NARUC

National Association of Regulatory Utility Commissioners

Cybersecurity Preparedness Evaluation Tool

The Cadmus Group LLC

June 2019

Acknowledgments

This report was developed under the project "State and Local Innovation and Analysis in Support of Long-Term Energy Planning and Policy," of the National Association of Regulatory Utility Commissioners (NARUC) Center for Partnerships & Innovation. This material is based on work supported by the U.S. Department of Energy under Award Number DE-OE0000818.

Throughout the preparation process, state commissioners and staff provided NARUC with editorial comments and suggestions. However, the views and opinions expressed herein may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to:
Kate Marks, Kirsten Verclas, Victor Calderon, and Jeff Hood, U.S. Department of Energy
Dominic Saebeler and Wei Chen Lin, Illinois Commerce Commission
Hon. Jay Scott Emler, Kansas Corporation Commission
Morris Schreim, Maryland Public Service Commission
Dan Searfoorce and David Alexander, Pennsylvania Public Utility Commission
Hon. Ann Rendahl and Jason Ball, Washington Utilities Commission
Jeff Pillon, National Association of State Energy Officials
David Batz and Ivy Lyn, Edison Electric Institute
Lynn P. Costantini and Matthew Acho, NARUC

Please direct questions regarding this report to Lynn P. Costantini, Deputy Director, NARUC Center for Partnerships and Innovation, at lcostantini@naruc.org or Matthew Acho, Program Officer at macho@naruc.org.

Table of Contents

Preface

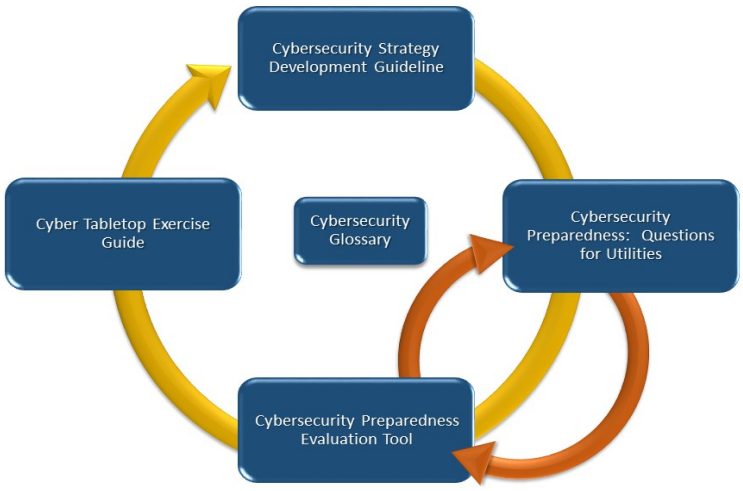
NARUC has developed a comprehensive suite of resources, collectively referred to as the Cybersecurity Manual, to help public utility commissions (PUCs or "commissions") gather and evaluate information from utilities about their cybersecurity risk management practices. These evaluations facilitate well-informed PUC decisions regarding the effectiveness of utilities' cyber security preparedness efforts and the prudence of related expenditures.

The Cybersecurity Manual is comprised of five complementary resources. The *Cybersecurity Preparedness Evaluation Tool (CPET)* is one of them. A brief description of each resource follows.

1. ***Cybersecurity Strategy Development Guide* | 2018**
   The Strategy Development Guide defines a roadmap that PUCs can follow to design and implement a structured approach for long-term engagement with utilities on cybersecurity matters. The Guide includes examples from PUCs that demonstrate the process steps and highlights practices that drive successful outcomes.
2. ***Understanding Cybersecurity Preparedness: Questions for Utilities* | 2019**
   The Questions for Utilities provides a set of comprehensive, context-sensitive questions that PUCs can ask of a utility to gain a detailed understanding of its current cybersecurity risk management program and practices. The questions build upon and add to those included in prior NARUC publications.
3. ***Cybersecurity Preparedness Evaluation Tool (CPET)* | 2019**
   The CPET provides a structured approach for PUCs to use in assessing the maturity of a utility's cybersecurity risk management program and gauging capability improvements over time. The CPET is designed to be used with the *Questions for Utilities* on an iterative basis to help PUCs identify cybersecurity gaps, spur utilities' adoption of additional mitigation strategies, and inform cybersecurity investment decisions.
4. ***Cybersecurity Tabletop Exercise (TTX) Guide* | 2019**
   This guide details the steps that PUCs can take to design and execute an exercise to examine utilities' and other stakeholders' readiness to respond to and recover from a cybersecurity incident. It includes exercise scenarios and examples.
5. ***Cybersecurity Glossary* | 2019**
   The *Glossary* contains cybersecurity terms used throughout the Cybersecurity Manual, as well as "terms of art" that utilities may use during discussions with PUCs.

Resources within the Cybersecurity Manual can be used individually but are designed to work together. NARUC's intent is to provide a comprehensive set of assessment tools that, when applied, provide a consistent, complete view of utilities' cybersecurity preparedness. **Figure 1** depicts the complementary, process-oriented relationship among these components.

Figure 1: NARUC Cybersecurity Manual Components



The content of each component in the Cybersecurity Manual is customizable to meet specific goals, objectives, and requirements that PUCs have established around cybersecurity, complementing resources developed by and for utilities and other practitioners. Geared toward non-technical, policy-oriented users, each component captures information in sufficient detail to support PUC decision making.

1. Introduction

As cyberattacks against the critical infrastructure sector have increased over the years, the National Association of Regulatory Utility Commissioners (NARUC) has engaged with utilities and state PUCs to determine how best the regulatory community can support the growth of strong, mature cybersecurity practices. Several tools and resources, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the U.S. Department of Energy (DOE) C2M2, have been developed to help entities identify their cybersecurity vulnerabilities and understand their level of cybersecurity maturity and resilience. However, feedback from NARUC working groups and interviews consistently reveal that many PUCs do not have access to the resources and technical knowledge necessary to apply highly technical tools like the C2M2. As such, NARUC developed a cybersecurity manual, aligned to cybersecurity standards and industry best practices, that is tailored to the needs and unique environment of PUCs. By helping commissions understand their unique cybersecurity needs and familiarizing PUC staff with effective practices, the cybersecurity manual promotes a higher cybersecurity baseline, and will allow for the future development of cybersecurity capabilities and the application of robust cybersecurity models.

NARUC developed the CPET as part of the Cybersecurity Manual to help PUCs evaluate the level of cybersecurity preparedness of utilities within their jurisdictions. PUCs have oversight responsibility within their jurisdictions to ensure that utilities are reliably delivering key services (e.g., water, natural gas, electricity) to their customers. Commissions can most effectively accomplish this when they have a thorough understanding of their utilities' cybersecurity preparedness efforts and capabilities. The CPET helps provides PUCs with a valuable tool to work with utilities to confirm that they have the appropriate plans and policies ready, have safeguarded their information technology (IT) and operational technology (OT) systems, and have the right personnel and stakeholder relationships in place before an incident occurs to effectively respond and recover as quickly as possible.

2. Purpose

The CPET provides commissions with a simple, easy to apply tool to evaluate utilities' cybersecurity program maturity. By regularly engaging with utilities (e.g., annually, semi-annually) using the *Questions for Utilities* and analyzing the information received using the CPET, commissions can assess the year-over-year change in cybersecurity preparedness of individual utilities within a PUC jurisdiction, promote continuous improvement, and increase the overall awareness and visibility of cybersecurity preparedness and resilience across the utility landscape within their states.

The CPET helps commissions understand an individual utility's cybersecurity preparedness and maturity over time.

How is cybersecurity preparedness different from cybersecurity resilience?

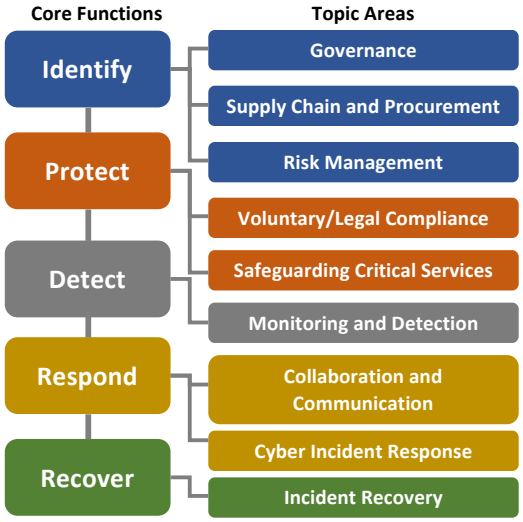
Preparedness and resilience are concepts that are closely linked. **Cybersecurity preparedness** refers to any actions, such as developing and exercising plans or training and equipping personnel, that contribute to an organization's readiness and ability to respond to or recover from an incident affecting its IT or OT systems. **Cybersecurity resilience** refers to an organization's ability to continue delivering services during a cybersecurity incident or quickly resume services following a cybersecurity incident. In this way, strong cybersecurity resilience is typically a product of effective cybersecurity preparedness.

Using the CPET, commissions can process a utility's answers to the *Questions for Utilities* against established criteria and assign a maturity level based on their assessments of the qualitative data inputs that the answers provide. The results provide valuable insights for both regulatory industry oversight and utility capability improvements. Although the *Questions for Utilities* and the CPET were designed to be complementary, the CPET may also be used independently, provided that commissions have access to data that can inform the evaluation (e.g., the commission has its own set of cybersecurity questions).

The intention of the CPET is to enable PUCs to understand an individual utility's cybersecurity preparedness and maturity over time, and evaluate them against generally accepted standards, best practices, and the utilities' identified needs. However, the CPET should not be used to compare one utility's preparedness or maturity level against another, as the operating environment and resource availability for each utility is unique and does not lend to a one-to-one comparison.

The CPET does not prescribe a specific approach, and this flexibility accommodates a wide range of different cybersecurity practices. The specific needs of each utility differ and, as such, each utility should adopt the cybersecurity practices that best fit its unique circumstances. For example, utilities should build a network of IT and OT systems appropriate for their environment, considering their size and available resources.

Figure 2:
CEPT Core Functions and Topic Areas



3. Overview

The CPET is compatible with NARUC's *Understanding Utility Cybersecurity Preparedness: Questions for Utilities*, another component of the NARUC Cybersecurity Manual. Both the *Questions for Utilities* and the CPET explore activities and capabilities across traditional cybersecurity risk management process steps—Identify, Protect, Detect, Respond, and Recover—from the NIST CSF, which are relevant to both IT and OT assets. Within these five core functions, the CPET further identifies nine topic areas for evaluation. Within these streamlined topic areas are specific evaluation criteria established to reduce subjectivity and enable commissions to gain a nuanced understanding of a utility's cybersecurity maturity.

The topic area criteria for evaluation are divided into the same two categories as in the *Questions for Utilities*:

1. **Policy and Plans**
   The Policy and Plans questions and criteria aim to identify (and understand) the extent to which utilities have documented the processes and activities they will undertake to ensure cybersecurity resilience.
2. **Implementation and Operations**
   The Implementation and Operations questions and criteria aim to identify (and understand) the degree to which utilities have followed through with the policies, processes, and plans they have developed.

Commission staff can assess both categories during a single evaluation or assess them separately. If a commission elects to assess both categories at the same time, it will result in two maturity levels for each topic area. Having insight into the two distinct categories is beneficial for PUCs over the long term, as those maturity levels will allow more targeted discussions with the utility in the future

How is the CPET different from other maturity models, and what are the benefits?

- NARUC does not intend for the CPET to be a replacement for other established tools, including C2M2 developed by DOE. Rather, the CPET is a complement to the library of resources that already exists and fulfills a current need identified by PUCs for a high-level tool to understand a utility's current level of cybersecurity program maturity.
- By focusing on key subject areas, the goal is to help maximize commissions' understanding of utilities' cybersecurity preparedness without diving deeply into technical matters. By separating policy from implementation, the CPET takes a flexible approach to cybersecurity assessments that enables evaluators to focus on cybersecurity elements that are most familiar to them.
- The CPET does not require the same level of technical detail as other current cybersecurity models and frameworks.
- By focusing only on the aspects of cybersecurity most important to commissions, completing an assessment using the CPET is likely to be less resource intensive on both the Commission and the utility than assessments using other maturity models.
- The CPET is intended to provide an assessment of the overall utility, whereas DOE's C2M2 may be used to assess operational areas such as generation, transmission, or distribution operations separately.
- Use of the CPET is voluntary; PUCs can instead use DOE's C2M2 or other resources to categorize a utilities' responses to their questions as they desire.

4. CPET Structure

The CPET draws on industry best practices, such as the NIST CSF and C2M2, to outline six different maturity levels related to a utility's cybersecurity preparedness. These maturity levels include options for utilities that do not conduct cybersecurity activities and those that do not elect to share information, as well as four distinct maturity levels that describe a utility's capabilities—No Criteria, No Information, Level 1: Initial, Level 2: Established, Level 3: Mature, and Level 4: Optimized (see **Section 5. CPET Implementation**). Commission staff can review a utility's response to the *Questions for Utilities*—or other information available to the commission—and determine which maturity level best describes the utility based on the criteria provided in the CPET (see **Section 6. CPET Criteria**).

4.1 Core Functions and Topic Areas

Both the *Questions for Utilities* and the CPET use the five core functions of cybersecurity risk management—Identify, Protect, Detect, Respond, and Recover—as a foundation. The CPET divides the five core functions into more specific topic areas, allowing commissions to gain a more granular appreciation of utilities' capabilities and track specific capabilities over time. The topic areas evolved from NARUC's previous evaluative framework tool and are consistent with, and informed by, widely accepted cybersecurity standards such as the NIST CSF, the North American Electricity Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, and International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) standards. The topic areas outline the primary capabilities required for comprehensive cybersecurity practice. **Table 1: Definitions** identifies the five core functions and nine topic areas outlined in the CPET.

Table 1: CPET Core Functions and Topic Area Definitions

Core Functions	Topic Areas	Definition
IDENTIFY	**Governance**	Identify and document the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements and inform the management of cybersecurity risk.
	Supply Chain and Procurement	Identify critical IT and OT assets (e.g., hardware, software, data); document the utility's priorities, tolerance, and constraints related to procurement, supply chain risk, and impact of a compromise of these assets; and establish and maintain controls to manage risks associated with the utility's dependencies on external entities.
	Risk Management	Identify and document cybersecurity risks, assess and manage their anticipated consequences, and prioritize activities to address them in a manner that aligns with the needs of the organization.
PROTECT	**Voluntary/Legal Compliance**	Maintain and document the procedures and processes necessary to support compliance of cybersecurity activities with applicable standards, laws, regulations, and requirements, and best practices, including NERC CIP, NIST CSF, and ISO/IEC standards.
	Safeguarding Critical Services	Develop and implement appropriate policies and protections suggested by the Risk Management assessment to ensure the security and resilience of information and operational systems and assets and safeguard against a loss of confidentiality, availability, or integrity.
DETECT	**Monitoring and Detection**	Develop and implement activities to collect, monitor, and analyze information related to cybersecurity to enable the timely discovery of cybersecurity threats, such as detection of unauthorized changes to the configuration of assets or failure of security systems.
RESPOND	**Collaboration and Communication**	Establish and maintain relationships with internal and external stakeholders across the cybersecurity domain and create a network for information and intelligence sharing to effectively communicate threats and vulnerabilities, response activities, and lessons learned.
	Cyber Incident Response	Develop and implement activities to address a detected cybersecurity incident, support the ability to contain the impact, limit the potential damage, and manage the consequences of a cyber incident.
RECOVER	**Incident Recovery**	Develop and implement activities to maintain plans for resilience and business continuity, support timely recovery to normal operations, and implement corrective actions through after-action review, and use lessons learned to reduce the impact from a cybersecurity incident and improve policies, plans, and procedures.

5. CPET Implementation

As discussed in NARUC's *Cybersecurity Primer*, the recommended process for evaluating a utility's cybersecurity includes a verbal interview during which a commission can use the *Questions for Utilities* as a guide for topics to cover and questions to ask. A utility is likely to share more detailed information in a setting such as an in-person interview or meeting where no notes or records are kept as opposed to providing written responses, due to security concerns related to sensitive information-sharing. Further, if a commission can engage with utilities on cybersecurity as a discrete issue, separated from a regulatory proceeding, the PUC is likely to get more complete information.

Many PUCs have found they are able to get more contextual information by holding meetings on utility premises to avoid taking possession of the information and possibly exposing it to public disclosure. Commission staff delivering the interview may consider bringing a CPET into this type of meeting, in addition to the *Questions for Utilities* document, to help guide the conversation and prompt clarifying questions. If the arrangements of the meeting include a no note-taking provision, NARUC recommends completing the CPET for the relevant topic areas as soon as possible following the interview to maximize the amount of information retained from the interview process. Regardless of how the commission engages the utility, the most important aspect of implementation is that the commission applies the CPET using a consistent approach.

5.1 Maturity Levels

The CPET establishes maturity levels that describe a utility's capabilities and options for utilities that either do not meet any criteria or do not share information with the PUC (see **Table 2**).

Table 2: CPET Maturity Ratings

Maturity Rating	Definition
No Criteria	The utility does not have any policies or plans related to this topic or does not conduct any technical activities related to this topic.
No Information	The utility has not shared sufficient information and, as such, the commission is unable to assign a maturity level.
LEVEL 1: Initial	The utility's practices are informal, uncoordinated, and/or ad hoc and display limited awareness with little or no internal or external coordination.
LEVEL 2: Established	The utility's practices meet minimum resource requirements, are organized to address a strategic need or specific guidance, and may align to an established strategy approved by management with informal information sharing and coordination.
LEVEL 3: Mature	The utility's practices are formally defined, organized, and regularly updated across the organization; prioritized according to needs; adequately resourced, incorporate industry best practices, and are championed by leadership.
LEVEL 4: Optimized	The utility's practices are proactive, informed by objective feedback, embody a culture of continuous improvement, reviewed, and adapted regularly based on lessons learned, and can serve as industry best practices.

Criteria for each maturity level are divided into two categories: 1) Policy and Plans and 2) Implementation and Operations. For each of the evaluated topic areas, the categories within have distinct evaluation criteria (see **Section 6**). Commission staff can review the topic area categories using the responses to the *Questions for Utilities*—or other information as appropriate—and assign a maturity level to each category individually. Because the categories are independent of each other, the commission staff may assign different levels to each topic area category.

5.2 Evaluation Guidelines

The maturity levels are designed to build upon one another. The criteria for each level represent an ascending level of maturity. The criteria serve as a guide to help evaluators make an informed decision regarding the level of maturity for each category. However, the final determination of the maturity level is up to the evaluator's discretion.

During the CPET evaluation process, the commission staff evaluating the utility can use their judgement when assigning the category-specific level of maturity to the utility, but may use the following recommendations as a guideline to help inform their decision:

- If a utility meets all of the criteria for a level, but none of the criteria for the next level, it is recommended that the utility be assigned the lower maturity level with fully met criteria.

  An example is provided in the "Policy and Plans" column in **Table 3**. The utility has addressed all criteria for Level 1 and Level 2, but none of the criteria for Level 3 or Level 4. Therefore, the recommended maturity level is Level 2: Established.

Table 3:
Sample Topic Area Evaluation

Governance		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
✓ Criteria 1 ✓ Criteria 2	**Level 1: Initial**	✓ Criteria 1 ✓ Criteria 2
✓ Criteria 1 ✓ Criteria 2	**Level 2: Established**	✓ Criteria 1 ✓ Criteria 2
– Criteria 1 – Criteria 2	**Level 3: Mature**	✓ Criteria 1 – Criteria 2
– Criteria 1 – Criteria 2	**Level 4: Optimized**	– Criteria 1 – Criteria 2

Level 2: Established	Recommended Level	**Level 2: Established** or **Level 3: Mature**

- If a utility meets some, but not all, criteria, in a level, the commission staff can use their discretion to determine the appropriate maturity level.

  An example is provided in the "Implementation and Operations" column in **Table 3**. The utility has addressed all criteria in Level 1 and Level 2 and some of the criteria in Level 3. In this instance, the recommended maturity level is either a Level 2 or a Level 3 and the commissioner or staff must make an informed judgment and assign a maturity level based on the information they have.

However, the criteria are not exhaustive, and the evaluator is encouraged to consider all available information related to the category and topic area when they make their assessment. In some instances, evaluators may have information that does not fit the specific criteria outlined in the CPET. In those instances, the evaluator may assign a maturity level higher or lower based on their best assessment of the situation.

The final determination of the maturity level is up to the evaluator's discretion.

6. CPET Criteria

Completing the entire CPET will result in two separate maturity levels for each topic area, totaling 18 different ratings.

The following subsections outline the specific criteria for each topic area. Evaluators are encouraged to read all criteria and assess the utility within the context of the utility's responses to the *Questions for Utilities* (or other information, as appropriate) and determine a maturity level for both "Policy and Plans" and "Implementation and Operations" based on the guidance provided in the previous sections. As such, completing the entire CPET will result in two separate maturity levels for each topic area, totaling 18 different ratings (see **Table 4**).

Table 4: Sample Complete CPET Evaluation

Topic Area	Policy and Plans	Implementation and Operations
Governance	LEVEL 1: Initial	LEVEL 2: Established
Supply Chain and Procurement	LEVEL 2: Established	LEVEL 3: Mature
Risk Management	LEVEL 4: Optimized	LEVEL 4: Optimized
Voluntary/Legal Compliance	No Information	No Criteria
Safeguarding Critical Services	LEVEL 3: Mature	LEVEL 2: Established
Monitoring and Detection	LEVEL 4: Optimized	LEVEL 3: Mature
Collaboration and Communication	LEVEL 2: Established	LEVEL 2: Established
Cyber Incident Response	LEVEL 1: Initial	No Criteria
Incident Recovery	No Information	LEVEL 2: Established

6.1 IDENTIFY: Governance

Identifying and documenting the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements and inform the management of cybersecurity risk.

Evaluation Criteria: Governance		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Has plans and policies within its IT or security department that assign responsibilities for cybersecurity. ❑ Has dedicated security policies that govern IT and OT systems.	**LEVEL 1: Initial**	❑ Staffed with part-time or multi-duty individuals to manage cybersecurity and does not have a dedicated budget.
❑ Has a cybersecurity plan or strategy that includes an organizational structure stretching beyond IT and/or security departments that outlines the roles and responsibilities related to cybersecurity and information protection.	**LEVEL 2: Established**	❑ Minimally staffed or resourced with budgeted full-time cybersecurity professionals and associated expenses.
❑ Regularly reviews, updates, and improves its cybersecurity plan, strategy, and other governance. ❑ Identifies relevant external stakeholders for cybersecurity events and effectively coordinates cybersecurity roles and responsibilities with external partners.	**LEVEL 3: Mature**	❑ Fully staffed or resourced with budgeted full-time employees who understand the technical, legal, and regulatory requirements regarding cybersecurity.
❑ Identifies a clear policy for incorporating senior leadership during a cybersecurity incident, meeting pre-identified thresholds, and has clearly outlined their roles and responsibilities with respect to providing strategic support for incident response activities.	**LEVEL 4: Optimized**	❑ Senior leadership is actively engaged with cybersecurity activities by championing budgets, taking ownership of plans and policies, and/or regularly meeting to discuss the utility's cybersecurity posture.

6.2 IDENTIFY Supply Chain and Procurement

Identifying and documenting critical IT and OT assets (e.g., hardware, software, data), the utility's priorities, tolerance, and constraints related to procurement, supply chain risk, and impact of a compromise of these assets, as well as establishing and maintaining controls to manage risks associated with the utility's dependencies on external entities.

Evaluation Criteria: Supply Chain and Procurement		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Identifies IT and OT supplier dependencies and associated risks. ❑ Identifies customer dependencies and associated risks.	**LEVEL 1: Initial**	❑ Prioritizes vendors based on the utility's demonstrated needs and input from cybersecurity professionals. ❑ Maintains, and periodically updates, a basic inventory of assets.
❑ Establishes criteria for assessing and prioritizing dependencies. ❑ Considers cybersecurity requirements related to vendor relationships. ❑ Establishes policies to protect assets and sensitive information.	**LEVEL 2: Established**	❑ Considers vendors' and suppliers' potential cybersecurity risks when sourcing materials or personnel. ❑ Maintains an active, updated inventory of deployed assets.
❑ Documents policies that guide procurement activities and adhere to specific standards, guidelines, and/or best practices.	**LEVEL 3: Mature**	❑ Includes cybersecurity requirements in agreements with vendors ❑ Maintains records for software and firmware versioning, patch levels, and configurations for critical assets ❑ Uses risk management processes for deploying, upgrading, replacing and decommissioning assets.
❑ Establishes policies and plans for incorporating vendors and suppliers into response and recovery activities.	**LEVEL 4: Optimized**	❑ Ensures that vendors' and suppliers' cybersecurity capabilities are periodically reviewed for their alignment with utility requirements. ❑ Incorporates vendors and suppliers into exercises, drills, or tests to support response and recovery activities. ❑ Enhances asset inventory information with known vulnerability information and active scanning.

6.3 IDENTIFY Risk Management

Identifying and documenting cybersecurity risks, assessing and managing their anticipated consequences, and prioritizing activities to address them in a manner that aligns with the needs of the organization.

Evaluation Criteria: Risk Management		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Identifies, assesses, and documents cybersecurity risks, as part of an overarching strategy.	**LEVEL 1: Initial**	❑ Conducts and assigns risk management activities randomly or in response to an incident.
❑ Documents processes and procedures informally across multiple documents, plans, or strategies. ❑ Consolidates cybersecurity processes, procedures, and requirements in a dedicated component of an enterprise wide risk-management strategy.	**LEVEL 2: Established**	❑ Performs risk assessments and documents/ monitors identified risks related to information systems, control systems, and other networks systems.
❑ Periodically updates its risk management strategy to prioritize risks and incorporate threats and/or standards, guidelines, and best practices (e.g., NIST, NERC CIP). ❑ Clearly outlines risk management roles and responsibilities. ❑ Incorporates risk training and education into the "Knowledge, Skills, and Abilities" requirements for personnel with IT or OT operational responsibilities.	**LEVEL 3: Mature**	❑ Dedicates resources (e.g., funding, personnel, technology) for risk management activities. ❑ Leverages resources and industry best practices to support risk assessments (e.g., ICS-CERT, DHS Critical Infrastructure Cyber Community [C3] Program, Federal Energy Regulatory Commission [FERC] Architectural Reviews).
❑ Identifies stakeholders associated with risks and involves them in mitigation/resolution. ❑ Requires that risks be reviewed and updated annually. ❑ Defines specific criteria for defining and measuring risk.	**LEVEL 4: Optimized**	❑ Demonstrates the capabilities and resources (e.g., funding, personnel, technology) to address all high-priority risks identified during a risk assessment.

6.4 PROTECT: Voluntary/Legal Compliance

Maintaining and documenting the procedures and processes necessary to support compliance of cybersecurity activities with applicable standards, laws, regulations, and requirements, and best practices, including NERC CIP, NIST CSF, and ISO/IEC standards.

Evaluation Criteria: Voluntary/Legal Compliance		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Uses mandatory standards (e.g., NERC CIP) as a basis for cybersecurity plans and activities.	**LEVEL 1: Initial**	❑ Meets baseline reporting requirements related to cyber incidents.
❑ Assigns responsibility for cybersecurity reporting obligations to specific personnel.	**LEVEL 2: Established**	❑ Reports significant cybersecurity incidents to regulatory and law enforcement agencies.
❑ Incorporates voluntary or "beyond compliance" cybersecurity activities into its policies and plans (e.g., reporting requirements, thresholds). ❑ Prioritizes cybersecurity resources appropriate to the importance of the asset and the greatest risk (Confidentiality, Availability, or Integrity) to each asset.	**LEVEL 3: Mature**	❑ Integrates legal and regulatory personnel into its response structure. ❑ Reports significant cybersecurity incidents to federal and industry partners (e.g., sector-specific Information Sharing and Analysis Center [ISAC], U.S. Department of Homeland Security [DHS] National Cybersecurity Communications and Integration Center [NCCIC]/U.S. Computer Emergency Readiness Team [US-CERT]).
❑ Establishes agreements with external organizations (e.g. PUCs in neighboring states or other regions, governors, federal partners) to facilitate incident reporting and the sharing of information.	**LEVEL 4: Optimized**	❑ Incorporates legal and regulatory considerations, including utility personnel and/or external stakeholders, into drills and exercises.

6.5 PROTECT: Safeguarding Critical Services

Developing and implementing appropriate policies and protections to ensure the security and resilience of information and operational systems and assets and safeguard against unauthorized access.

Evaluation Criteria: Safeguarding Critical Services		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Has limited policies and regulations regarding its security or its physical and cyber operating environment.	**LEVEL 1: Initial**	❑ Assigns responsibilities for the performance of cybersecurity activities to specific individuals.
❑ Employs a coordinated approach to cybersecurity that links response and recovery plans and policies to activities related to physical and cyber operating environment security. ❑ Establishes a budget for cybersecurity practices.	**LEVEL 2: Established**	❑ Dedicates funding for cybersecurity equipment, personnel, and training/ exercises to develop utility-wide cyber-hygiene practices. ❑ Segregates critical systems; provides access permissions based on requirements; physical access controls; and backs up data.
❑ Outlines specific practices governing access, asset inventory, configuration, change management, and records/logs. ❑ Has an established records retention policy governing the information retained, the purpose for the retention, and the length of retention.	**LEVEL 3: Mature**	❑ Conducts objective vulnerability assessments. ❑ Implements defense in depth (e.g., network segregation/segmentation to all key systems, employs basic remote and physical asset management).
❑ Employs a systems development life cycle for planning, developing, testing, and deploying IT and OT. ❑ Regularly reviews, updates, and communicates its policies and plans to incorporate new information and developments.	**LEVEL 4: Optimized**	❑ Employs comprehensive, advanced risk and vulnerability management programs (e.g., applies change management practices at all stages of asset life cycle; provides access permissions based on the principle of least privilege and risk to function; ensures data is properly protected, stored, and destroyed). ❑ Implements a robust corrective action process for prioritizing and addressing gaps and shortfalls.

6.6 DETECT: Monitoring and Detection

Developing and implementing activities to collect, monitor, and analyze information related to cyber activity, enabling the timely discovery of cybersecurity threats, such as detection of unauthorized changes to the configuration of assets or failure of security systems.

Evaluation Criteria: Monitoring and Detection		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Does not have policy or plans related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Assigns roles and responsibilities for monitoring and detection to specific individuals or positions, and these assignments are realistic given the background, training, and other responsibilities of those employees.	**LEVEL 1: Initial**	❑ Conducts basic assessments to monitor activities for suspicious behavior (e.g., periodic review of log data).
❑ Employs a coordinated approach to monitoring and detection that includes documented detection processes and procedures which are informed by industry standards and/or guidelines, and communicated to employees.	**LEVEL 2: Established**	❑ Establishes a baseline of network operations and expected data flows for users and systems and employs alarms and alerts for suspicious events.
❑ Outlines specific monitoring requirements that include defined indicators of compromise and timeframes for review of suspicious activity that are aligned with the utility's threat profile.	**LEVEL 3: Mature**	❑ Collects, analyzes, and shares data from cybersecurity events to inform cybersecurity efforts (e.g., Security Incident and Event Management automated log analytic tools) ❑ Maintains relationships with monitoring and/or detection vendors.
❑ Regularly updates its monitoring and detection requirements to address evolving threats and incorporates established best practices.	**LEVEL 4: Optimized**	❑ Conducts vulnerability scans and penetration tests to identify potential opportunities for exploits in its IT and OT systems. ❑ Collects information from outside the organization to proactively address cybersecurity threats, including from sector-specific information sharing and analysis centers (ISACs).

6.7 RESPOND: Collaboration and Communication

Establishing and maintaining relationships with internal and external stakeholders across the cybersecurity domain, creating a network for information and intelligence sharing to effectively communicate cybersecurity threats and vulnerabilities, response activities, and lessons learned.

Evaluation Criteria: Collaboration and Communication		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ Does not have policy or plans related to this topic.	**No Criteria**	❑ Has no technical activities related to this topic
❑ Did not share information.	**No Information**	❑ Did not share information
❑ Assigns responsibility for, and staffs, cybersecurity planning, reporting and communications to personnel within the organization.	**LEVEL 1: Initial**	❑ Collects information from and provides information to selected individuals and/or organizations.
❑ Identifies external stakeholders for information collection and sharing based on their relevance to the organization. ❑ Identifies alternate channels for communication in the absence of functional mainstream IT or communications technology.	**LEVEL 2: Established**	❑ Engages in information-sharing practices that address both standard operations and incident response operations. ❑ Coordinates response activities with internal and external stakeholders (e.g. external support from law enforcement agencies).
❑ Identifies the information-sharing requirements and thresholds associated with specific activities (e.g., to law enforcement, PUC, other regional utilities, US-CERT), and identifies technical subject-matter experts to consult on cybersecurity issues during steady state and times of cyber incident.	**LEVEL 3: Mature**	❑ Establishes a network of internal and external trust relationships (e.g., formalized agreements) to validate information surrounding cyber threats, vulnerabilities, and incidents. ❑ Engages in voluntary information sharing with external stakeholders, such as information sharing and analysis centers, industry partners, and surrounding utilities, to achieve situational awareness.
❑ Establishes trusted relationships with external stakeholders (e.g., industry and government partners) that include information sharing agreements and pre-identified points of contact for incident management. ❑ Identifies procedures to de-conflict information from multiple sources.	**LEVEL 4: Optimized**	❑ Coordinates incident response and restoration activities enterprise-wide and with external entities (e.g., coordinating centers, Internet Service Providers, system owners, other cybersecurity incident response teams [CSIRTs], and vendors).

6.8 RESPOND: Cyber Incident Response

Developing and implementing activities to address a detected cybersecurity incident, supporting the ability to contain the impact, limit the potential damage, and manage the consequences of a cyber incident.

Evaluation Criteria: Cyber Incident Response		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❑ The utility does not have policy or plans related to this topic.	**No Criteria**	❑ The utility has no technical activities related to this topic.
❑ Did not share information.	**No Information**	❑ Did not share information.
❑ Uses a generic incident response plan that includes some guidance for cyber incidents.	**LEVEL 1: Initial**	❑ Meets baseline reporting requirements of escalated cybersecurity incidents.
❑ Establishes a dedicated cyber incident response plan that identifies roles and responsibilities for specific personnel and includes response procedures for escalation, containment, and eradication of the threat, including requirements of third-party vendors or service providers. ❑ Establishes and formalizes the criteria for incident declaration and escalation.	**LEVEL 2: Established**	❑ Logs, tracks, and reports cybersecurity events and incidents in a manner consistent with the response plans. ❑ Provides training for personnel with specific response duties. ❑ Leverages law enforcement, government, vendor, or external industry resources for incident response.
❑ Requires that cyber incident response plan is updated and exercised intermittently, incorporating lessons learned from previous incidents or exercises.	**LEVEL 3: Mature**	❑ Maintains a dedicated cybersecurity response team that has the knowledge and resources to contain detected incidents and conduct a coordinated response. ❑ Identifies lessons learned after an incident.
❑ Requires that cyber incident response plans are exercised annually. ❑ Establishes procedures and processes for collecting and analyzing information to mitigate future incidents.	**LEVEL 4: Optimized**	❑ Ensures cyber response team coordinates with external agencies to support industry-wide response efforts. ❑ Establishes cyber mutual aid agreements and/or non-disclosure agreements with key stakeholders.

6.9 RECOVER: Incident Recovery

Developing and implementing activities to maintain plans for resilience and business continuity, supporting timely recovery to normal operations and implementation of corrective actions through after-action review and using lessons learned to reduce the impact from a cybersecurity incident and improve policies, plans, and procedures.

Evaluation Criteria: Incident Recovery		
Policy and Plans	**Maturity Level**	**Implementation and Operations**
❏ Does not have policy or plans related to this topic.	**No Criteria**	❏ Does not have policy or plans related to this topic
❏ Did not share information.	**No Information**	❏ Did not share information
❏ Has generic recovery and continuity plans that meet basic requirements.	**LEVEL 1: Initial**	❏ Provides training for personnel with recovery process responsibilities
❏ Develops formal plans for continuity and recovery that reflect specific restoration priorities and include reconstitution measures. ❏ Incorporates lessons learned and corrective actions from real events into continuity and recovery plans. ❏ Identifies the activities necessary to sustain the minimal functions of operations during recovery operations and restoration of critical assets.	**LEVEL 2: Established**	❏ Demonstrates the capabilities and possesses resources to complete the minimum activities necessary to return to normal operations. ❏ Tests continuity and recovery plans by drilling/exercising capabilities.
❏ Outlines specific recovery objectives and priorities in recovery and continuity plans, such as recovery time and point objectives, and IT/OT system recovery priorities. ❏ Recovery and continuity plans include alternative locations for operational control to ensure continuous service delivery.	**LEVEL 3: Mature**	❏ Compares results of continuity plan activation to recovery objectives to assess effectiveness. ❏ Conducts after-action reporting to identify and assess capability gaps and areas for improvement.
❏ Identifies likely impacts of cyber events and incorporates considerations into recovery planning. ❏ Conducts an annual review of mission critical functions and updates recovery and continuity plans.	**LEVEL 4: Optimized**	❏ Contracts with third party organizations to perform additional cyber forensics beyond the scope of internal capabilities. ❏ Prioritizes continuous improvement as part of its culture.

7. Summary

Through the effective use of the CPET, state utility regulators will have a comprehensive tool to analyze and refine utility responses to the NARUC *Questions for Utilities* and establish a set of reliable, measurable indicators of cybersecurity maturity over time. By engaging directly with utilities regarding their cybersecurity preparedness capabilities, commissions can identify trends, target resources, and inform long-term strategies for supporting the development of cybersecurity capabilities. Although the CPET is not intended to assess utilities against each other, commissions can use the data collected from its analysis to develop a comprehensive view of cybersecurity preparedness across its jurisdiction, including strengths, challenges, best practices, and other valuable information that will help guide their long-term activities and future engagements with utilities.

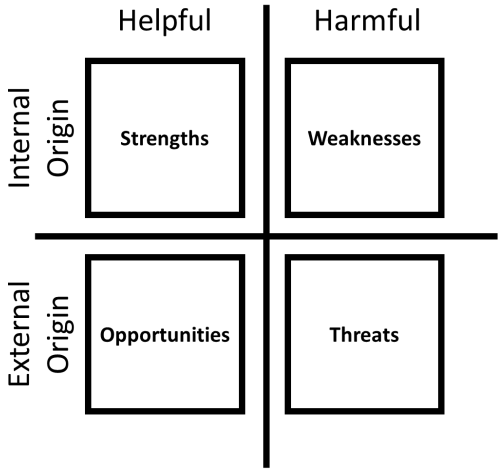
7.1 Additional Tools

Once a commission has completed its evaluation of a utility, it can use the information to inform future interactions with the utility. Commissions and utilities can implement other tools to build upon the information obtained through the CPET assessment and inform further discussion regarding utility cybersecurity investments, rate cases, etc. Two such examples are outlined below.

Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis

A SWOT analysis is a strategic planning technique that can help commissioners or their staff arrange findings from the CPET into four categories: Strengths, Weaknesses, Opportunities, and Threats. Traditionally, the four categories are arranged into a two-by-two matrix (see **Figure 3**). A SWOT analysis can be applied to a single utility or a "roll up" of findings to provide a broad view of a jurisdiction's maturity as a whole. It presents a four-way look at CPET findings and helps organize planning efforts by identifying elements that are within the control of the PUC and its jurisdictions (i.e., Internal Origin) and those outside of its control (i.e., External Origin). Additionally, it also separates findings into both helpful and harmful elements (e.g., things that may improve or impede cybersecurity maturity). Organizing SWOTs is helpful because it can enable the commission to set objectives and become more informed about the planning steps needed to achieve a better cybersecurity plan (e.g., Improve cybersecurity planning efforts for municipalities). Commissions can find more information about SWOT analyses and how they can support planning efforts in the Project Management Institute's Project Management Body of Knowledge (PMBOK).[1]

Figure 3: SWOT Analysis



1 Project Management Institute. 2004. A guide to the project management body of knowledge (PMBOK guide). Newtown Square, Pa: Project Management Institute.

Five Whys

Another useful tool for assessing the results of the CPET and determining cause and effect are the "Five Whys." The goal of the Five Whys technique is to determine the root cause of an issue by repeatedly applying the question "why?" to a problem until the source of the issue is determined. Although the technique is called "Five Whys," commissions may find that they will need to ask more questions to identify the root cause of an issue. The Five Whys technique is used as a standard practice in many strategic planning and management resources such as the PMBOK and the International Association for Six Sigma Certification.[2]

2 Munro, Roderick A., Govindarajan Ramu, and Daniel J. Zrymiak. *The Certified Six Sigma Green Belt Handbook, Second Edition.* Milwaukee: ASQ Quality Press, 2015.

Appendix A.

Acroynms

CIP	Critical Infrastructure Protection
CPET	Cybersecurity Preparedness Evaluation Tool
CSET	Cyber Security Evaluation Tool
CSF	Cybersecurity Framework
CSIRT	Cybersecurity Incident Response Team
C2M2	Cybersecurity Capability Maturity Model
C3	Critical Infrastructure Cyber Community
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
FERC	Federal Energy Regulatory Commission
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
IOU	Investor-Owned Utility
NARUC	National Association of Regulatory Utility Commissioners
NCCIC	National Cybersecurity Communications and Integration Center
NERC	North American Electricity Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operational Technology
PMBOK	Project Management Body of Knowledge
PUC	Public Utility Commission
SWOT	Strengths, Weaknesses, Opportunities, and Threats
US-CERT	U.S. Computer Emergency Readiness Team


NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
DEDICATED TO PUBLIC SERVICE
1889