UNDERSTANDING CYBERSECURITY MATURITY MODELS WITHIN THE CONTEXT OF ENERGY REGULATION

September 2020
This publication was produced for review by the United States Agency for International Development (USAID). It was prepared by the National Association of Regulatory Utility Commissioners (NARUC).

UNDERSTANDING CYBERSECURITY MATURITY MODELS WITHIN THE CONTEXT OF ENERGY REGULATION

Project Title:	Cybersecurity – Energy Regulatory Training on Maturity Models & Technical Expertise
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Cooperative Agreement #:	AID – OAA-A-16-00049
Recipient:	National Association of Regulatory Utility Commissioners (NARUC)
Date of Publication:	September 2020
Author:	Marc Levesque, NEOS Advisory (NEOS Group, Inc.)

This publication was made possible through support provided by the Energy and Infrastructure Division of the Bureau for Europe and Eurasia under the terms of its Cooperative Agreement with the National Association of Regulatory Utility Commissioners, No. # AID – OAA-A-16-00049. The contents are the responsibility of the National Association of Regulatory Utility Commissioners (NARUC) and do not necessarily reflect the views of USAID or the United States Government.

Cover Photo: © denisismagilov / Adobe Stock

Table of Contents

1 FOREWORD 6

2 PREFACE 7

3 EXECUTIVE SUMMARY 8

4 INTRODUCTION 9

5 THE REGULATOR'S ROLE IN CYBERSECURITY 10

6 MATURITY MODELS 12

6.1 APPLICABILITY OF CYBERSECURITY MATURITY MODELS TO UTILITIES 13
6.2 WHAT IS A CYBERSECURITY MATURITY MODEL MEASURING? 13
6.3 CYBERSECURITY MATURITY MODEL TRAITS FOR REGULATORS 14
6.4 MATURITY MODEL CHARACTERISTICS 15
6.4.1 CARNEGIE MELLON'S CAPABILITY MATURITY MODEL INTEGRATION (CMMI), INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA) 16
6.4.2 ELECTRICITY SUBSECTOR – CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2) 17
6.4.3 NEMERTES MATURITY MODEL 19
6.4.4 DEPARTMENT OF DEFENSE (DOD) CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) 20
6.4.5 ISO/IEC 21827:2008 IT – SYSTEMS SECURITY ENGINEERING – CAPABILITY MATURITY MODEL (SSE-CMM) 22
6.4.6 COMMUNITY CYBERSECURITY MATURITY MODEL (CCSMM), CENTER FOR INFRASTRUCTURE ASSURANCE AND SECURITY (CIAS) 23
6.4.7 NIST – CYBERSECURITY FRAMEWORK 24
6.4.8 NARUC - CYBERSECURITY PREPAREDNESS EVALUATION TOOL 26
6.5 MATURITY MODEL COMPARISONS 28
6.6 MATURITY MODEL BENEFITS 30

7 USING MATURITY MODEL ASSESSMENT RESULTS IN REGULATORY PRACTICE 31

7.1 PREPARE A CYBERSECURITY MATURITY LEVEL ASSESSMENT 31
7.2 IMPLEMENT A CYBERSECURITY MATURITY LEVEL ASSESSMENT 32
7.3 ANALYZING AND INTERPRETING THE COLLECTED INFORMATION 32
7.4 INFLUENCING THE REGULATORY PROCESS 33

8 SUMMARY 34

9 BIBLIOGRAPHY 35

List of Figures

Figure 1: Relationship between the influencing factors of a maturity model. 12
Figure 2: Cybersecurity layers of protection. 14
Figure 3: CMMI maturity levels 17
Figure 4: ES-C2M2 cybersecurity capability maturity model....18
Figure 5: ES-C2M2 process 19
Figure 6: Nemertes security maturity model....20
Figure 7: DoD CMMC framework model 21
Figure 8: Maturity capability levels of the ISO/IEC 21827:2008 IT – Systems Security Engineering – Capability Maturity Model 22
Figure 9 - Cybersecurity community model 23
Figure 10: NIST – Cybersecurity framework....25
Figure 11: NARUC – Cybersecurity Preparedness Evaluation Tool – Cybersecurity Maturity Model......27
Figure 12: Generic cybersecurity maturity model 28

List of Tables

Table 1: Regulator responsibilities and their influence on cybersecurity....11
Table 2: Maturity models covered in this document 16
Table 3: ES-C2M2 maturity indicator level characteristics....18
Table 4: CCSMM cybersecurity maturity levels 24
Table 5: Cybersecurity maturity model comparison 29

Acronyms

Acronym	Definition
C2M2	Cybersecurity Capability Maturity Model
CCMS	Community Cybersecurity Maturity Model
CIAS	Center for Infrastructure Assurance and Security
CMM	Capability Maturity Model
CMMC	Cybersecurity Maturity Model Certification
CMMI	Capability Maturity Model Integration
CPET	Cybersecurity Preparedness Evaluation Tool
DoD	Department of Defense
DOE	U.S. Department of Energy
ES-C2M2	Electricity Subsector - Cybersecurity Capability Maturity Model
FOIA	Freedom of Information Act
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Standards Organization
IT	Information Technology
ISACA	Information Systems Audit and Control Association
MILs	Maturity Indicator Levels
NARUC	National Association of Regulatory Utility Commissioners
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OT	Operational Technology
SSE-CMM	Systems Security Engineering – Capability Maturity Model
US	United States

1 Foreword

The role of regulators in the energy sector has seen an immense transformation of regulatory responsibilities due, in part, to the development of new technologies. While such innovation has proved impressive for modernization of the electric grid and development of new types of energy, such as solar and wind, it has also generated more points of access and opened new doors for potential cyberattacks to the critical infrastructure and systems – which utilities and state regulators play a huge role in protecting.

As the Chair of the NARUC Critical Infrastructure Committee and Chairman of the Pennsylvania Public Utility Commission, I have been honored to take a lead role in engaging state regulators in discussions of our role to understand the impact of cyberattacks on the nation's critical infrastructure in both generation and distribution. This discerning path of the role of state regulators on the cybersecurity front has resulted in providing access to tools and resources to assist along the way.

As we entered a new decade in 2020, the challenges of a pandemic have impacted not only our lives and public health, but also the way we communicate and do business. The increased demand for internet access has been driven by virtual learning; the need to remotely operate businesses and government agencies on all levels, and for deeply personal uses – allowing families and friends to maintain those vital human connections in the midst of a global crisis that requires social distancing in order to control the spread of COVID-19. This expansion on the use of digital technology places a further emphasis on protecting the critical infrastructure of our nation from cyberattacks.

This publication is very timely in providing state regulators with another substantial resource. As an engineer, the author is able to bring a wealth of professional expertise in Cyber Maturity Assessments and Critical Infrastructure Risk Assessments, to provide clarity and understanding of cyber maturity models to state regulators in their role for assuring safe, reliable, and affordable delivery of utility services to consumers in a world dealing with an ever-present increase in cyber threats.

For commissioners looking for useful tools that they and their staff can use to build up their regulatory responsibilities as they delve into cybersecurity, this publication is a "must read!" State utility commissions can use this tool without feeling a void from the lack of cybersecurity knowledge and expertise within their Commission.

Gladys Brown Dutrieuille, Esquire
Chairman, Pennsylvania Public Utility Commission

2 Preface

In addition to this guide, NARUC has developed a comprehensive suite of resources to help regulators increase their cybersecurity proficiency through USAID's Europe and Eurasia Cybersecurity Initiative. These resources are meant to help regulators take action consistent with their respective needs and priorities. Although these documents were developed for energy regulators of Europe and Eurasia, their content can be applied all over the world. These evaluations facilitate decisions regarding the effectiveness of utilities' cyber security preparedness efforts, setting national cybersecurity standards, and the prudence of cyber expenditures. A brief description of each resource follows.

1. **Black Sea Cybersecurity Strategy Development Guide | 2017**

   This guide was developed to provide information and lessons learned to support Black Sea regulators, and others, in developing their own commissions' cybersecurity strategies. Drawing from experiences and best practices from U.S. state-level regulatory commissions and elsewhere, the document has been designed to cover the important issues and questions that regulators should address as they begin the process of developing their unique cybersecurity strategies.

2. **Cybersecurity Evaluative Framework for Black Sea Regulators | 2017**

   This evaluative framework is an easy-to-use tool for regulators to evaluate utilities' cybersecurity preparedness. It is designed to provide a structured way for regulators to assess what level of cyber-preparedness utilities have reached and identify areas for improvement.

3. **The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards | 2020**

   This guide was initially developed for regulators in Europe and Eurasia to reinforce their knowledge of practical cybersecurity solutions in the face of ongoing threats within the energy sector. However, the questions of how to evaluate risks, assess mitigation measures, and select standards are relevant for regulators around the world.

4. **Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators | 2020**

   These guidelines were developed to assist regulators in ensuring that investments made in the name of cybersecurity are reasonable, prudent, and effective. They are intended to assist regulators in defining tariffs by establishing a regulatory approach to enhance the cybersecurity stance of their power systems, and are based on literature and current practices.

3 Executive Summary

We are living in a time of cyberwarfare. Cybersecurity threats are becoming more frequent and prevalent these days as criminals seek financial gain, terrorists seek to disrupt, rogue nations seek political advantage, and script kiddies want to disrupt just for the fun of it. Regardless of who the threat source is, the outcome of a cyberattack can be very damaging to operations, safety, and reputation. For this reason, it is necessary to endeavor to stay at least one step ahead of cyber threats by always being on the alert, ready for attacks, and by establishing controls to protect against and repel invasions.

When appropriately used, cybersecurity maturity models can be a powerful tool to help protect against cybersecurity threats by demonstrating the areas of possible vulnerability where improvement is desired. These models also help track progress over time. The ability to use maturity models as a tool comes from understanding the information used by the various maturity models now considered, their relative strengths and weaknesses, and how each of them may be used to support the regulatory process and the cybersecurity posture of an organization.

Using a cybersecurity maturity model does not require a regulator to be a cybersecurity expert; a basic knowledge of cybersecurity is sufficient to leverage the capabilities of a cybersecurity maturity model during the course of the regulatory review process.

Utilities provide customers with a critical service, intending to ensure 24 hour/7 day/365 days a year operation. They are responsible for ensuring that service disruptions are avoided and minimized, and it is the regulator's responsibility to ensure that utilities are prepared for disruptive events, including cyber-attacks. With the increasing level of digitization and the introduction of digital control systems into utility operations, the opportunity for customer service disruption from digital equipment failures or cyber-attacks also increases.

The cybersecurity maturity level of a utility requires time to improve. A cybersecurity maturity model provides regulators with a tool to measure and monitor the rate and magnitude of cybersecurity improvement over time, as well as judge the prudency of utility efforts to be more cyber secure.

Cybersecurity maturity models provide regulators with a means to measure the cybersecurity readiness of a utility and compare this level of preparedness against previous assessments, a target baseline, and other utilities. Regulators can use the models to identify both good and bad trends. The cybersecurity maturity model data gathered by regulators can also influence regulatory changes.

Having a good understanding of cybersecurity maturity models benefits regulators by ensuring that utilities are properly prepared to deal with cyber-attacks, and provides data to support prudent improvements in cybersecurity-related regulatory oversight.

It is the goal of this document to provide an understanding of the fundamental principles of maturity models so that the greatest benefit can be realized from their use, rather than ranking maturity models against each other. This will permit regulators to work efficiently and effectively with utilities on the subject of cybersecurity regardless of the cybersecurity model that is selected for use, whether by the regulator or the utility.

4 Introduction

Cybersecurity has quickly become one of the most significant risks to critical infrastructure with the advent of state-sponsored attacks, terrorist attacks, and attacks by collaborative teams of individuals.

Cyber-attacks have typically focused on Information Technology (IT) and Operational Technology (OT) hardware and software infrastructure, such as breaking through firewalls and exploiting operating systems and application software vulnerabilities. Although these types of assaults continue, a rise in attacks on IT and OT systems by targeting people within the organization (such as staff, vendors, maintainers, and others) is becoming more prevalent. On the horizon, trends predict sophisticated attacks by teams with detailed knowledge of the inner workings of utilities, with these types of cyber-attacks targeting policies, processes, and workflows, such as supply chains, operations, and logistics.

Defending against the ever-changing nature of cyber-attacks requires a constant vigil to safeguard against known cyber-attack vectors and to identify new cyber-attack strategies and methods. In doing so, appropriate defenses can be put in place before cyber-attacks occur. A cybersecurity maturity model-based approach is a compelling first step in determining the appropriate level of defense needed against cyber-attacks.

This primer discusses cybersecurity maturity models within the context of energy regulation to provide a fundamental understanding of their application, benefits, and the value that they can afford in the regulatory process. This primer provides insight into:

- the basics of maturity models;
- how maturity models pertain to cybersecurity for utilities;
- the role of the regulator with regards to cybersecurity;
- the use of cybersecurity maturity models as a regulatory tool; and
- the use of cybersecurity maturity models to influence regulatory practices and decisions.

A cybersecurity maturity model assessment on its own does not ensure a good cybersecurity posture. Cybersecurity models are successful when used to identify gaps and weaknesses, and thus help determine possible recommended courses of actions. Using a cybersecurity maturity model and analyzing its resulting assessment provides regulators with an indication of the current capabilities of a utility, and helps to identify areas where practices are reactive to cybersecurity threats. These findings can be reported to internal and external stakeholders and used for benchmarking purposes between utility organizations regionally, nationally, or internationally.

5 The Regulator's Role in Cybersecurity

As energy infrastructure becomes increasingly more automated and the Internet of Things (IoT) becomes more prevalent within energy sectors, ensuring the cybersecurity of energy infrastructure is of critical importance. Utility regulators, already overburdened to ensure the safety, reliability, and efficiency of utility services' delivery, are now required to oversee the cybersecurity of their regulated utilities as well.

While regulators are entrusted with the responsibility of protecting the public interest, their role is wide-ranging; not surprisingly, regulators may lack the technical background, capability, and resources needed to scrutinize a utility's cybersecurity posture. In this regard, a cybersecurity maturity model is a useful framework in that it summarizes, at a more strategic level, a utility's cybersecurity posture. It does not require a regulator to understand the detailed cyber tactics and infrastructure protections that are in place at a detailed level, but it provides sufficient insight into the utility's overall posture. Of course, this also presumes that the cybersecurity maturity model has been completed properly. This is likely an area of increasing regulatory follow-up, such as through regulatory auditing practices.

As security and business continuity costs continue to increase, regulators must come to accept that textbook cybersecurity solutions and procedures are impracticable under present-day regulatory and governing standards. Cybersecurity controls have advanced tremendously, and hackers continue to find new ways to outwit and bypass them, requiring utility organizations to continually monitor and enhance or augment their controls.

Regulators can improve their understanding of cybersecurity through training and certifications, and they can choose from several available software and business process tools to assist with their cybersecurity responsibilities. A cybersecurity maturity model will best support them because it ensures the cybersecurity maturity level assessment undertaking will be at a level sufficient for regulatory review and oversight, without delving into considerable details well beyond the purview of most regulators.

It is prudent for regulators to collaborate closely with utility organizations to understand the cybersecurity challenges they face. Information sharing and cross-sector collaboration are critical to tackling these jurisdictional concerns and for preventing duplication of efforts. A robust information-sharing system helps ensure that cyber threats are shared with other utility organizations, thus helping to mitigate potential cyber risks before they occur.

As a regulatory tool, cybersecurity maturity models help assess organizational processes and support strategies going forward. Regulators can work to modify or change policies or directives to be more pre-emptive and measurable, as well as regionally, nationally, or internationally consistent and efficient with regards to cybersecurity requirements or improvements. Only then can controls be put in place to counter cybersecurity threats as they evolve.

The information gained from cybersecurity maturity model assessments helps regulators establish an acceptable level of risk for delivery of services and convey this as their risk tolerance to utility organizations. As regulatory risk tolerance is defined and understood (and what this implies for cost prudency), utility organizations also have better information to prioritize cybersecurity activities. This will help equip utility executives to make more informed decisions regarding cybersecurity response and expenditures. Regulators must work to ensure executive support for cybersecurity efforts required for energy infrastructure. In addition, the use of resources needed to accomplish them should be persistent and not merely in response to a breach.

Not surprisingly, utility organizations that consistently monitor and improve cybersecurity controls based on maturity model assessments typically have leadership invested in, and committed to, cybersecurity as a fundamental priority. A regulator is responsible for achieving a balance across each core responsibility when providing oversight and supporting regulatory changes regarding cybersecurity.

Table 1 outlines the core responsibilities of a regulator and how the cybersecurity posture of a utility influences all of these areas:

Table 1: Regulator responsibilities and their influence on cybersecurity.

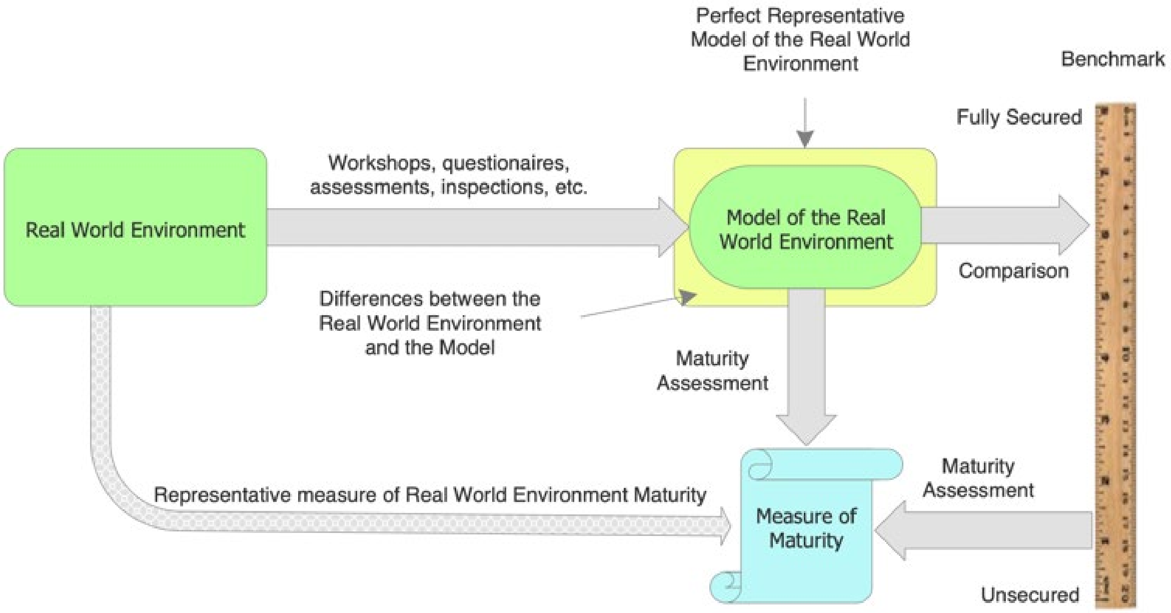
Core Responsibilities	Cybersecurity Influences
Design and manage tariffs	Cybersecurity costs are reflected in the revenue requirements and tariffs.
Enforce system reliability and expand service accessibility	Appropriate cybersecurity controls can minimize the impact on system reliability caused by cyber-attacks.
Ensure the financial health of utilities	Appropriate cybersecurity controls ensure that the utility is able to continue the delivery of services, the billing of customers, collections, maintenance, system operations, and so on, when faced with cyber-attacks. In the face of particularly disruptive attacks, it is able to provide evidence of due diligence to counter liability concerns.
Facilitate private investment	Appropriate cybersecurity controls ensure a good reputation for protecting utility assets from cyber-attacks; to do otherwise could discourage investment. For instance, if there are concerns as to the robustness of the utility's cyber posture, the utility could face difficulties attracting private participation (e.g., IPPs).
Protect the interests of the poor and those requiring dedicated utility services	Appropriate cybersecurity controls ensure the continued delivery of utility services to the poor. Further, some customers that are reliant on reliability of service due to medical or other issues could be at risk if controls and measures (e.g., backup supply) are inadequate.
Support technical safety and reliability of a utility system	Appropriate cybersecurity controls reduce the risk of cyber-attack-related technical safety events from occurring and also minimizes the chances of cyber-attacks reducing the reliability of the utility system.
Enhance energy security and with it, economic security	Appropriate cybersecurity controls reduce the risk of energy security being affected and the consequent impact that may have on the economy.
Ensure customer information privacy	Appropriate cybersecurity controls reduce the risk of customer information being lost, stolen, or accidentally exposed.

6 Maturity Models

A model is the representation of a real-world environment in terms of words, diagrams, and pictures. The challenge in developing a model is to ensure that it accurately depicts the real world it intends to represent. An accurate model is determined by the correctness and the level of detail of the information that is used to describe the real-world environment. The development of an indicative model is achieved through questionnaires, assessments, inspections, and a review of artifacts related to the real-world environment.

The maturity of a real-world environment is determined by evaluating the gathered information (i.e., the model) used in creating the model for appropriateness, completeness, accuracy, and quality against a benchmark. Figure 1 depicts the relationship between the "Real-World Environment," a "Model of the Real-World Environment," the Benchmark, and the Measure of Maturity.

Figure 1: Relationship between the influencing factors of a maturity model.[1]


Perfect Representative Model of the Real World Environment
Benchmark
Fully Secured
Workshops, questionaires, assessments, inspections, etc.
Real World Environment
Model of the Real World Environment
Comparison
Differences between the Real World Environment and the Model
Maturity Assessment
Representative measure of Real World Environment Maturity
Measure of Maturity
Maturity Assessment
Unsecured

A perfect representation of the "Real-World Environment" is depicted in the diagram by the yellow rectangle behind the "Model of the Real-World Environment" green oval. The goal is for the "Model of the Real-World Environment" to align as closely as possible with the yellow rectangle.

Cybersecurity maturity is determined by understanding the varying degrees of security from unsecured to fully secured across the entire environment and by using maturity as a gauge to measure the difference between where it is presently and where it can be.

The value that a cybersecurity maturity model provides consists of the following:

- It aggregates the information related to a utility's cybersecurity environment, making it relatively easy to visualize;
- It helps establish documented baselines of the cybersecurity posture of a utility;

[1] Marc Levesque, Neos Advisory, July 2020.

- It provides a means to measure the progress that a utility makes in its cybersecurity posture and maturity level over time;
- It helps to visualize gaps in the cybersecurity posture of a utility, identify areas to improve, and increase the cybersecurity maturity level;
- It provides the opportunity to compare the cybersecurity posture and maturity level of a utility against a benchmark and other utilities; and
- The documented baselines of the cybersecurity maturity level data provide opportunities to use the data to justify additional investments in people, processes, and technology to regulators.

6.1 Applicability of cybersecurity maturity models to utilities

Cybersecurity plays a much more significant role in energy markets and infrastructure today than in recent decades. With digital computer technology now deployed in the IT and the OT environments, the opportunities for disrupting a nation's critical infrastructure have increased significantly. This rise in technological ability and political rivalries has led to the advent of certain countries being identified as cyber threats to other countries. Today, cyber treats pose an ever-increasing risk of disrupting critical infrastructure service, thus warranting it to be considered in line with other disruptive forces such as bad weather, poor maintenance, physical security encroachments, natural disasters, equipment failure, operator error, and so on.

Successful cyber-attacks may result in loss of revenue and incur costs for recovery for the utility. More importantly, they can also cause a loss of service to customers due to service disruption, damage to equipment, damage to facilities, personnel-related interruptions, and the loss of data including personal data and information used to corroborate customer billing or data used for other financial purposes.

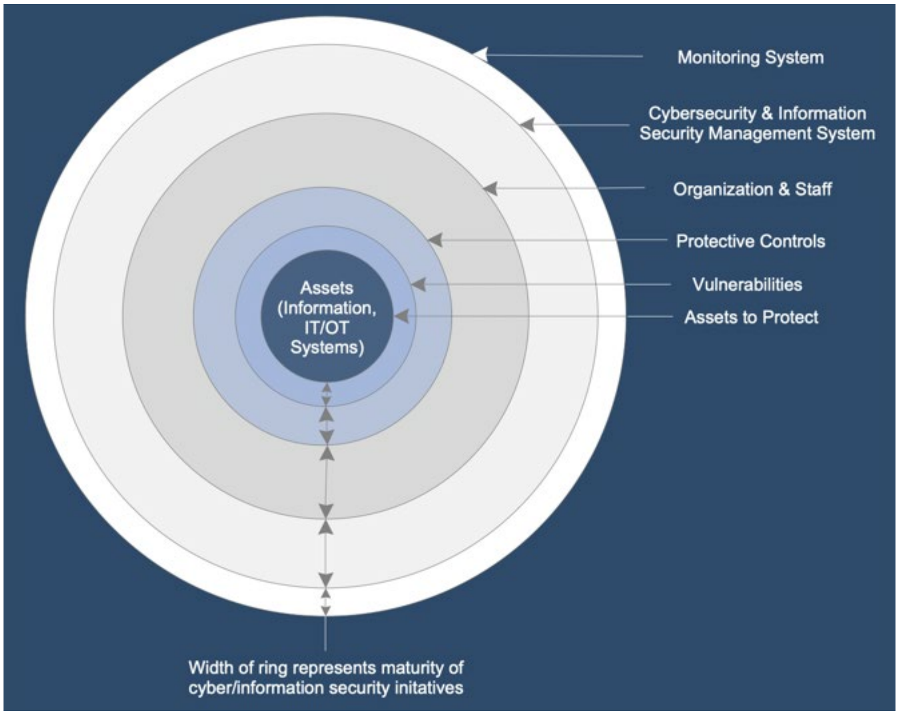
While the technical and operational failures to critical infrastructure are well understood and can be managed and controlled through various processes and procedures (such as periodic maintenance), cyber threats are unique. They can occur at any time, can occur frequently, may originate from anywhere, and exploit both known and unknown vulnerabilities while potentially remaining undetected.

Cybersecurity protects a utility’s assets from the various threats that exploit or plan to leverage asset vulnerabilities to harm the utility. The ultimate goal of cybersecurity is to identify all asset vulnerabilities that must be protected in order to avoid harm to the utility, and to put in place the appropriate protective controls along with monitoring equipment and protocols to measure their effectiveness.

6.2 What is a cybersecurity maturity model measuring?

Cybersecurity maturity is a measure of the ability of a utility to protect its assets from harm. Figure 2 shows a simplified diagram of a cybersecurity environment that depicts a group of assets at the center, with vulnerabilities being protected by protective controls along with the organization and staff and its cybersecurity and information security management system. It is the effectiveness of the cybersecurity measures that are being measured by the cybersecurity maturity models.

Figure 2: Cybersecurity layers of protection.[2]


Monitoring System
Cybersecurity & Information Security Management System
Organization & Staff
Protective Controls
Vulnerabilities
Assets to Protect
Assets (Information, IT/OT Systems)
Width of ring represents maturity of cyber/information security initatives

The measure of this effectiveness is accomplished by the monitoring system that evaluates the domains covering the following areas:

- cybersecurity and information security management system;
- organization and staff;
- protective controls;
- vulnerabilities; and
- assets to protect.

These domains are measured through the assessment process of a cybersecurity maturity model.

6.3 Cybersecurity maturity model traits for regulators

Numerous cybersecurity maturity models have been developed, each for its own specific purpose. Thus, not all cybersecurity maturity models are perfectly suited for electric utilities or publicly funded regulators; some are better than others.

The following characteristics can assist regulators in determining the appropriateness of a cybersecurity maturity model for their environment.

[2] Marc Levesque, Neos Advisory, July 2020.

- be simple to use and not require a background in cybersecurity since regulators are not expected to be cyber experts;
- be sufficiently expansive to represent the utility's cybersecurity posture;
- represent the utility's cybersecurity posture without having them divulge confidential or proprietary information;
- gather sufficient and accurate information to be able to establish the cybersecurity maturity of the utility organization; and
- contain sufficiently defined and tangible information to perform maturity level comparisons over time of a utility's changes in cybersecurity maturity posture.

6.4 Maturity Model Characteristics

In general terms, the purpose of a maturity model is to assess the as-is situation and optionally to diagnose and eliminate deficient capabilities through a continuous improvement process based on a set of predefined criteria. A maturity model is a meta-model with hierarchical layers representing maturity levels that consist of one or more competence objects, criteria, descriptors, descriptions, process areas, or activities. Supporting this are methods for data collection and analysis.

A maturity model is used for as-is assessments where the current capabilities under investigation are assessed to a designated criterion. Maturity models serve a prescriptive purpose of identifying desirable maturity levels and providing guidelines on improvement measures, or a comparative purpose for internal or external benchmarking.

The first maturity model was developed in 1987 by Carnegie Mellon University as a U.S. Office of the Secretary of Defense initiative, Capability Maturity Model (CMM), to assess software development's maturity.[3] This model's driving principles continue to be used today to create alternative models. These principles apply a designated set of processes to determine the maturity of an organization by evaluating and classifying them into categories or levels.

Various cybersecurity maturity models have since evolved. Most maturity models originate from the Carnegie Mellon Capability Maturity Model Integration (CMMI) model. The derivations are typically a tailoring of CMMI to a target environment. A brief overview of the more prominent models is included in this document to demonstrate the variations that exist between the various models. If additional information is desired on any of the models, the reader is encouraged to read publicly available information for each model, beginning with the documents referenced in the bibliography.

The Maturity Models that are considered in this document are listed below in Table 2.

[3] Software Engineering Institute (SEI), "*CMMI for Development*", Carnegie Mellon University, 2010.

Table 2: Maturity models covered in this document

#	Maturity Model	Abbreviation
1	Carnegie Melon Capability Maturity Model Integration	CMMI
2	Electricity Subsector - Cybersecurity Capability Maturity Model	ES-C2M2
3	Nemertes Maturity Model	N/A
4	Department of Defense (DoD) Cybersecurity Maturity Model Certification	CMMC
5	ISO/IEC 21827:2008 Information Technology – Security techniques – Systems Security Engineering – Capability Maturity Model	SSE-CMM
6	Center for Infrastructure Assurance and Security (CIAS) Community Cybersecurity Maturity Model	CCSMM
7	National Institute for Standards and Technology – Cybersecurity Framework	NIST
8	NARUC - Cybersecurity Preparedness Evaluation Tool	CPET

6.4.1 Carnegie Mellon's Capability Maturity Model Integration (CMMI), Information Systems Audit and Control Association (ISACA)

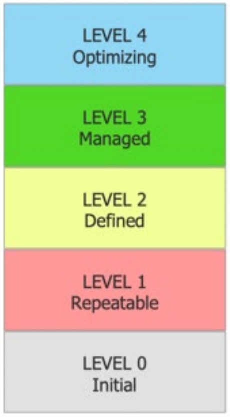
CMMI is the original maturity model first defined by Carnegie Mellon University of Pennsylvania in 1987.[4] Its development was in response to a U.S. Office of the Secretary of Defense initiative under the name of CMM to assess software development's maturity, and it has undergone a series of changes over the years. Although Carnegie Mellon University was originally responsible for the model, the rights are now owned by the Information Systems Audit and Control Association (ISACA), which is an international organization that focuses on IT governance.

CMMI, shown in Figure 3, is a generic maturity model that can be applied to any organization, venture, or domain. For this reason, it is often the basis for many other maturity models.

Since the model is generic, it allows the user to adapt it to the environment being assessed, which is advantageous when there are no existing predefined models in place. The main downside of the model is the extensive amount of tailoring required to align it to cybersecurity, as compared to other models that have already been established for this purpose.

[4] SEI, "CMMI for Development", Carnegie Mellon University, 2010.

Figure 3: CMMI maturity levels[5]



6.4.2 Electricity Subsector – Cybersecurity Capability Maturity Model (ES-C2M2)

The ES-C2M2, tailored for the electricity subsector, was developed by the Department of Energy (DOE) and is a subset of C2M2. The most current version is 1.1, issued in February 2014.[6] ES-C2M2 focuses on the implementation and management of cybersecurity for critical infrastructure. It is based on the NIST Cybersecurity Framework, and is easily scalable.

This cybersecurity maturity model is intended to be used by an organization for self-assessment. In order for this model to be effectively implemented, it is best to use it as part of a continuous enterprise risk management process. This implies that detailed organizational information that would be considered business sensitive or proprietary must be included in the model.

The ES-C2M2 model, shown in Figure 4, is organized into ten domains made up of logical groupings of cybersecurity practices. The practices within each domain are then mapped into objectives supporting the domain and categorized into 'approach objectives' and 'management objectives.' For each objective, the practices are categorized by Maturity Indicator Levels (MILs) ranging from zero to three, and the characteristics of each MIL can be found in Table 3. The practices, also known as functions, indicate the operations of the organization that are being evaluated by the maturity model.

[5] Illustrative Interpretation by author, Ibid.

[6] Jason D. Christopher, Fowad Muneer, John Fry, and Paul Skare, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1*. Washington DC: U.S. Department of Energy.

Figure 4: ES-C2M2 cybersecurity capability maturity model[7]

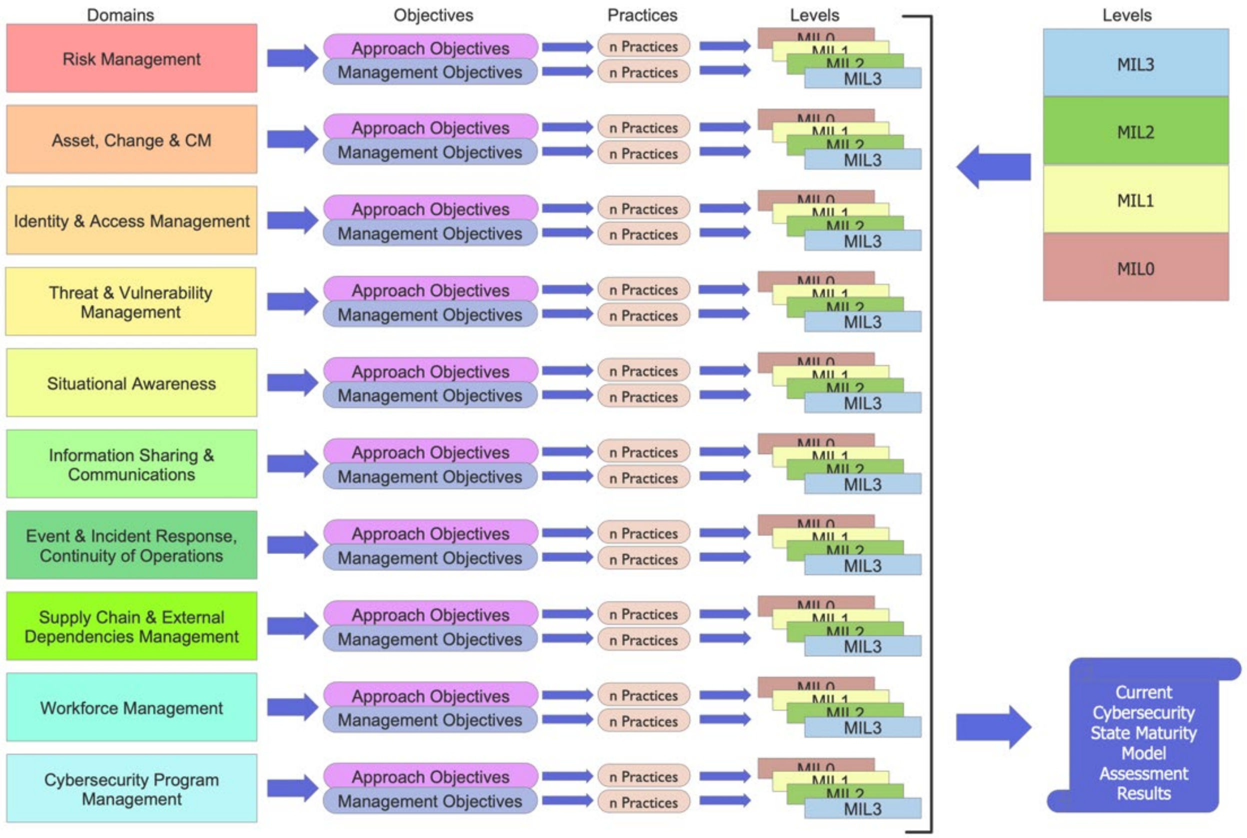


Table 3: ES-C2M2 maturity indicator level characteristics[8]

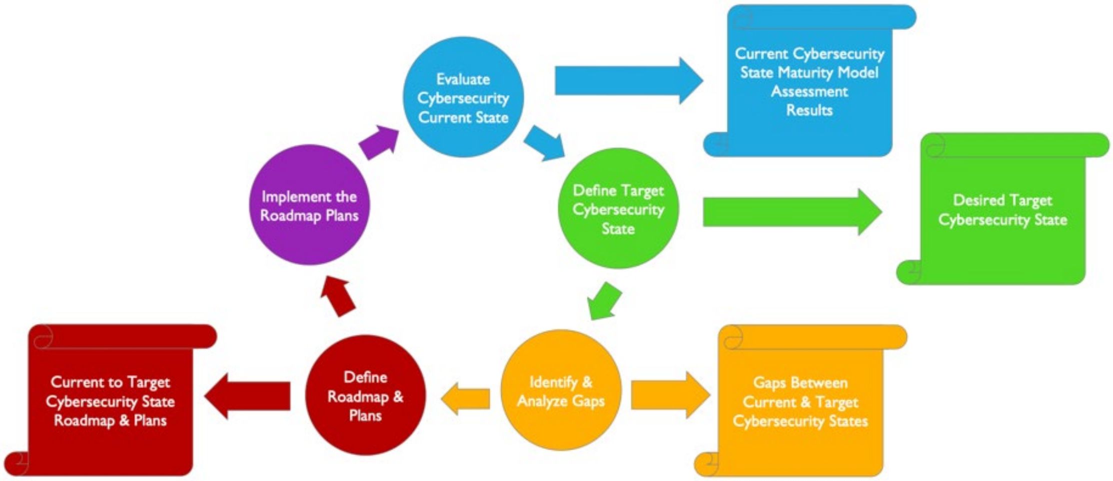
Level	Characteristic
MIL0	• Practices are not performed.
MIL1	• Practices are performed, but typically in an ad hoc manner.
MIL2	• Practices are documented; • Stakeholders are identified and involved; • Activities and initiatives are properly resourced; and • Implementations are guided by standards and guidelines.
MIL3	• Governance and policies provide guidance; • Compliance requirements are defined; • Reviews are performed to ensure compliance to requirements; • Responsibility, Accountability, and Authority are assigned; and • Staff have the proper skills and knowledge.

[7] Christopher et al, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1,* Illustrative Interpretation by author.

[8] Christopher et al, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1,* Adaptation by author.

The ES-C2M2 model goes beyond an assessment of cybersecurity maturity level as depicted by the process shown in Figure 5 below. The ES-C2M2 model uses the cybersecurity maturity level information to identify gaps between the current cybersecurity posture and the desired target cybersecurity posture. With this gap definition, a roadmap and plans can be established to evolve the organization from the current level of preparedness to the target cybersecurity maturity level.

Figure 5: ES-C2M2 process[9]


Evaluate Cybersecurity Current State
Current Cybersecurity State Maturity Model Assessment Results
Implement the Roadmap Plans
Define Target Cybersecurity State
Desired Target Cybersecurity State
Current to Target Cybersecurity State Roadmap & Plans
Define Roadmap & Plans
Identify & Analyze Gaps
Gaps Between Current & Target Cybersecurity States

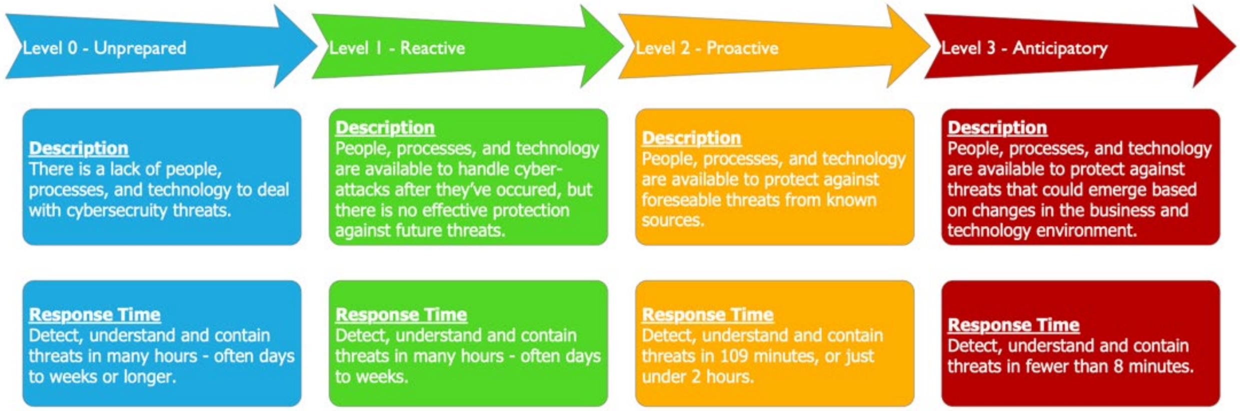
6.4.3 Nemertes Maturity Model

Nemertes Research is an independent advisory and consulting firm that analyzes business value from emerging technologies. Nemertes has developed "The Security Maturity Model," which includes four levels: Unprepared, Reactive, Proactive, and Anticipatory.[10]

[9] Christopher et al, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1,* Illustrative Interpretation by author.

[10] Nemertes, *The Nemertes Security Maturity Model.* Nemertes Research, 2017.

Figure 6: Nemertes security maturity model[11]



Level 0 - Unprepared	Level 1 - Reactive	Level 2 - Proactive	Level 3 - Anticipatory
Description There is a lack of people, processes, and technology to deal with cybersecruity threats.	**Description** People, processes, and technology are available to handle cyber-attacks after they've occured, but there is no effective protection against future threats.	**Description** People, processes, and technology are available to protect against foreseeable threats from known sources.	**Description** People, processes, and technology are available to protect against threats that could emerge based on changes in the business and technology environment.
Response Time Detect, understand and contain threats in many hours - often days to weeks or longer.	**Response Time** Detect, understand and contain threats in many hours - often days to weeks.	**Response Time** Detect, understand and contain threats in 109 minutes, or just under 2 hours.	**Response Time** Detect, understand and contain threats in fewer than 8 minutes.

The Nemertes Security Maturity Model considers the organizational aspects of security management and operational metrics, mapping them into the maturity model's four levels. For the organizational aspects, the model examines multiple dimensions of the organization, including budgeting and procurement, organization, planning, policies and processes, and technology. The fundamental approach of the Nemertes Security Maturity Model is to gather operational metrics which, for the most part, are time-based and aligned with those contained in the NIST Cybersecurity Framework.[12] These include:

- the time to detect that a potentially dangerous event has occurred;
- the time that it takes to understand if the event represents a breach;
- the time to contain the breach; and
- the time that it takes to recover from the breach.

The outcome of collecting and analyzing this information is a model that represents the cybersecurity maturity of the organization. This maturity information determines the steps required to improve the organization's cybersecurity maturity.

6.4.4 Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)

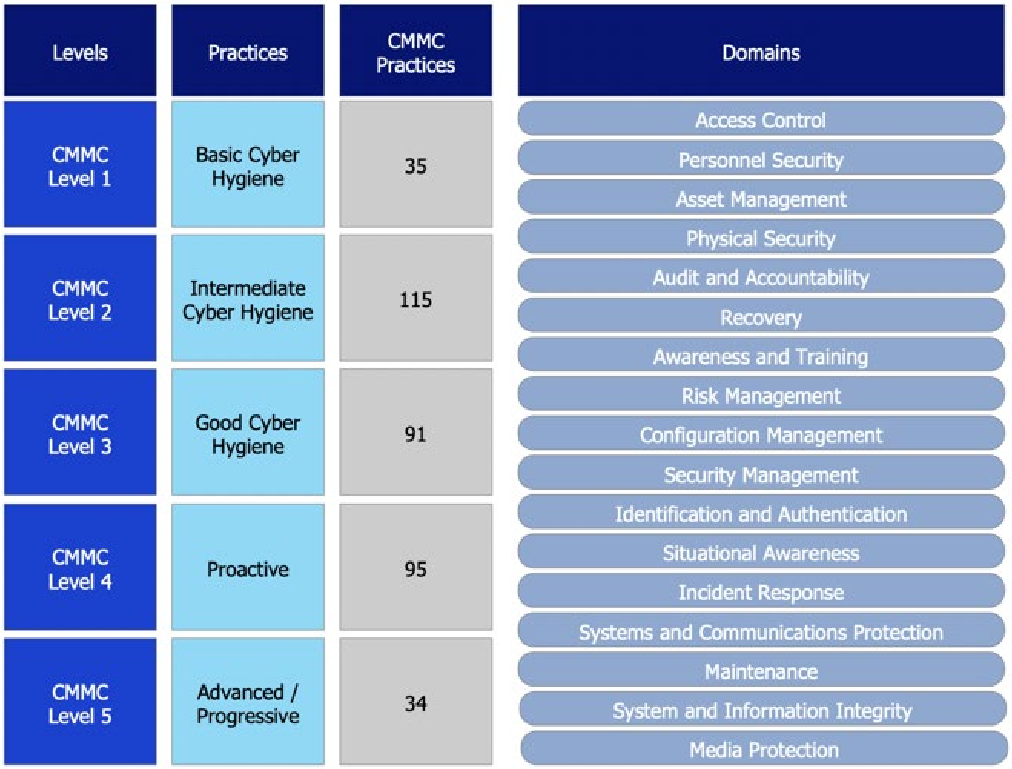
The Cybersecurity Maturity Model Certification (CMMC) was recently developed by the U.S. Department of Defense (DoD) because it was felt that cybersecurity maturity model self-assessments could not be trusted, and therefore a new approach was needed. There is no self-certification in the CMMC model; it requires an organization to coordinate directly with an accredited and independent third-party commercial certification organization to request and schedule a CMMC assessment.[13]

The CMMC Model is based on the best practices of different cybersecurity standards, including NIST SP 800-171, NIST SP 800- 53, ISO27001, ISO27032, AIA NAS9933, and others, being brought into one

[11] Illustrative interpretation by author, Ibid.
[12] J.T. Johnson, *"Cybersecurity maturity model lays out four readiness levels", Techtarget, 2019.*
[13] Department of Defence (DoD), Cybersecurity Maturity Model Certification (CMMC). DoD, 2020.

cohesive standard for cybersecurity. Version 1.0 of the CMMC framework was made available in January 2020.[14]

Figure 7: DoD CMMC framework model[15]



Levels	Practices	CMMC Practices
CMMC Level 1	Basic Cyber Hygiene	35
CMMC Level 2	Intermediate Cyber Hygiene	115
CMMC Level 3	Good Cyber Hygiene	91
CMMC Level 4	Proactive	95
CMMC Level 5	Advanced / Progressive	34

Domains

- Access Control
- Personnel Security
- Asset Management
- Physical Security
- Audit and Accountability
- Recovery
- Awareness and Training
- Risk Management
- Configuration Management
- Security Management
- Identification and Authentication
- Situational Awareness
- Incident Response
- Systems and Communications Protection
- Maintenance
- System and Information Integrity
- Media Protection

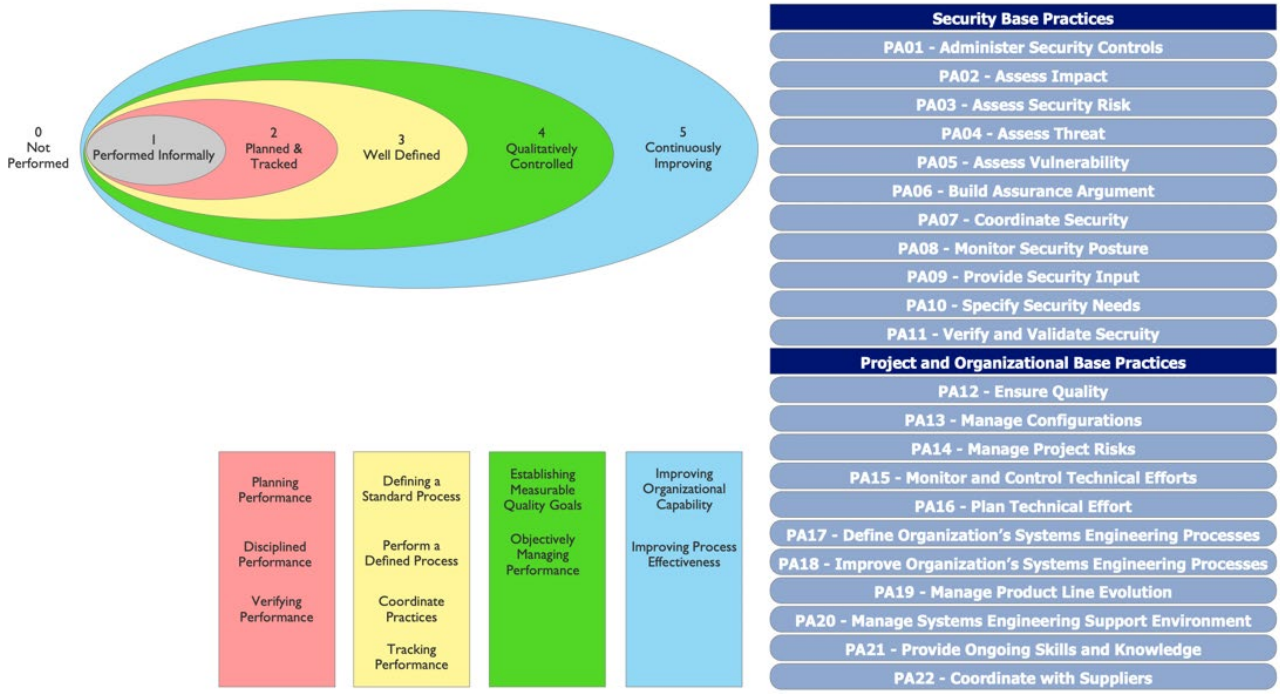
[14] C. Kellep, A. Williams, Understanding Cybersecurity Maturity Model Certification (CMMC), Security Boulevard, 2020.
[15] DoD. Cybersecurity Maturity Model Certification (CMMC), DoD, 2020, Illustrative Interpretation by author.

The CMMC, depicted in Figure 7, contains five levels ranging from basic hygiene to state-of-the-art practices. The CMMC is intended to serve as a mechanism to verify that appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene. Compliance with the framework consists of achieving a level of implementation within 17 domains.

6.4.5 ISO/IEC 21827:2008 IT – Systems Security Engineering – Capability Maturity Model (SSE-CMM)

The SSE-CMM® is a compilation of security engineering best practices intended to determine an organization's process maturity with regards to security, and is controlled by the International Standards Organization (ISO) in Bern, Switzerland. [16] The objective of the SSE-CMM® is to advance security as a defined, mature, and measurable discipline. The SSE-CMM® model and appraisal methods are tools for organizations to evaluate their security practices and identify improvements to establish confidence in an organization's security assurance.

Figure 8: Maturity capability levels of the ISO/IEC 21827:2008 IT – Systems Security Engineering – Capability Maturity Model[17]


0 Not Performed
1 Performed Informally
2 Planned & Tracked
3 Well Defined
4 Qualitatively Controlled
5 Continuously Improving
Planning Performance
Disciplined Performance
Verifying Performance
Defining a Standard Process
Perform a Defined Process
Coordinate Practices
Tracking Performance
Establishing Measurable Quality Goals
Objectively Managing Performance
Improving Organizational Capability
Improving Process Effectiveness
Security Base Practices
PA01 - Administer Security Controls
PA02 - Assess Impact
PA03 - Assess Security Risk
PA04 - Assess Threat
PA05 - Assess Vulnerability
PA06 - Build Assurance Argument
PA07 - Coordinate Security
PA08 - Monitor Security Posture
PA09 - Provide Security Input
PA10 - Specify Security Needs
PA11 - Verify and Validate Secruity
Project and Organizational Base Practices
PA12 - Ensure Quality
PA13 - Manage Configurations
PA14 - Manage Project Risks
PA15 - Monitor and Control Technical Efforts
PA16 - Plan Technical Effort
PA17 - Define Organization's Systems Engineering Processes
PA18 - Improve Organization's Systems Engineering Processes
PA19 - Manage Product Line Evolution
PA20 - Manage Systems Engineering Support Environment
PA21 - Provide Ongoing Skills and Knowledge
PA22 - Coordinate with Suppliers

[16] ISO (International Standards Organization), *ISO 21827:2008 IT – Systems Security Engineering – Capability Maturity Model (SSE-CMM)*, ISO, 2008.
[17] Illustrative interpretation by author, Ibid.

The SSE-CMM® is organized into 22 process areas that are evaluated based on the five Capability Maturity Levels depicted in Figure 8 along with the 22 process areas that are grouped into two (2) categories: Security Base Practices and Project and Organizational Base Practices.

The model is a standard metric for security practices covering:

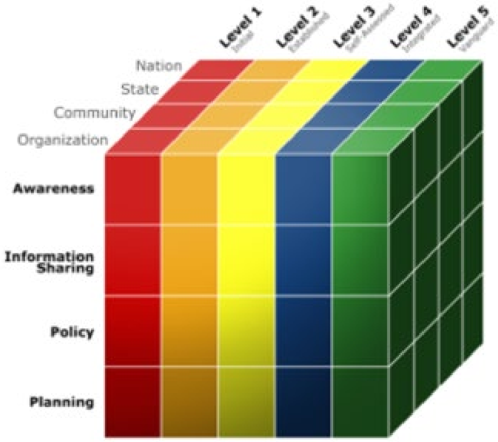
- the entire life cycle, including development, operation, maintenance, and decommissioning activities;
- the whole organization, including management, organizational, and technical activities;
- concurrent interactions with the system, software, hardware, operation, and maintenance; and
- interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation.

6.4.6 Community Cybersecurity Maturity Model (CCSMM), Center for Infrastructure Assurance and Security (CIAS)

The CIAS was established by The University of Texas at San Antonio in 2001 as a part of the creation of a cybersecurity program, with the goal to advance cybersecurity capabilities. [18] The CIAS often works in collaboration with the U.S. Department of Homeland Security (DHS) and the U.S. DoD. The CIAS has developed the CCSMM as a community-based model to support jurisdictions to develop their own cybersecurity programs.

The CCSMM takes a community-based view that encompasses national, state, communities and organizations, within its goal of ensuring overarching consistency in achieving desired levels of cybersecurity maturity. The concept of communities includes organizations, cities, towns, citizens or other groupings of common interest. The concept behind the CCSMM is that a cybersecurity model cannot exist in isolation but must collaborate on the subject of cybersecurity.

Figure 9 - Cybersecurity community model[19]



[18] CIAS, "*About the Center for Infrastructure Assurance and Security (CIAS)*", CIAS, 2020.
[19] Ibid.

The CCSMM is a three-dimensional model with maturity levels on one axis, communities on a second axis, and dimensions of improvement on the third axis as shown in Figure 9.

This model responds to the linkages that exist among the jurisdictions, the community, and the organizations and their dimensions of improvement. This model performs a high-level assessment because it is focused on jurisdictions, communities, and organizations. Depicted in Table 4 is a description of each CCSMM cybersecurity maturity level.

Table 4: CCSMM cybersecurity maturity levels[20]

Level	Description
Level 1- Initial	Little or no cybersecurity awareness, analysis and evaluation
Level 2- Established	Aware of cyber threats, problems and the imperative of adopting cybersecurity
Level 3- Self Assessed	Actively promote cybersecurity awareness and cooperate with others in establishing training and education programs
Level 4- Integrated	Cybersecurity is incorporated into every process of an organization.
Level 5- Vanguard	Cybersecurity is a business imperative.

6.4.7 NIST – Cybersecurity Framework

The "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology" was issued on April 16, 2018. [21] It was developed in response to the NIST's updated role in the resilience of infrastructure by the Cybersecurity Enhancement Act of 2014 and the Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" issued in February 2013.

The NIST Cybersecurity framework is not a maturity model; it is a framework for reducing cybersecurity risk and a tool for aligning policy, business, and technological approaches to managing risk. The diagram shown in Figure 10 depicts the structure of the NIST framework. The five core framework functions on the left of the diagram represent an operational view for dealing with cybersecurity risk.

The categories (i.e., domains) represent organizational functional areas. The subcategories (i.e., practices) divide the categories into technical and managerial activities. The informative references identify applicable standards, best practices, and guidelines. The framework implementation tiers do not represent maturity levels; they represent organizational decisions for investments pertaining to cybersecurity based on the assessment of risks.

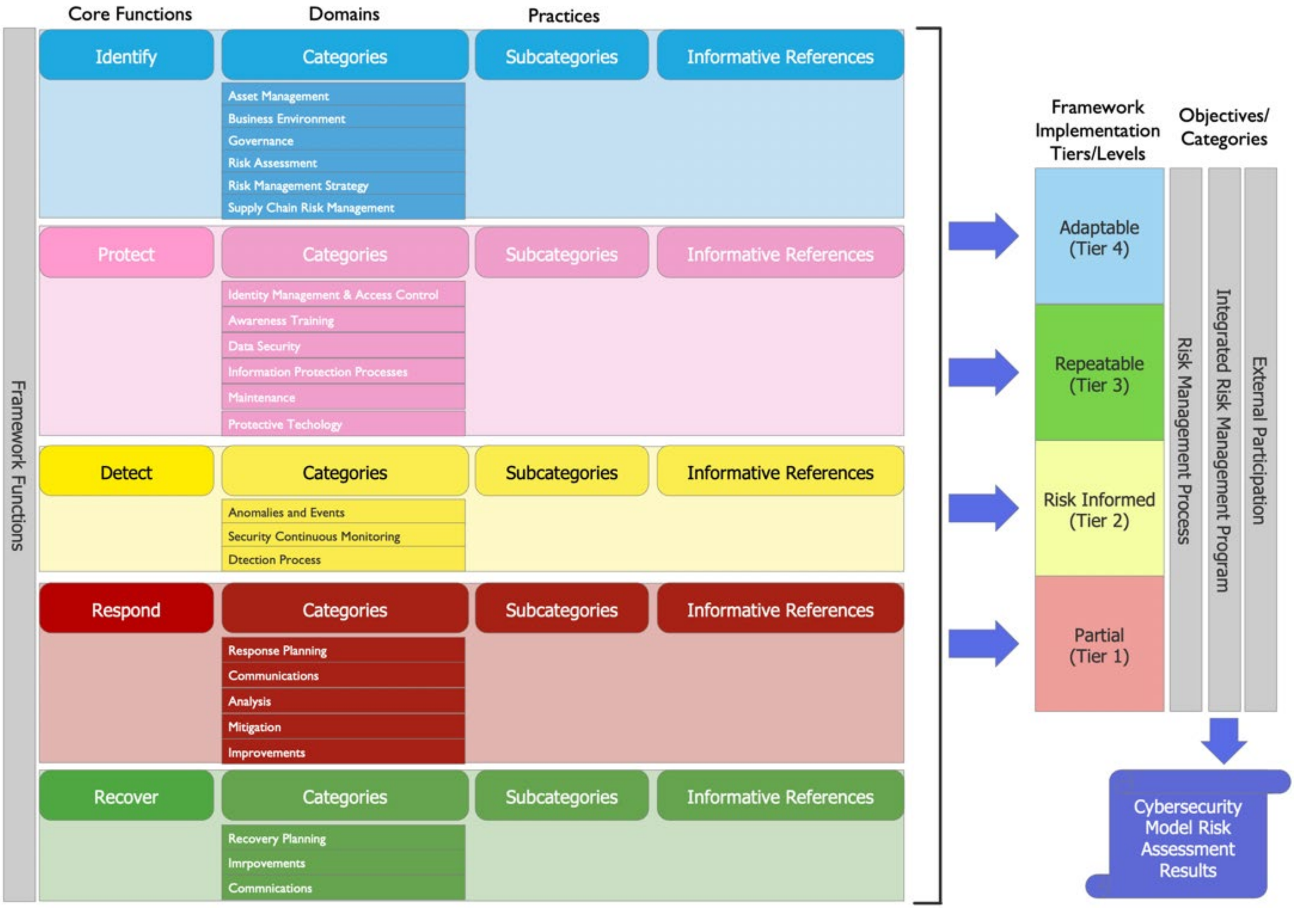
The process for using the NIST framework consists of:

- determining the current cybersecurity posture;
- describing the desired target cybersecurity posture;

[20] CIAS, "*About the Center for Infrastructure Assurance and Security (CIAS)*", CIAS, 2020.
[21] NIST (National Institute of Standards and Technology). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST, 2018.

- performing a gap analysis and defining a roadmap to identify and prioritize the improvements based on the desired framework implementation tier to be achieved; and
- implementation of the roadmap.

Figure 10: NIST – Cybersecurity framework[22]



[22] NIST (National Institute of Standards and Technology). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST, 2018. Illustrative interpretation by author.

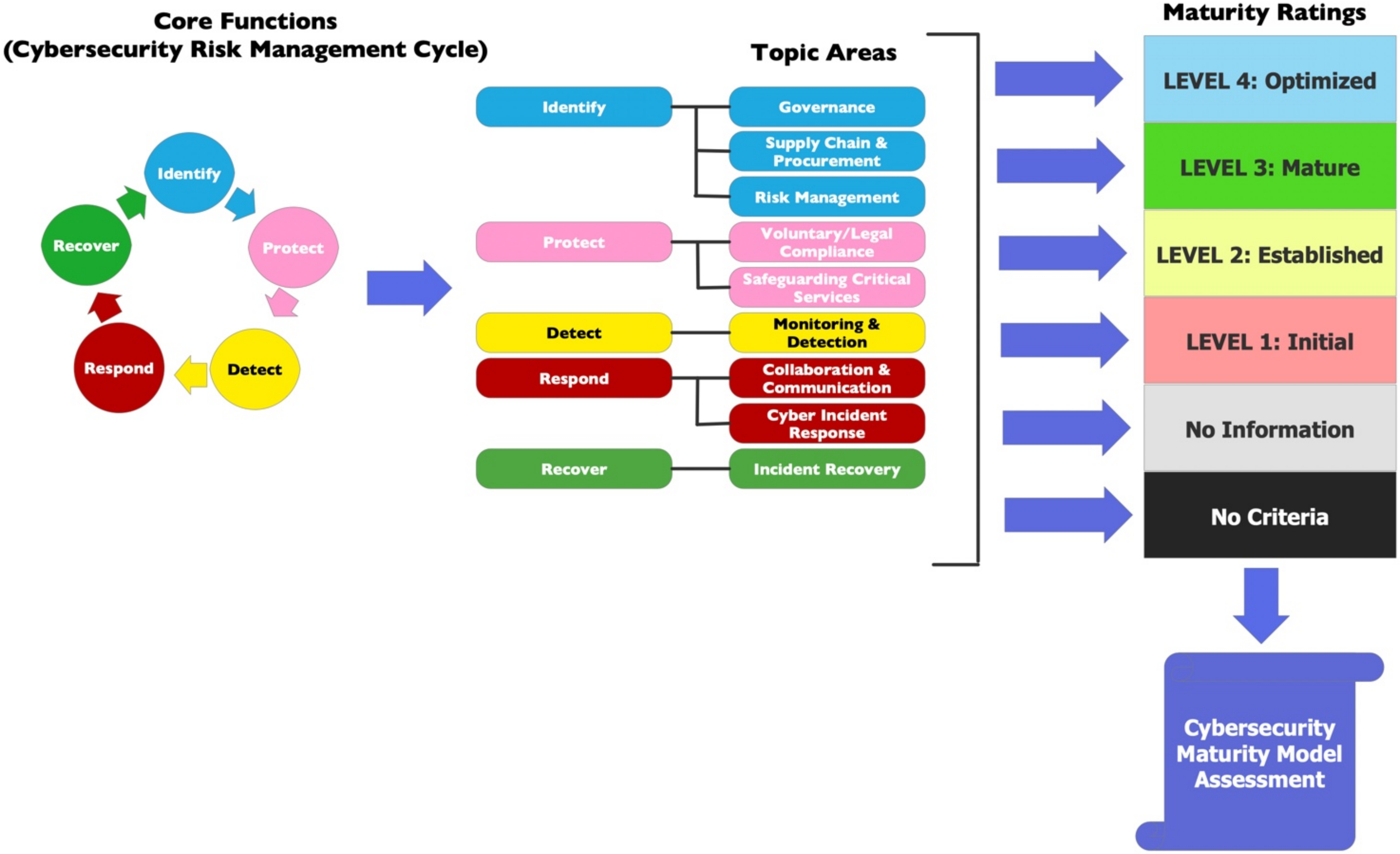
6.4.8 NARUC - Cybersecurity Preparedness Evaluation Tool

The purpose of the NARUC – Cybersecurity Preparedness Evaluation Tool (CPET), issued in June 2019, is to provide regulators with the capability to evaluate the cybersecurity program maturity of utilities. It is intended to complement already existing resources, such as NARUC's "Understanding Utility Cybersecurity Preparedness: Questions for Utilities," and existing maturity models such as C2M2. [23]

The CPET cybersecurity maturity model is shown in Figure 11. Beginning from the left, the CPET model considers the five states of the Core Functions, which are a part of the Cybersecurity Risk Management Cycle. These are mapped onto nine topic areas for evaluation, which are considered the primary capabilities required for a comprehensive cybersecurity posture. Each of the nine topic areas are then addressed for each maturity rating from the perspective of the two maturity level categories: Policy and Plans and Implementation and Operations. The resulting responses across all of the topic areas, maturity levels, policies and plans, and implementation and operations are analyzed to produce the "Cybersecurity Maturity Models Assessment Results."

[23] Cadmus Group, Cybersecurity Preparedness Evaluation Tool. NARUC Center for Partnerships and Innovation. 2019.

Figure 11: NARUC – Cybersecurity Preparedness Evaluation Tool – Cybersecurity Maturity Model[24]



The outcome of a CPET assessment provides the regulator with information that identifies a utility's cybersecurity maturity level.

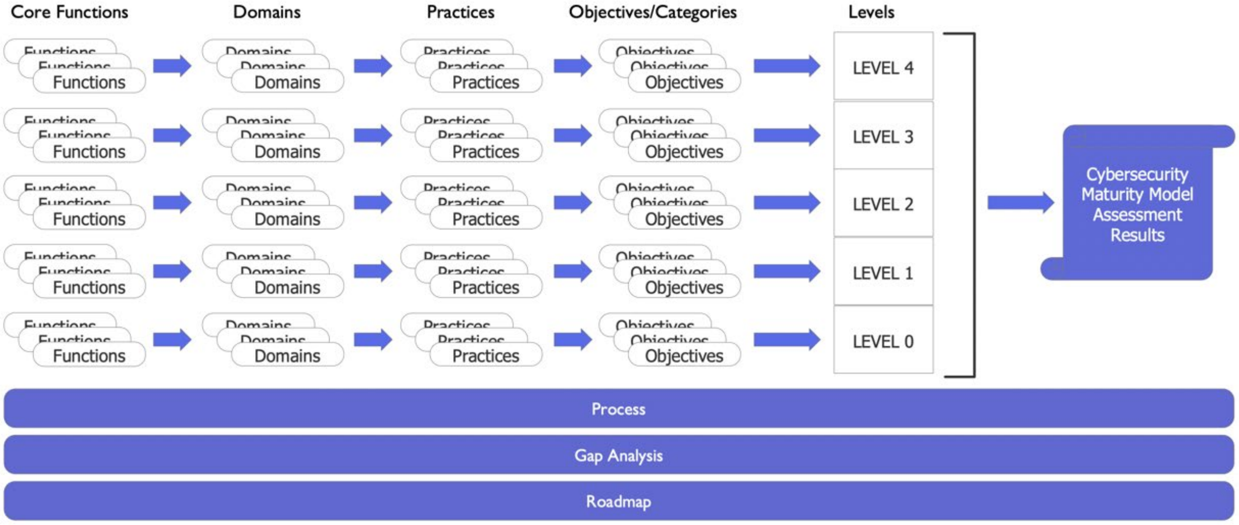
[24] Illustrative interpretation by author. Ibid.

6.5 Maturity Model Comparisons

There are many maturity models in existence today, and none of them is one-size-fits-all maturity model. Each one has been developed for a purpose with a defined input, output, and an associated process for applying the model. When it comes to evaluating the cybersecurity maturity level of a utility, many models could be used, but few are genuinely fit for this purpose. The ideal cybersecurity maturity models suitable for utilities must be considered based on both the utility and the regulator's needs.

Utilities require a cybersecurity maturity model that can assist them in managing and improving their cybersecurity maturity level and, at the same time, be useful to regulators for assessment purposes. This provides both utilities and regulators with a standard and uniform view when using the same cybersecurity maturity model. When comparing models, it is not sufficient to simply consider the purpose and measure of maturity levels, since on the surface they will have many similarities. It is necessary to make a comparison across all aspects of the models. Figure 12 shows the main components of a cybersecurity model. Not all of them apply to every model.

Figure 12: Generic cybersecurity maturity model[25]



Each of these components are defined as follows:

- Core Functions: This comprises the organizational functions that are within the scope of the environment that is being evaluated. These are typically a subset of operations, such as departments within the organization that are able to influence the maturity assessment.
- Domains: This is a logical grouping of practices such as Asset Management, Access Management, Risk Management, Incident Response, Communications, etc.
- Practices: These are the methods that relate to the actions that are repeatedly performed within the scope of the domain that determine a measure of maturity level.
- Objectives/Categories: This is a definition of the expected behavior or results for the designated level.

[25] Marc Levesque, Neos Advisory, July 2020.

- Levels: This is a numeric or descriptive grading of goodness related to maturity.
- Process: This is the approach to perform the maturity level assessment.
- Gap Analysis: This is the analysis of the maturity level assessment against a target goal to establish the differences between the current state and the target state.
- Roadmap: This is a plan that describes an approach to be followed to change the current state to the target state.

Note that the component names used in Figure 12 are for a generic maturity model, and when comparing specific models should be mapped to the specific model definitions.

Table 5 provides a comparison between each of the models. The models developed specifically for use by utilities are the ES-C2M2 and the CPET. The second last column in the table, labelled "Utility," is used to identify the maturity models that have been specifically developed with utilities in mind. This does not preclude the use of other models by utilities and regulators.

Table 5: Cybersecurity maturity model comparison

#	Model	Core Functions	Domains	Practices/ Questions	Objectives/ Categories	Process	Gap Analysis	Roadmap	Utility	Maturity Level
1	CMMI	No	No	No	No	No	No	No	No	4 Levels
2	ES-C2M2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	4 Levels
3	Nemertes	No	Yes	Yes	No	Yes	No	No	No	4 Levels
4	CMMC	No	Yes	Yes	No	Yes	Yes	Yes	No	5 Levels
5	ISO21827	No	Yes	Yes	No	Yes	No	No	No	5 + 1 Levels
6	CCSMM	No	Yes	No	Yes	No	No	Yes	No	5 Levels
7	NIST	Yes	Yes	Yes	Yes	Yes	No	No	No	4 Levels
8	CPET	Yes	Yes	Yes	Yes	Yes	No	No	Yes	4 + 2 Levels

6.6 Maturity Model Benefits

Cybersecurity is a major influencing factor in the operation of utilities, and cybersecurity oversight forms an important part of a regulator's duties. Due to the complexity and continuous evolution of cybersecurity, regulators require tools to help them deal with this subject. Cybersecurity maturity models can fill this need because these models provide regulators with the ability to review cybersecurity assessment results without being cybersecurity experts.

Cybersecurity maturity models accomplish this with a well-structured approach. Regulators can engage a utility by assessing its cybersecurity posture based on an already developed set of strategic questions that the regulator is free to tailor to meet the goals of each assessment.

The structure of the cybersecurity maturity model ensures that all relevant cybersecurity areas are covered and that the collected information is well-structured for analysis to determine the organization's cybersecurity maturity level. Additional model benefits derived from its structure are the ability to leverage past assessments' results to monitor for cybersecurity behavior trends on the part of the utility and to coordinate with the utility to determine where improvements are needed.

By consistently applying the cybersecurity maturity model across multiple utilities, it provides the regulator with a powerful tool to identify trends within the industry and pull together the necessary data to support making regulatory changes. In order to be useful, the cybersecurity maturity model must provide value and benefits to the regulator.

7 Using Maturity Model Assessment Results in Regulatory Practice

The use of Cybersecurity Maturity Model assessment results for purposes of regulatory practice requires that the information gathered from the utility be captured following good record-keeping practices. Before implementing the assessment, an appropriate level of preparation and planning must be done. ISO19011, "Guidelines for Auditing Management Systems," outlines preparations guidelines for assessments.

After completing the engagement with the utility, the collected information is analyzed to summarize findings and determine the utility's cybersecurity maturity level.

7.1 Prepare a cybersecurity maturity level assessment

Thorough preparation for a cybersecurity maturity level assessment will help maximize the benefits. Preparation should consist of the following steps:

- review past assessments to assist with tailoring the questions for the upcoming assessment;
- review of past and recent incidents and associated responses and corrective action;
- establish the objectives of the upcoming assessment, based on the outcome of past assessments;
- Determine the legal requirements regarding the treatment of the information provided by the utility. Ensure that the regulatory agency can comply with these legal requirements and inform the utility;
- identify the regulatory resources that will be needed, such as cybersecurity experts, note-taking support, policies, and standards;
- identify the utility resources that will be needed, such as staff, documents, evidence, and inspections;
- define an agenda and a schedule with a defined timeline to ensure that the utility staff are aware of what is expected; and
- inform the utility to ensure their awareness of the assessment.

Challenges that can arise when performing a cybersecurity maturity assessment include:

- The utility may not want to share information which they feel is confidential, and must be keep secret for security reasons. This makes it challenging to perform any cybersecurity maturity assessment. Establishing Non-Disclosure Agreements (NDAs) is a possible way around this.
- Legislative constraints that require the public disclosure of any gathered information into the public domain, such as with the U.S. Freedom of Information Act (FOIA). The impact is that information, therefore, becomes available to cyber-attackers, unless the jurisdiction has a Critical Infrastructure Confidentiality Statute. For this reason, cybersecurity maturity models leveraged by regulators must be capable of determining the cybersecurity posture of a utility organization without compromising this posture.

7.2 Implement a cybersecurity maturity level assessment

At the start of the assessment implementation with the utility, it is important to:

- confirm the assessment objectives and the scope with the utility;
- confirm the availability of the expected utility resources; and
- Review the legal requirements regarding the treatment of the information provided by the utility and explain the manner in which the collected information will be managed by the regulator.

Once the assessment begins, gather the information based on the established cybersecurity maturity model assessment process. Information that is provided must be verifiable and cannot be hearsay. The information can consist of:

- written documents;
- photographs and videos;
- inspections;
- demonstrations; and
- verbal explanations.

The details of each piece of information provided should be recorded in the assessment minutes, along with any impressions or other observations that are made when examining the information. It is important to make note of any information that the utility objects to, providing the reason for the objection.

As the assessment is progressing, collected information that leads to assessment findings should be flagged. If any new or changed circumstances are noticed, these should be addressed.

When collecting information, only verifiable information should be accepted as assessment evidence. For this reason, it is important to tag or note in the minutes any collected information that is verifiable. Non-verifiable information can also be recorded, but it should not carry any weight during the assessment.

7.3 Analyzing and interpreting the collected information

Analysis of the collected information is done after the information collection session with the utility has been completed, and any verifiable information is evaluated against the assessment criteria. As a part of the analysis, the following would be considered:

- the cybersecurity maturity level criteria of the model;
- the past results of the utility; and
- the state of other comparable utilities.

7.4 Influencing the regulatory process

Cybersecurity maturity models can be very beneficial to the regulatory process for both regulators and utilities, as digitization has made cybersecurity a critical function that impacts all aspects of a utility's operations.

When considering the cybersecurity maturity level of a utility, the domain drivers for each level and how they relate to the utility's cybersecurity posture need to be understood. Cybersecurity is a significant initiative for utilities, and achieving an increase in maturity level can be very challenging, requiring substantial investment and effort. The cost of attaining an increased cybersecurity maturity level can be cost prohibitive for some utilities.

The regulatory process can be used to incentivize and motivate utilities to achieve and maintain a designated cybersecurity maturity level. To support the decision-making during the regulatory process, the cybersecurity maturity level information can be used to:

- Monitor the cybersecurity posture of individual utilities:
    - How does a utility measure up against expectations?
    - Is the utility trending in the direction of improvement or degradation?
    - What are the most challenging cybersecurity initiatives for utilities to achieve without legislative or regulatory support?
- Monitor the cybersecurity of posture of groups of utilities:
    - the average, minimum, maximum and median cybersecurity maturity level of groups of utilities
    - As a group, are utilities trending towards improvement?

The data gathered in support of these points provides tangible, irrefutable data to assist in guiding the regulatory process with regards to cybersecurity. Regulators are able to use the assessment results to make well informed regulatory decisions, which greatly benefit the energy sector by helping to make it more secure and resilient.

8 Summary

Cybersecurity maturity models are a useful tool for regulators to measure the cybersecurity readiness of utilities and compare this level of preparedness against a target baseline and the cybersecurity maturity level of other utilities. Cybersecurity maturity model assessments should be performed at least on a quarterly or biannual basis in order to be effective. However, they can be performed monthly if the regulator feels that there is a need for a utility to demonstrate an improvement in its cybersecurity posture or in the presence of an elevated national threat level to ensure that critical infrastructure protections are in place.

The cybersecurity posture and maturity level of a utility cannot be changed overnight. It is something that evolves. A cybersecurity maturity model provides regulators with a tool to measure and monitor the magnitude and the associated rate of change in maturity level over time by collecting a significant amount of information on each utility. This information allows for trends to be monitored on a per-utility basis and also across multiple utilities. This trending information can then prove to be invaluable in establishing pertinent cybersecurity regulations that are meant to ensure cybersecurity trends do not go in the wrong direction and can assist in providing the tracking of standard metrics related to cybersecurity.

When using cybersecurity maturity models, regulators must realize that the models are merely representations of the real world and not the real world itself. Therefore, they must be cognizant of the accuracy of the model. By having a good understanding of the strengths and weaknesses of cybersecurity maturity models, the regulator can use the model to benefit the utility and its customers.

Eight cybersecurity maturity models have been examined. From the regulatory perspective, they are not all suitable for assessing utilities, and only two of the models have been specifically designed for the electricity utility market: ES-C2M2 and CPET.

9 Bibliography

Cadmus Group. 2018. *Cybersecurity Strategy Development Guide*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204. (Jul 2020) (based on the USAID Black Sea Cybersecurity Strategy Development Guide)

Cadmus Group. 2019. *Cybersecurity Preparedness Evaluation Tool*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0. (Jul 2020)

Christopher, Jason D., Fowad Muneer, John Fry, and Paul Skare. 2014. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - Version 1.1*. Washington DC: U.S. Department of Energy. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf. (Jul 2020)

CIAS. 2020. *"About the Center for Infrastructure Assurance and Security (CIAS)"*. CIAS. https://cias.utsa.edu/the-ccsmm.html. (Jul 2020)

Costantini, Lynn P., and Matthew Acho. 2019. *Understanding Cybersecurity Preparedness: Questions for Utilities*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220. (Jul 2020)

Costantini, Lynn P., and Matthew Acho. 2019. *Cybersecurity Manual – Cybersecurity Glossary*. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/7932B897-CF16-0368-BF79-EDC5C5A375EE. (Jul 2020)

CMMI Institute. 2019. "What is CMMI?". CMMI, https://cmmiinstitute.com/cmmi/intro. (Jul 2020)

DoD. 2020. Department of Defence (DoD) Cybersecurity Maturity Model Certification (CMMC). DoD. https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf. (Jul 2020)

ISO (International Standards Organization). 2018. *ISO 19011:2018 Guidelines for auditing management systems*. ISO. https://www.iso.org/standard/70017.html. (Jul 2020)

ISO (International Standards Organization). 2013. *ISO 27001:2013 Information Technology – Security techniques – Information security management systems - Requirements*. ISO. https://www.iso.org/standard/54534.html. (Jul 2020)

ISO (International Standards Organization). 2008. *ISO 21827:2008 IT – Systems Security Engineering – Capability Maturity Model (SSE-CMM)*. ISO. https://www.iso.org/standard/44716.html. (Jul 2020)

Johnson, J.T. 2019. *"Cybersecurity maturity model lays out four readiness levels"*. TechTarget SearchSecurity. https://searchsecurity.techtarget.com/tip/Cybersecurity-maturity-model-lays-out-four-readiness-levels. (Jul 2020)

Kellep, C., Williams, A. 2020. Understanding Cybersecurity Maturity Model Certification (CMMC), Security Boulevard. https://securityboulevard.com/2020/01/understanding-cybersecurity-maturity-model-certification-cmmc/. (Jul 2020)

Keogh M., Thomas S. 2017. Cybersecurity. A Primer for State Utility Regulators. Version 3.0. NARUC Center for Partnerships and Innovation. https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F. (Jul 2020)

NARUC. 2017. *Cybersecurity Evaluative Framework for Black Sea Regulators*. NARUC. https://pubs.naruc.org/pub.cfm?id=E3CE75B5-155D-0A36-31FD-1B268F7BD125. (Jul 2020)

NARUC. 2020. *Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards*. NARUC. https://pubs.naruc.org/pub.cfm?id=C3597EE6-155D-0A36-31AC-3F82F33A665B. (Jul 2020)

Nemertes 2017. *The Nemertes Security Maturity Model*. Nemertes Research. https://nemertes.com/research/nemertes-security-maturity-model/. (Jul 2020)

NIST (National Institute of Standards and Technology). 2018. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST. https://www.nist.gov/cyberframework/framework. (Jul 2020)

SEI (Software Engineering Institute). November 2010. *CMMI for Development, Version 1.3*. Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf. (Jul 2020)

For questions regarding this publication, please contact
Erin Hammel (ehammel@naruc.org).

National Association of Regulatory Utility Commissioners (NARUC)
1101 Vermont Ave, NW, Suite 200
Washington, DC 20005 USA
Tel: +1-202-898-2210
Fax: +1-202-898-2213
www.naruc.org