoline), and other critical infrastructure (e.g., electric power, water, lighting, shelter, food) to the locations where personnel and physical assets are needed to support restoration activities for electric power transmission. Plans for movement of assets and personnel are important because assets in storage yards and personnel stuck at home or in their offices cannot be used to restore service at remote location.

Assets, such as equipment, personnel, and fuel must be available where they are needed to perform their function. Transportation capabilities must be functional during the adverse conditions that are causing the resilience event or shortly after those conditions abate. This involves the need for transportation capabilities to operate during or in the aftermath of severe weather events (e.g., hurricanes, ice storms, tornadoes, snow storms), natural disasters (wildfires, earthquakes, geomagnetic events, floods), and human-caused events (e.g., cyberattacks, bombings, electromagnetic pulses (EMP)).

Transportation capabilities may involve a variety of transport methods including ground transportation (e.g., trucks, cars, trains), aircraft (e.g., jets, helicopters, drones), and watercraft (e.g., cargo vessels, barges, small boats). A range of personnel is needed to support the transportation and operation of equipment in the field. This includes drivers, loaders, and trained equipment operators. Fuel supplies and other critical infrastructure may not be readily available in the wake of a resilience event, adversely impacting transportation and transmission restoration activities. As a result, the transportation management program needs to involve the transportation of fuel and other critical assets.

The Transportation Management (TM) domain comprises two objectives:

1. Establish and maintain a transportation program
2. Management support activities

An effective transportation program establishes, maintains, and executes transportation capabilities for event response. This includes establishing appropriate relationships with business partners and suppliers to provide supplementary transportation capabilities when needed. Periodic exercises and drills can enhance the performance of transportation capabilities and identify areas for improvement, especially for more severe and nontraditional events.

The transportation program should address management of transportation resources, both internal and external, to provide adequate transportation capabilities. This includes assigning transportation roles and responsibilities, providing appropriate training to support transportation activities, and conducting periodic reviews to improve the program.

Example: Transportation Management

In planning for a resilience event, the transmission business unit (TBU) for Anywhere Utility Inc. (AUI) has developed and implemented a transportation program. The program documentation includes objectives for transporting fuel, assets, and people during resilience events. It also calls

for the transportation management program to incorporate lessons learned from real world events and exercises. TBU management is responsible for reviewing and updating the transportation management objectives at least once every three years (e.g., to account for changes in the TBU, operating environments, threat profiles).

AUI's TBU has created and implemented a detailed transportation plan for deploying assets, personnel, fuel, and other critical infrastructure to where they are needed before, during, and after the onset of an event that challenges transmission resilience. The plan supports the TBU in carrying out the timely transportation of replacement equipment, the personnel need operate that equipment, and the supplies needed to support this work.

Specifically, the plan includes:

- detailed roles and responsibilities of staff – including senior decision-makers, local managers, support staff, and contractors
- required resources necessary to support transportation planning and execution of the transportation plan for different types of resilience events
- requirements for personnel training in order to prepare for mobilization during an event
- equipment and contractual arrangements to support effective transportation capabilities during a resilience event
- provisions for transportation needs during longer-term events and for specialized transportation options
- provisions for acquiring alternative or additional transportation capabilities if needed.

The transportation plan is supported by a database containing AUI's transportation and logistics assets (e.g., vehicles, fuel) and those available from partners. The transportation database is reviewed and updated on at least a quarterly basis. In addition, transportation capabilities are tested during annual resilience drills/exercises; this includes participation by key transportation partners.

A recent improvement to the transportation plan includes provisions for types of resilience events that were not covered in earlier plans (e.g., events involving geomagnetic disturbances electromagnetic pulses (EMP), cyberattacks). AUI's transportation plan is updated every year to capture changes in potential resilience events and available resources.

Objectives and Practices

1. Establish and Maintain a Transportation Program

ID	Practice	MIL
8.1.1	Transportation resources (e.g., equipment, personnel, external partners) that are important to maintaining resilience and responding to a resilience event are identified even if only in an ad hoc manner.	1
8.1.2	The TBU is prepared to deploy its own and external partners' transportation resources during a resilience event, even if only in an ad hoc manner.	1
8.1.3	The documented transportation program addresses transporting resources (e.g., fuel, equipment, materials, supplies, people) that are important to maintaining resilience and responding to a resilience event and is updated at an organization-defined frequency.	2
8.1.4	The documented transportation program addresses longer-term (e.g., weeks to months) and larger impact (e.g., one or more FEMA areas) events.	2
8.1.5	The documented transportation program addresses the need for transporting large and heavy transmission equipment.	2
8.1.6	The documented transportation program addresses the need for contracts with key external partners that are important for responding in a timely manner to provide transportation-related services during a resilience event.	2
8.1.7	Redundancy requirements/alternate transportation capabilities that may be needed during a resilience event (e.g., when the fleet is damaged, there are fuel shortages, roads are closed) are documented.	2
8.1.8	Drills/exercises are conducted with internal and external parties to verify the documented transportation program addresses longer-term (e.g., weeks to months) and larger impact (e.g., one or more FEMA areas) events.	3
8.1.9	The documented transportation program addresses not only road and highway transportation options, but also specialized transportation options (e.g., rail, barge, air).	3
8.1.10	The documented transportation program is reviewed and updated to maintain effectiveness and leverage the latest technological advances (e.g., mobile equipment, drones).	3

2. Management Support Activities

ID	Practice	MIL
8.2.1	Internal stakeholders for transportation management activities are identified and involved, even if only in an ad hoc manner.	1
8.2.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support transportation management activities, even if only in an ad hoc manner.	1
8.2.3	Adequate resources (people, funding, training, and tools) are provided for resilience-related transportation management activities.	2
8.2.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) are consulted to support the development of resilience-related policies and procedures for transportation management activities.	2

ID	Practice	MIL
8.2.5	Responsibility and authority for the performance of resilience activities related to this domain are assigned to specific personnel.	2
8.2.6	Formal processes are used to incorporate resilience lessons learned into future plans for transportation management activities.	3
8.2.7	Leveraging research and development activities to support the deployment of new processes, tools, and technologies for resilience activities related to this Domain are supported by senior management.	3
8.2.8	Metrics exist to monitor, measure, and trend transportation management activities in order to track and improve resilience capabilities.	3

7.9 Workforce and Family Care Management (WFM)

Purpose: Raise resilience awareness in the workforce and prepare them to contribute during a resilience event by providing plans, training, tools, and peace of mind.

Workforce management for resilience events is critical to the successful restoration of the grid. Procedures should provide direction for workforce life cycle activities (e.g., hiring, security screening, transfer and termination practices), awareness and training, assignment of responsibilities, and family care plans.

The workforce must understand their roles. Adequate training on resilience processes and tools is necessary to prepare employees for their expected roles.

In addition, awareness activities are important to prepare the entire workforce for a resilience event. Planning should consider the full utilization of the workforce, for potentially extended periods of time, in roles that may be different from their traditional roles.

Planning should also recognize that resilience-related events may pose significant personal challenges for employees and their families. For employees to be fully engaged in the response to an event, they need assurances of the safety and well-being of their families. Assistance plans should be developed for impacted employees and their families. These should include defined processes that are established and communicated to employees.

In order to effectively manage a large workforce, a company must be able to communicate with the workforce. Efficient and robust methods are needed to communicate with the workforce. A workforce communication plan should be implemented, verified, and practiced under many scenarios.

The Workforce and Family Care Management (WFM) domain comprises six objectives:

1. Increase employee resilience awareness/create a culture of resilience
2. Assign resilience event responsibilities
3. Provide training to response and recovery personnel
4. Control the workforce life cycle

5. Develop, maintain, and execute family care plan
6. Management support activities

Example: Workforce and Family Care Management

The transmission business unit (TBU) for Anywhere Utility Inc. (AUI)recognizes that the availability and performance of its employees and contractors play a critical role in dealing with resilience events that can impact its transmission system. AUI has a long history of dealing with the severe weather events that periodically impact its service area. AUI has developed and implemented practices during these severe weather events to ensure that it has adequate workforce resources identified, trained, and in place to meet historical resilience needs. Several years ago, TBU expanded and updated its workforce management program to better support longer-term, more widespread, and nontraditional resilience events.

The TBU's current workforce management plan has multiple components. The plan lays out workforce roles and responsibilities. Both primary and backup roles are assigned for key resilience responsibilities to ensure adequacy and redundancy of coverage. The plan calls for maintaining a workforce with the appropriate skills to support the resilience program. This starts with activities designed to enhance workforce awareness of resilience events through the use of periodic briefings and other communications. Mandatory training prepares the workforce to efficiently perform their resilience duties. Resilience event knowledge, skill, and ability gaps are identified. Identified resilience event knowledge gaps are addressed through recruiting and/or training.

The workforce management plan includes guidance for obtaining supplementary workforce support from contractors and industry partners (e.g., those located outside of the affected area). The implications for the resilience program are considered as part of the decision-making process for worker assignments, transfers, and succession planning. New employees and contractor staff are subject to security vetting commensurate with the sensitivity of their potential assignments.

The newest component of the workforce management plan is the development and implementation of procedures to ensure the safety and security of workers' families during resilience events. This includes provisions for basic support for the workforce's families during emergencies and the establishment and maintenance of reliable communication channels between workforce members and their families. This family care plan is integral in maintaining the willingness of employees to report to work and providing peace of mind that loved ones are safe and cared for. Providing peace of mind to employees is an extension of safety since it enables performance of assigned tasks with the best frame of mind during difficult times.

Procedures are in place to ensure adequate resources are available to support the logistical requirements of the workforce over the range of potential resilience events.

Objectives and Practices

1. Increase Employee Resilience Awareness/Create a Culture of Resilience

ID	Practice	MIL
9.1.1	Resilience awareness activities (e.g., discussions among staff or participation in industry resilience activities) are conducted to build a culture of resilience, even if only in an ad hoc manner.	1
9.1.2	Personnel leading awareness activities have some resilience expertise, even if acquired in an ad hoc manner.	1
9.1.3	There is a culture of resilience awareness and preparedness (i.e., the importance of resilience and preparedness is consistently acknowledged and communicated by management.)	2
9.1.4	Objectives for and content of resilience awareness activities are documented and updated on an organization-defined frequency.	2
9.1.5	Resilience awareness activities are conducted for all TBU positions (including employees and contractor personnel) on an organization-defined frequency.	2
9.1.6	Resilience principles are incorporated into everyday practices.	3
9.1.7	The effectiveness of resilience awareness activities is evaluated on an organization-defined frequency.	3

2. Assign Resilience Event Responsibilities

ID	Practice	MIL
9.2.1	Resilience event responsibilities are identified, even if only in an ad hoc manner.	1
9.2.2	Resilience event responsibilities are documented (e.g., in position/job descriptions, management directives).	2
9.2.3	Resilience event responsibilities are assigned to applicable personnel, which includes employees as well as contract personnel who have responsibilities during an event.	2
9.2.4	Resilience event responsibilities address the responsibilities for both primary response and recovery and support response and recovery personnel that may have roles during an event.	2
9.2.5	Both primary and backup roles are assigned for key response and recovery activities during an event.	2
9.2.6	Resilience event responsibilities are reviewed and updated on an organization-defined frequency.	2
9.2.7	Resilience event responsibilities are included in TBU job performance evaluation criteria.	3

3. Provide Training to Response and Recovery Personnel

ID	Practice	MIL
9.3.1	Training on resilience roles and responsibilities is provided to response and recovery personnel, at least in an ad hoc manner (e.g., self-guided study, reading resilience-related articles, participation on industry resilience groups).	1
9.3.2	The TBU's training plan for resilience-related activities is documented and updated at an organization-defined frequency.	2

ID	Practice	MIL
9.3.3	The documented training plan for resilience-related activities establishes training requirements based on the specific roles and responsibilities assigned to personnel.	2
9.3.4	The documented training plan addresses severe (longer and larger impact) events and the necessary skills of response and recovery personnel to address these events.	2
9.3.5	Resilience event knowledge, skill, and ability gaps are identified and addressed through training or talent acquisition.	2
9.3.6	Resilience training content is based on the full spectrum of identified risks to transmission resilience (e.g., considering both historical and nontraditional events as may be documented in the TBU's design basis resilience events).	3
9.3.7	The effectiveness of resilience training activities is evaluated for improvements at an organization-defined frequency.	3
9.3.8	Improvements are made to the resilience training program based on a formal process to include lessons learned and the latest information and technologies.	3

4. Control the Workforce Life Cycle

ID	Practice	MIL
9.4.1	Personnel security screening (e.g., a background check) is performed at hire, even if only in an ad hoc manner.	1
9.4.2	Formal personnel security screening (e.g., a background check, drug testing) is performed following documented procedures for prospective hires to positions that have access to resilience-related assets or perform key resilience responsibilities.	2
9.4.3	Personnel transfer and termination policies address potential security concerns.	2
9.4.4	Personnel transfer and termination policies address continuity for performing key resilience responsibilities.	2
9.4.5	Personnel security screening is reassessed at an organization-defined frequency for positions that have access to key resilience-related assets or perform key resilience responsibilities.	2
9.4.6	All employees that have access to resilience-related assets or processes are categorized to indicate criticality to resilient operations (e.g., no or minimal impact, significant impact, critical impact).	2
9.4.7	All contract personnel that have access to resilience-related assets or processes are categorized to indicate criticality to resilient operations (e.g., no or minimal impact, significant impact, critical impact).	2
9.4.8	Personnel security screening is reassessed for all employees at a level and periodicity consistent with the position's criticality categorization.	2
9.4.9	Personnel security screening is assured for contract personnel through proper vetting and contractual arrangements at a level and periodicity consistent with the position's criticality categorization.	3
9.4.10	The criticality categorization of personnel's resilience skills and responsibilities is an input to workforce and succession planning.	3
9.4.11	Recruiting and retention are aligned to support resilience workforce management goals.	3
9.4.12	A formal and multifaceted insider threat program has been implemented to detect and protect against insider threats.	3

5. Develop, Maintain, and Execute Family Care Plan

ID	Practice	MIL
9.5.1	The TBU is prepared to perform family care activities during resilience events (e.g., take steps to ensure the safety and security of staff members' families to encourage staff members to report to work and focus on their jobs), even if only in an ad hoc manner.	1
9.5.2	Family care plan is documented and updated on an organization-defined frequency.	2
9.5.3	The documented family care plan includes provisions for effective communications with employees' families during and after resilience events.	2
9.5.4	The documented family care plan includes a list of essential needs for employees' families during and after resilience events.	2
9.5.5	The documented family care plan includes active "life assistance" support for employees' families during and after longer duration, larger impact events (e.g., family emergency center, safe zones, food and water delivery, pet care).	3
9.5.6	The documented family care plan includes psychological support for employees' families during and after extended resilience events.	3

6. Management Support Activities

ID	Practice	MIL
9.6.1	Internal stakeholders for workforce and family care management activities are identified and involved, even if only in an ad hoc manner.	1
9.6.2	Resilience resource needs (people, funding, training, tools) have been identified (although not necessarily allocated) to support workforce and family care management activities, even if only in an ad hoc manner.	1
9.6.3	Adequate resources (people, funding, training, and tools) are provided for resilience-related workforce and family care management activities.	2
9.6.4	External sources (e.g., international, national, or industry standards/guidance documents; good utility practices) consulted to support the development of resilience-related policies and procedures for workforce and family care management activities.	2
9.6.5	Responsibility and authority for the performance of resilience activities for this domain are assigned to specific personnel.	2
9.6.6	Formal processes are used to incorporate resilience lessons learned into future plans for workforce and family care management activities.	3
9.6.7	Leveraging research and development activities to support the deployment of new processes, tools, and technologies for resilience activities related to this Domain are supported by senior management.	3
9.6.8	Metrics exist to monitor, measure, and trend workforce and family care management activities in order to track and improve resilience capabilities.	3

APPENDIX A: BIBLIOGRAPHY & REFERENCES

The table below indicates the applicability of the references (left-hand column) to the various TRMM domain topics (right-hand columns). References that inform more broadly have no marker in the TRMM Domains columns. Items included as references below either served as resources in the development of the TRMM and/or may serve as resources for the user in applying the TRMM. Publicly available references have a link included; other references are included for awareness and can be accessed by contacting the owner, with certain fees applicable.

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
[CEII] Federal Energy Regulatory Commission. (2010). *Critical energy infrastructure information (CEII) regulations*. http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp									
[CERT RMM] Caralli, R. A., Allen, J. H., & White, D. W. (2011). *CERT resilience management model: A maturity model for managing operational resilience* (CERT-RMM Version 1.1). Boston, MA: Addison-Wesley.									
[Climate Resilience Toolkit] National Oceanic and Atmospheric Association (NOAA). (2019). *U.S. Climate Resilience Toolkit.* https://toolkit.climate.gov/									
[DHS CISA/Dept. of State Security and Resiliency Guide] Department of Homeland Security, in collaboration with the U.S. Department of State. (2019, November). *A Guide to Critical Infrastructure Security and Resilience*. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf									
[DOE Climate Change Resilience Planning] Department of Energy. (2016). *Climate Change and the Electricity Sector: Guide for Climate Change Resilience Planning.* https://www.energy.gov/sites/prod/files/2016/10/f33/Climate%20Change%20and%20the%20Electricity%20Sector%20Guide%20for%20Climate%20Change%20Resilience%20Planning%20September%202016_0.pdf									
[DOE NAERM] Department of Energy. (2019). *North American Energy Resilience Model (NAERM).* https://www.energy.gov/sites/prod/files/2019/07/f65/NAERM_Report_public_version_072219_508.pdf									
[DOE RMP] Department of Energy. (2012). *Electricity subsector cybersecurity risk management process.*									

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
[DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity] Energy Sector Control Systems Working Group. (2011). *Roadmap to achieve energy delivery systems cybersecurity.* https://www.energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf									
[EOPUS Policy Framework] Executive Office of the President of the United States. (2011). *A policy framework for the 21st Century grid: Enabling our secure energy future.* https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nstc-smart-grid-june2011.pdf									
[EPRI EMP Grid Resiliency] Electric Power Research Institute. (2016). *Electromagnetic Pulse (EMP) Grid Resiliency: Transmission Vulnerability and Mitigation.* https://www.epri.com/#/pages/product/3002007463/									
[EPRI Overhead Line Hardening] Electric Power Research Institute. (2018). *Practical Overhead Line Hardening Techniques: Enhancing Structural Resiliency of Transmission Lines.* https://www.epri.com/#/pages/product/3002012644/									
[EPRI Resiliency Metrics and Analytical Frameworks] Electric Power Research Institute. (2018). *Technical Assessment of Resiliency Metrics and Analytical Frameworks.* https://www.epri.com/#/pages/product/3002014571/									
[EPRI Resiliency White Paper] Electric Power Research Institute. (2016). Electric Power System Resiliency: Challenges and Opportunities. https://www.epri.com/#/pages/product/3002007376/									
[EPRI Risk Analysis in Transmission Planning] Electric Power Research Institute. (2018). *Incorporating Risk Analysis into Transmission Planning.* https://www.epri.com/#/pages/product/3002010916/		✓							
[EPRI Transmission Resiliency Decision Support Framework] Electric Power Research Institute. (2019). *Transmission Resiliency Decision Support Framework.* https://www.epri.com/#/pages/product/3002016914/									
[EPRI Transmission Resiliency Research] Electric Power Research Institute. (2015). *How the Transmission Resiliency Research Fits Together.* https://www.epri.com/#/pages/product/3002006429/									
[ES-C2M2] Department of Energy (2014). *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).* https://www.energy.gov/oe/downloads/electricity-subsector-cybersecurity-									

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
capability-maturity-model-v-11-february-2014									
[ES-ISAC] Electricity Sector Information Sharing and Analysis Center. (2019). [Home page] https://www.eisac.com/			✓						
[ES-SPP] U.S. Department of Homeland Security and U.S. Department of Energy. (2010). *Energy sector-specific plan: An annex to the national infrastructure protection plan.* https://www.hsdl.org/?view&did=7902									
[GridWise Alliance] GridWise Alliance. (2013). *Improving Electric Grid Reliability and Resilience: Lessons Learned from Superstorm Sandy and Other Extreme Events.* https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/improvingelectricgridreliabilityandresilienceintheusa.htm#tab_description									
[ICS] Federal Emergency Management Agency (FEMA). (2017). *Incident Command System (ICS) Resource Center.* https://training.fema.gov/EMIWeb/IS/ICSResource/index.htm				✓					
[ISACs] National Council of Information Sharing and Analysis Centers (ISACs). (2019). [Home page]. https://www.nationalisacs.org/			✓						
[ISO/IEC 21827:2008] International Organization for Standardization. (2008). *Systems Security Engineering – Capability Maturity Model (SSE-CMM)* (ISO/IEC 21827:2008).									
[ISO 22320:2018] International Organization for Standardization. (2018). *Security and resilience – Emergency management – Guidelines for incident management.* https://www.iso.org/standard/67851.html				✓					
[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).							✓		

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
[NATF BES Monitoring and Control] North American Transmission Forum (NATF). (2016). *Bulk Energy System Monitoring and Control – A Review of Backup Capabilities.* https://www.natf.net/docs/natf/documents/resources/resiliency/natf-bes-monitoring-and-control---overview-of-backup-capabilities.pdf				✓		✓			
[NATF Conservative Operations and Emergency Tools Practices] North American Transmission Forum (NATF). (2018). *Emergency tools to alleviate emergency conditions and maintain reliability.*				✓					
[NATF RAICC Maturity Tool] North American Transmission Forum (NATF). (2017). Risk Assessment, Internal Controls, and Compliance Self-Assessment Tool. *Guidance and mechanism for evaluating RAICC maturity.*		✓							
[NATF Resilience and Transmission Planning] North American Transmission Forum (NATF). (2020). Resilience and Transmission Planning Reference Document.									
[NATF RESTORE] Overview of NATF's Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) Program https://www.natf.net/docs/natf/documents/natf-restore-program-overview.pdf					✓				
[NATF SOS] North American Transmission Forum (NATF). (2019). *Supplemental Operating Strategies and Resiliency Practices*				✓					
[NATF Supply Chain CIP-013-1] North American Transmission Forum (NATF). (2019). *NATF CIP-013-1 Implementation Guidance.* https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-cyber-security-supply-chain-risk-management-guidance.pdf							✓		
[NATF Supply Chain Assessment Model] North American Transmission Forum (NATF). (2020). *Supplier Cyber Security Assessment Model* https://www.natf.net/docs/natf/documents/resources/supply-chain/supplier-cyber-security-assessment-model.pdf							✓		
[NATF Supply Chain Home Page] North American Transmission Forum (NATF). *Supply Chain Cyber Security Industry Coordination (public webpage)* https://www.natf.net/industry-initiatives/supply-chain-industry-coordination							✓		
[NATF Spare Tire] North American Transmission Forum (NATF). (2017). *Bulk Electric Systems Operations Absent Emergency Management System and Supervisory Control and Data Acquisition Capabilities (SCADA) – a Spare*				✓					

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
Tire Approach. https://www.natf.net/docs/natf/documents/resources/resiliency/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf									
[NATF Transmission System Resiliency] North American Transmission Forum (NATF). (2017). *Transmission System Resiliency – An Overview.* https://www.natf.net/docs/natf/documents/resources/resiliency/transmission-system-resiliency-an-overview.pdf									
[NERC ALR] North American Electric Reliability Corporation (NERC). (n.d). *Definition: Adequate Level of Reliability (ALR) for the Bulk Electric System.* https://www.nerc.com/comm/Other/Adequate%20Level%20of%20Reliability%20Task%20Force%20%20ALRTF%20DL/Final%20Documents%20Posted%20for%20Stakeholders%20and%20Board%20of%20Trustee%20Review/2013_03_26_ALR_Definition_clean.pdf									
[NERC Event Analysis Reports] North American Electric Reliability Corporation (2003-2018). *Major Event Analysis Reports.* Reports available for various major events (e.g., blackouts, cold weather, hurricane, wildfires) from 2003 to 2018. https://www.nerc.com/pa/rrm/ea/Pages/Major-Event-Reports.aspx.									
[NERC Reliability Standards] North American Electric Reliability Corporation (2019). *Reliability Standards for the Bulk Electric Systems of North America.* https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf									
[NERC RISC] North American Electric Reliability Corporation Report on Resilience (NERC RISC). (2018). *Report on Resilience.* https://www.nerc.com/comm/RISC/Related%2520Files%2520DL/RISC%2520Resilience%2520Report_Approved_RISC_Committee_November_8_2018_Board_Accepted.pdf									
[NIAC Critical Infrastructure Resilience] National Infrastructure Advisory Council. (2009). *National Infrastructure Advisory Council Critical Infrastructure Resilience: Final Report and Recommendations.* https://www.dhs.gov/publication/niac-critical-infrastructure-resilience-final-report									
[NIAC Resilience Framework] National Infrastructure Advisory Council. (2010). *A Framework for Establishing Critical Infrastructure Resilience Goals.* https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf									

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
[NIMS Framework] Federal Emergency Management Agency. (2019). *National Incident Management System (NIMS) Doctrine Supporting Guides and Tools.* https://www.fema.gov/nims-doctrine-supporting-guides-tools				✓					
[NIST SP800-16] Wilson, M., Stine, K., & Bowen, P. (2009). *Information security training requirements: A role- and performance-based model* (NIST Special Publication 800-16, revision 1.0). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf									
[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. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf									✓
[NIST SP800-53] National Institute of Standards and Technology, Joint Task Force Transformation Initiative. (2009). *Recommended security controls for federal information systems and organizations* (NIST Special Publication 800-53, revision 3). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf						✓			
[OE-417] U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability. (2011). *The electric emergency incident and disturbance report* (Form OE-417). https://www.oe.netl.doe.gov/oe417.aspx			✓						
[PPD 21] Obama Administration. (2013). *Presidential Policy Directive – Critical Infrastructure Security and Resilience.* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil									
[Sandia RAP Metrics] Watson, J., Guttromson, R., Silva-Monroy, C., Jeffers, R., Jones, K., Ellison, J., Rath, C., Gearhart, J., Jones, D., Corbet, T., Hanley, C., & Walker, L. (2014). *Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States.* https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/EnergyResilienceReportSAND2014-18019o.pdf									

References	TRMM Domains								
	PM	RM	SA	ERR	EqM	ISC	SCE	TM	WFM
[TRMM Facilitator Guide] Transmission Resilience Maturity Model Facilitator Guide. 2020. Found at https://trmm.labworks.org/resources.									
[TRMM Supplementary Explanations] Transmission Resilience Maturity Model Help Guide. 2020. Found at https://trmm.labworks.org/resources.									
[TRMM Home Page] Transmission Resilience Maturity Model Home Page. *Links to the TRMM Tool, supporting documentation, and contact information can be found at* https://trmm.labworks.org									

APPENDIX B: GLOSSARY

Term	Definition	Source
ad hoc	In the context of this model, *ad hoc* (i.e., an ad hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training. The methods, tools, and techniques used, the priority given a particular instance of the practice, and the quality of the outcome may vary significantly depending on who is performing the practice, when it is performed, and the context of the problem being addressed. With experienced and talented personnel, high-quality outcomes may be achieved even though practices are ad hoc. However, because lessons learned are typically not captured at the organizational level, approaches and outcomes are difficult to repeat or improve across the organization.	ES-C2M2
asset *(specific to Transmission and Supporting Equipment Management Domain)*	Something of value to the organization. Assets may include many things including equipment, tools, software, computer hardware, databases, and facilities. For the purposes of the EqM domain, assets to be considered are: • transmission system equipment (e.g., transformers, poles, relays) • transmission support equipment (e.g., tools for repairing transmission system equipment, vehicles for transporting materials and personnel, tools for system analyses, monitoring, and managing restoration processes)	TRMM
Bulk Electric System	Unless modified by specified "inclusions" and "exclusions," all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.	Adapted from NERC Glossary of Terms Used in NERC Reliability Standards
Bulk Power System	facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. (Note that the terms "Bulk-Power System" or "Bulk Power System" shall have the same meaning.)	NERC Glossary of Terms Used in NERC Reliability Standards

Term	Definition	Source
common operating picture (COP)	A single identical display of relevant information shared by all affected groups. A COP facilitates collaborative planning and assists all groups to achieve situational awareness. The COP aggregates information from multiple topical areas such as cyber, physical, telecommunications, and operations that provides situational awareness. The COP leverages various technologies to collect, analyze, alarm, present, and use the aggregated information for timely TBU decision-making and actions.	Adapted from US DOD
communication partners	Relevant parties to which the TBU communicates important and pertinent information before, during, and after a resilience event. Partners may be either internal or external: • Internal partners are pertinent parties within an organization or enterprise • External partners may include electric, gas, telecommunications, water utilities and critical end users; vendors; local, state and federal governments (including both elected officials and first responders); meteorological organizations; the news media; and the general public.	
consequence	Something produced by a cause or necessarily following from a set of conditions; in terms of risk, consequences are determined by looking at the potential threats in combination with the organization's vulnerabilities. Once the scope of consequences is known, the organization's risk can be ranked by severity of impact.	Adapted from Merriam-Webster

Term	Definition	Source
critical entities *(specific to Supply Chain and Critical Entities Domain)*	Critical entities fall into one or more of the following categories: 1. Supply chain critical entities: Entities that have a contract with the TBU/enterprise to deliver products or services to allow the TBU/enterprise to conduct business. • Equipment providers (e.g., breaker manufacturer) • Key service providers to the TBU (e.g., telecom) 2. Electricity subsector critical entities: Entities who are not supply chain entities and provide essential products or services to the electricity subsector **AND** whose electricity is provided either directly from the TBU or indirectly from the TBU (e.g., through a distribution utility that is reliant on the TBU for power). • Examples include natural gas compressor stations, generators. 3. Society critical entities: Entities who are not supply chain or electricity subsector critical entities and provide essential products or services to the society at large **AND** whose electricity is provided either directly from the TBU or indirectly from the TBU (e.g., through a distribution utility that is reliant on the TBU for power). • Examples include telecommunication nodes, defense and military facilities, water pumping stations, hospitals and medical centers.	TRMM
critical infrastructure	Assets that provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction through terrorist attack could have a debilitating effect on security and economic well-being. https://www.cisa.gov/critical-infrastructure-sectors	HSPD-7

Term	Definition	Source
design basis resilience event	Postulated, reasonable, worst-case resilience events used to establish the parameters to which a TBU will design and plan its system resilience capabilities. Designs and plans will include capabilities to withstand events, continue transmission system operations or quickly bounce back from events, and minimize the risk to the health and safety of society at large. These resilience events should be of sufficient magnitude such as: 1) duration counted in weeks or months versus days and 2) geographic impacts on the order of FEMA areas or large Regional Entities versus a TBU's service territory plus adjacent neighbors. Reference section 4.4 for a detailed discussion of design basis resilience events.	TRMM
disposition	A statement of the organization's intention for addressing an item, e.g., risks, threats. Typical dispositions include "accept," "transfer," "research," or "mitigate."	TRMM
domain	In the context of the model structure, a domain is a logical grouping of transmission resilience practices.	TRMM
drills/exercises	Exercising plans, policies, procedures, and staff members involved in management, direction, command, and control functions. In comparison to a full-scale exercise, a functional exercise involves fewer participants and the movement of personnel and equipment is simulated.	FEMA
domain objectives	The practices within each domain are organized into *objectives*. The objectives represent achievements that support the domain (such as "Perform Monitoring" for the Situational Awareness domain and "Manage/Maintain Communications Tools" for the Information Sharing and Communications domain). Each of the objectives in a domain comprises a set of practices, which are ordered by maturity indicator level.	TRMM
electricity sector information sharing and analysis center (ES-ISAC)	The Electricity Sector Information Sharing and Analysis Center (ES-ISAC) shares critical information with industry participants about infrastructure protection. The ES-ISAC serves the electricity sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, vulnerabilities, analyses, and warnings, together with interpretations, to help electricity sector participants take protective actions. *See Information Sharing and Analysis Center (ISAC).*	Adapted from Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website home page
electricity subsector	A portion of the energy sector that includes the generation, transmission, and distribution of electricity.	ES-SPP

Term	Definition	Source
enterprise	The largest (i.e., highest-level) organizational entity to which the organization participating in the TRMM survey belongs. See *organization.*	Adapted from SGMM v1.1 Glossary
establish and maintain	The development and maintenance of the object of the practice (such as a program). For example, "Establish and maintain identities" means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements.	CERT RMM
event	Any observable occurrence on the system or supporting networks that may have adverse impact to the transmission system and require action to resolve. To ensure consistency, criteria for response should align with the organization's risk criteria. For the purposes of this model, event may be used interchangeably with incident (as in incident response).	TRMM
event response and recovery (ERR)	TRMM domain with the purpose to establish, maintain, and exercise plans, procedures, and technologies to respond to and recover from events impacting transmission business unit (TBU) resilience, commensurate with the resilience objectives and risks to the transmission infrastructure.	TRMM
fuel assurance	Proactively taking steps to identify fuel arrangements or other alternatives that would provide confidence such that fuel interruptions are minimized to maintain reliable Bulk Power System (BPS) performance during both normal operations and credible disruptive events	NERC Reliability Guideline: Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System (March 2020)
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 (SME) and community consensus, or internally by an organization. Guidelines are typically less detailed than standards and with less stringent enforcement.	ES-C2M2
impact	Negative consequence to the electric transmission system.	TRMM

Term	Definition	Source
Incident Command System	The Incident Command System (ICS) is a management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.	FEMA
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. See *Electricity Sector Information Sharing and Analysis Center (ES-ISAC).*	Adapted from Electricity Sector Information Sharing and Analysis Center (ES-ISAC) website home page
information sharing and communications (ISC)	The TRMM domain with the purpose to establish and maintain relationships, procedures, and capabilities (both voice and data) with internal and external entities to collect and provide resilience information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with resilience objectives and risks to transmission infrastructure.	TRMM
interdependency risk	The risk due to a mutually dependent relationship, e.g., gas pipelines and the Bulk Electric System (BES) are interdependent due to the reliability of the BES being reliant, in part, on gas generation and because electricity is a necessity throughout the natural gas supply chain, including at production, pipeline, processing, and distribution facilities.	TRMM
markets	Venues where participants buy and sell products and services. In the context of this model, *markets* refers to trading involving wholesale electricity.	FERC
maturity	The extent to which an organization has implemented and institutionalized the transmission resilience practices of the model.	TRMM

Term	Definition	Source
maturity indicator level (MIL)	A measure of the transmission resilience maturity of an organization in a given domain of the model. The model currently defines four maturity indicator levels (MILs) and holds a fifth level in reserve for use in future versions of the model. Each of the four defined levels is designated by a number (0 through 3) and a name, for example, "MIL3: managed." A MIL is a measure of the progression within a domain from individual and team initiative, as a basis for carrying out transmission resilience practices, to organizational policies, plans, processes, and procedures that institutionalize those practices, making them repeatable with a consistently high level of quality. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the core activities in the domain.	TRMM
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)
mutual assistance	Agreements between agencies, organizations, and jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and after an incident. A signed agreement does not obligate the provision or receipt of aid, but rather provides a tool for use should the incident dictate a need.	FEMA
objective(s)	*See domain objectives* and *organizational objectives*.	
operational resilience	The organization's ability to adapt to risk that affects its core operational capacities. See the related term *operational risk*.	CERT RMM
operational risk	The potential impact on assets that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events. In the context of this model, our focus is on operational risk from transmission resilience threats.	Adapted from CERT RMM
organization	An organization of any size, complexity, or positioning within an organizational structure that is charged with carrying out assigned mission and business processes. In the context of the model, the organization is the entity using the model or that is under examination.	Adapted from DOE RMP

Term	Definition	Source
organization-defined frequency	This term is used throughout the model to indicate routine reviews and updates of documentation, databases, policies, processes, etc. on a frequency determined by the organization to be most appropriate to update, grow, and adapt content.	TRMM
organizational objectives	Performance targets set by an organization. See *strategic objectives*.	Adapted from CERT RMM
plan	Course of action for an organization in order to meet objectives; a plan informs the more detailed processes and procedures	TRMM
policy	A statement of position or intent, based upon a set of guidelines, rules, standards adopted by an organization for rational decision-making in order to meet objectives. Policies inform strategies.	TRMM
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 transmission resilience.	TRMM
primary response and recovery personnel	Personnel essential to key response and recovery activities; these specialized workers have specific knowledge from experience and training and may hold specialized licensing/certifications relevant to restoring and maintaining the transmission system and its supporting systems. Examples include control room operators, reliability engineers, field personnel.	TRMM
procedure	Step by step list of actions needed to complete a task or mission. A procedure is a prescribed way of undertaking a process or part of a process	TRMM
process	A set of main elements that contribute to the fulfillment of a task or mission. A process defines the big picture and highlights main elements (i.e., breadth.) A procedure captures those main elements and adds more information for functional responsibilities, objectives, methods and sequencing (i.e., depth.)	TRMM
resilience	For extreme and long-lived events: The ability [of the electric system] to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event.	FERC Grid Resilience Order (01/08/2018)
resilience program management (PM)	The TRMM domain with the purpose to establish and maintain a transmission business unit (TBU) resilience program that provides governance, overall program strategy, direction and sponsorship for the TBU's resilience activities. The PM aligns resilience objectives with the TBU's and enterprise's strategic objectives and the risk to infrastructure.	TRMM

Term	Definition	Source
risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.	DOE RMP
risk analysis	A risk management activity focused on understanding the condition and potential consequences of risk, prioritizing risks, and determining a path for addressing risks. Determines the importance of each identified risk and is used to facilitate the organization's response to the risk.	Adapted from CERT RMM
risk assessment	The process of identifying risks to organizational operations, facilities, or resources.	TRMM
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.	ES-C2M2
risk designation, as in "position risk designation"	An indication, such as high, medium, or low, of the position's potential for adverse impact to the efficiency, integrity, or availability of the organization's services.	Adapted from OPM
risk management program	The program and supporting processes to manage transmission resilience risk to organizational operations, facilities, or resources. 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.	Adapted from DOE RMP
risk identification, assessment, and management (RM)	The TRMM domain with the purpose to establish, operate, and maintain a resilience risk management program to identify, analyze, prioritize, select, develop, and implement actions to address resilience risks.	TRMM
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	The steps taken to reduce adverse effects to the enterprise. There are four types of risk mitigation strategies: risk acceptance, avoidance, transfer, and reduction. With the resilience operation of the transmission system a priority, options typically narrow to reducing the risk or accepting the risk that is too difficult or expensive to reduce.	TRMM
risk register	A structured repository where identified risks are recorded to support risk management. Documents key risks and what is known about the risk (severity, breadth, length of time).	TRMM

Term	Definition	Source
sector/subsector	refers to the critical infrastructure sectors and their sub-parts (subsectors); refer to https://www.cisa.gov/critical-infrastructure-sectors; e.g., energy is one sector, of which electricity is one subsector; cross sector or cross subsector would imply things that apply across multiple sectors or subsectors	TRMM
senior management	Transmission Business Unit (TBU) head executive (e.g., chief transmission officer) and their direct reports, and other comparable functions such as chief security officer or chief information officer and direct reports for topics/functions handled beyond the TBU	TRMM
situational awareness	A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system, in the context of the threat environment and risks to the system's mission, to support effective decision-making with respect to activities that depend on and/or affect how well a system functions. It involves the collection of data (e.g., via sensor networks), data fusion, and data analysis (which may include modeling and simulation) to support automated and/or human decision-making (for example, concerning power system functions). Situational awareness also involves the presentation of the results of the data analysis in a form (e.g., using data visualization techniques, appropriate use of alarms) that aids human comprehension and allows operators or other personnel to quickly grasp the key elements needed for good decision-making.	Adapted from SGMM Glossary
situational awareness (SA)	The TRMM domain with the purpose to establish and maintain activities to monitor, analyze, and communicate information in a common operating picture (COP), commensurate with the resilience objectives and risks to the transmission infrastructure. The Time Horizon covered by this domain is Operations Planning and Real-time Operations, i.e., the timeframe where the transmission business unit (TBU) must be aware of threats in order to adjust and implement mitigating strategies, but not far enough in advance to build or harden. Those Long-term Planning actions are covered under the Risk Identification, Assessment, and Management domain.	TRMM
sponsorship	Transmission business unit (TBU) and enterprise-wide support of transmission resilience objectives by senior management as demonstrated by formal policy or by declarations of management's commitment to the transmission resilience program along with provision of resources. Senior management monitors the performance and execution of the transmission resilience program and is actively involved in the ongoing improvement of all aspects of the transmission resilience program.	TRMM

Term	Definition	Source
stakeholder	An external organization or an internal or external person or group that has a vested interest in the transmission business unit (TBU) that is being evaluated using this model and its practices. Stakeholders involved in performing a given practice (or who oversee, benefit from, or are dependent upon the quality with which the practice is performed) could include those from within the TBU, from across the organization, or from outside the organization.	Adapted from CERT RMM
standard	A standard is a document, established by consensus, that provides rules, guidelines, or characteristics for activities or their results. For the purpose of this model, examples include NERC Reliability Standards, IEEE standards, internal company standards, etc.	Adapted from ISO/IEC Guide
strategic objectives	The performance targets that the organization sets to accomplish its mission, vision, values, and purpose.	CERT RMM
strategy	Strategy is a high-level plan of action, while policy is a principle of action. Strategy generally involves setting goals and priorities, determining actions to achieve the goals, and mobilizing resources to execute the actions. For purposes of this model, the hierarchy/relationships would be: The policy informs the strategy; the strategy is at a higher level than a plan (detailed formulation of a program of action). Processes and procedures are even more detailed – refer to their definitions herein.	TRMM
Superior Practice (NATF)	A leading industry practice that can be consistently applied under a range of circumstances and that is a safe, effective, and efficient process or activity for achieving near-optimal industry results in terms of quality, reliability, and maintainability.	NATF Practices documents
supply chain	The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. The supply chain encompasses the full product life cycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain.	NISTIR 7622 Source of 1st paragraph cited as [NDIA ESA]
supply chain and critical entities management (SCE)	The TRMM domain with the purpose to establish and maintain relationships with suppliers and other key resources needed to respond to a transmission resilience event commensurate with resilience objectives and the risk to the transmission infrastructure (e.g., establishing mutual aid agreements, managing key vendor and customer relations, establishing spare equipment sharing arrangements)	TRMM

Term	Definition	Source
support response and recovery personnel	Personnel essential to supporting response and recovery activities; these workers fill essential, but not specialized roles in response and recovery activities. Examples include food runners, call center agents.	TRMM
threat	Any circumstance or event with the potential to adversely impact organizational operations or critical facilities	TRMM
threat assessment	The process of evaluating the severity of threat to an organization and describing the nature of the threat.	Adapted from DOE RMP
threat profile	A characterization of the likely intent, capability, and targets for threats. It is the result of one or more threat assessments across the range of feasible threats to the TBU or enterprise, delineating the feasible threats, describing the nature of the threats, and evaluating their severity.	TRMM
transmission	The movement or transfer of electric energy over an interconnected group of lines and associated equipment between points of supply and points at which it is transformed for delivery to consumers or is delivered to other electric systems. Transmission is considered to end when the energy is transformed for distribution to the consumer.	EIA Glossary
transmission business unit (TBU)	Refers to the transmission portion of an entity's corporate business. For purposes of the TRMM model, it limits the scope of resilience measures to transmission functions only where TBU is indicated.	TRMM
transmission and supporting equipment management (EqM)	The TRMM domain with the purpose to identify and manage assets used to detect, identify, analyze, prepare for, respond to, and recover from resilience threats and events. For the purposes of this model, assets to be considered are equipment, tools, and resources, as well as essential operating information including tools, equipment, databases, etc.	TRMM
transmission infrastructure	Assets (lines, substations, towers, poles, control houses, etc.) that are integral in delivering energy from sources (e.g., generators) to loads. Portions of transmission infrastructure would be deemed critical infrastructure.	TRMM
transportation management (TM)	The TRMM domain with the purpose to establish and maintain transportation plans and capabilities for the timely delivery of personnel, assets, and fuel to where they are needed to both prepare for and respond to a transmission resilience event.	TRMM
vulnerability	A transmission resilience vulnerability is a weakness or flaw in transmission operations, facilities, or tools.	Adapted from NISTIR 7628 Vol. 1, pp. 8

Term	Definition	Source
workforce life cycle	For the purpose of this model, the *workforce life cycle* comprises the distinct phases of workforce management that apply to personnel both internal and external to the organization. The workforce life cycle includes recruiting, hiring, onboarding, skill assessments, training and certification, assignment to roles (deployment), professional growth and development, reassignment and transfers, promotions and demotions, succession planning, and termination or retirement. The phases may not be in strict sequences, and some phases (like training, reassignment, and promotions) may recur.	TRMM
workforce and family care management (WFM)	The TRMM domain with the purpose to raise resilience awareness in the workforce and prepare them to contribute during a resilience event by providing plans, training, tools, and peace of mind.	TRMM

APPENDIX C: ACRONYMS

Acronym	Definition
AUI	Anywhere Utility Inc. – a company name used for examples
BES	Bulk electric system
BPS	Bulk power system
CEII	Critical energy infrastructure information
CERT®-RMM	CERT® Resilience Management Model
CIP	critical infrastructure protection
COP	common operating picture
DHS	Department of Homeland Security
DOE	Department of Energy
EMP	Electromagnetic pulse
EPRI	Electric Power Research Institute
EqM	transmission and supporting equipment domain
ERR	event response and recovery domain
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FERC	Federal Energy Regulatory Commission
GMD	Geomagnetic disturbance
HILF	High impact, low frequency
ICS	FEMA Incident Command System
IEEE	Institute of electrical and electronics engineers
ISAC	Information Sharing and Analysis Center
ISC	information sharing and communications domain
MIL	maturity indicator level
NATF	North American Transmission Forum
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
PM	resilience program management domain
PNNL	Pacific Northwest National Laboratory
RM	risk identification, assessment, & management domain
SA	situational awareness domain

Acronym	Definition
SCADA	supervisory control and data acquisition
SCE	supply chain and critical entities management domain
TBU	transmission business unit
TM	transportation management domain
TRMM	Electricity Subsector Transmission Resilience Maturity Model
WFM	workforce and family care management domain

APPENDIX D: REVISION HISTORY

Version	Date	Changes
	November 2019	Developed original document for pilot assessments
	October 2020	Initial public TRMM version (Version 1.0) posted

NOTICES

The TRMM was developed by leaders and transmission experts from transmission-owning utilities who are members of the Electric Power Research Institute (EPRI), the North American Transmission Forum (NATF), or both, with assistance from the U.S. Department of Energy (DOE) and the Pacific Northwest National Laboratory (PNNL). Wherever possible, the TRMM initiative leveraged and built upon existing efforts, models, and best practices to enhance transmission resilience.

This version of TRMM is being maintained by PNNL for DOE and the industry. The U.S. Government has, at a minimum, unlimited rights to use, modify, reproduce, release, perform, display, or disclose this version the TRMM or corresponding toolkits provided by DOE, as well as the right to authorize others, and hereby authorizes others, to do the same.