USAID
FROM THE AMERICAN PEOPLE

CYBERSECURITY EVALUATIVE FRAMEWORK FOR BLACK SEA REGULATORS

December 2017
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).

CYBERSECURITY EVALUATIVE FRAMEWORK FOR BLACK SEA REGULATORS

Project Title:	Energy Sector Cybersecurity
Sponsoring USAID Office:	USAID/ Europe and Eurasia Bureau
Cooperative Agreement #:	AID-OAA-A-16-00049
Date of Publication:	December 2017
Authors:	Miles Keogh & Paul Stack, NARUC

National Association of Regulatory Utility Commissioners

This publication is made possible by the generous support of the American people through the United States Agency for International Development (USAID). 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.

Table of Contents

1. Introduction:

The USAID-NARUC Cybersecurity Evaluative Framework for Black Sea Regulators is an easy-to-use tool for regulators to evaluate utilities' cybersecurity preparedness. The framework is designed to provide a structured way for regulators to assess what level of cyber-preparedness utilities have reached and identify areas for improvement.

The framework is in many ways a companion to the *NARUC Cybersecurity Primer for State Regulators* (2017), which provides a comprehensive overview of cybersecurity fundamentals for economic regulators and outlines steps regulatory commissions can take to become effective partners with utilities in preventing and mitigating cyberattacks and bolstering overall security of the energy sector.

The Primer recommends that regulators take five initial steps. One of the first and most important steps is for regulators to ask questions of the entities they regulate. The Primer provides 107 sample questions drawn directly from cybersecurity interrogatories conducted by US regulators. The questions focus on 12 core cybersecurity subject areas, and they are designed to elicit responses from utilities that will give regulators enough information to gauge their overall level of cyber-preparedness.

The questions, however, are only as effective as regulators' ability to make sense of the answers. For this, regulators will have to work to build their knowledge of the basic concepts and strategies for cybersecurity defense. This will require time and effort on the part of regulatory staff to become familiar with the cybersecurity threat landscape and corresponding best practices for good cyber hygiene and defense postures. If regulators are to understand and review utilities' answers about cyber-preparedness, they need to be well-versed in the principles of defense-in-depth and system resilience; how to prioritize systems and networks over components; and effective utility governance structures, to name a few.

To complement these efforts, USAID and NARUC have developed this framework to serve as a systematic and structured mechanism for Black Sea regulators to evaluate utilities' answers and make holistic judgements about how well utilities are prepared and where there are areas for improvement. The framework has been tailored both to the specific challenges of cybersecurity and the unique role of the economic regulator. Cybersecurity can be especially technical, and at present, there are no metrics or comprehensive criteria to quantitatively measure one utility's cybersecurity performance. This lack of criteria limits efforts to benchmark one utility's progress or defense posture against another's.

In light of this, the framework aims to help regulators perform basic *quantitative* assessments of utilities in core cybersecurity categories (e.g., planning, procurement, personnel, etc.) by using largely *qualitative* responses from the Primer questions. The framework then allows regulators to synthesize each section into an overall evaluation highlighting strengths, areas for further development, areas of resistance, and areas for further exploration.

While this framework will not produce a precise figure (e.g., a utility is 66% cyber-secure) or allow for easy comparison across utilities, its function is similar to the the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), the self-evaluation tool used by utilities to measure and improve their cyber capabilities. Like the ES-C2M2, the framework affords regulators a holistic assessment of how developed and sophisticated a utility's approach is with regard to cybersecurity.

In addition to the framework itself (Section 5), we have included sections outlining how the tool has been informed by the role of the economic regulator (section 2); a step-by-step guide to use it (Section 3); and context and guidance for where and how it should be used (Section 4).

2. Role of the Regulator

So, what is it that economic regulators do and how will this change or remain the same when it comes to addressing the challenges of cybersecurity? This section aims to provide background as to what the role of the economic regulator is in cybersecurity and how the Cybersecurity Evaluative Framework has been designed to help regulators effectively serve in that role.

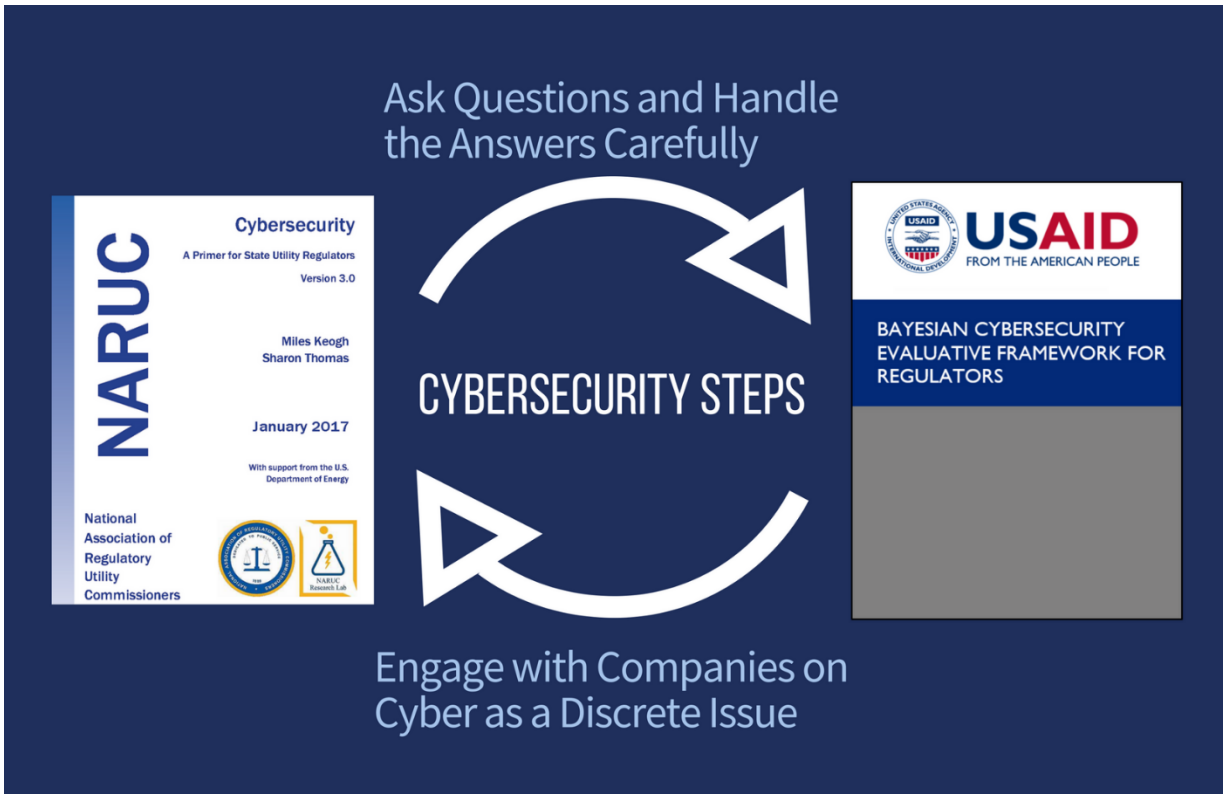
Regulators – the Before and After People

Economic regulators' core responsibility is to align cost-recovery with the public interest, ensuring that investments made by traditionally monopolistic companies align with various—and at times conflicting—policy objectives, such as affordability, reliability, safety, and security to name a few.

This is in many ways why regulators are considered "before" and "after" people—they set expectations and key objectives on the front end and evaluate utilities' actions and performance in realizing those goals after the fact. For example, as the figure below demonstrates, regulators set goals and evaluate performance in areas such as reliability and emergency preparedness, but they are not the ones in the field restoring power after storm outages.

For cybersecurity, regulators will continue to be "before" and "after" people. They will not be tasked with constructing cyber defense, but they will have to help set targets in line with policy objectives and periodically evaluate utilities' performance. This is why both the Primer and the *USAID-NARUC Regulatory Cybersecurity Strategy Development Guide*[1] emphasize that regulators first develop a strategy that lays out the goals and expectations of a commission and how the commission expects to work with utilities to identify objectives and measure progress.

[1] The *USAID-NARUC Regulatory Cybersecurity Strategy Development Guide is* a document that provides information and lessons learned for regulators to develop their own commissions' cybersecurity strategies. Drawing from experiences and best practices from U.S. state commissions, the document covers the important issues and questions that regulators should address as they begin the process of developing their unique cybersecurity strategies



Asking questions that target the most important cybersecurity issues[2] helps set expectations and signals to utilities that they should have a plan or approach for each of them. If this is the "before" component of regulators' engagement with utilities on cybersecurity, the "after" component involves reviewing the answers – i.e., how utilities have performed against those expectations.

In order to effectively evaluate utilities, regulators must have a basic understanding of what good answers look like – i.e., what constitutes good cybersecurity. In addition to the Primer, regulators should review the NERC[3] Critical Infrastructure Protection (CIP) Standards and the NIST[4] Cybersecurity Framework, which lays out a comprehensive framework for organizations to establish their approach to cybersecurity. While building understanding of the core concepts of cybersecurity will have to be an ongoing project of commissions, this Cybersecurity Evaluative Framework is designed to provide an organized approach for regulators to take a utility's answers on a wide range and scope of questions and to consolidate them into a single and holistic analysis.

[2] The core categories, both in the Primer and Evaluative Framework, are as follows: planning, standards, reporting, partnerships, procurement, personnel and policies, risk management, implementation, response and recovery, process questions, governance, and systems and operations.
[3] The North American Electric Reliability Corporation
[4] The National Institute of Standards and Technology

3. How to Use the Evaluative Framework

The Cybersecurity Evaluative Framework, located in Section 6, is structured and operates in many ways like the ES-C2M2, the tool most commonly used by utilities to perform self-assessments of their cyber defense policies, processes, and procedures. By asking themselves questions in core cybersecurity subject areas, utilities can evaluate the maturity of their current cybersecurity capabilities and generate a visual analysis of their overall posture (Figure 1). Afterwards, utilities can use these results to identify gaps and formulate an action plan to address and mitigate their most serious vulnerabilities (Figure 2).

Figure 1: A visual analysis of a utility based on the ES-C2M2 self-assessment

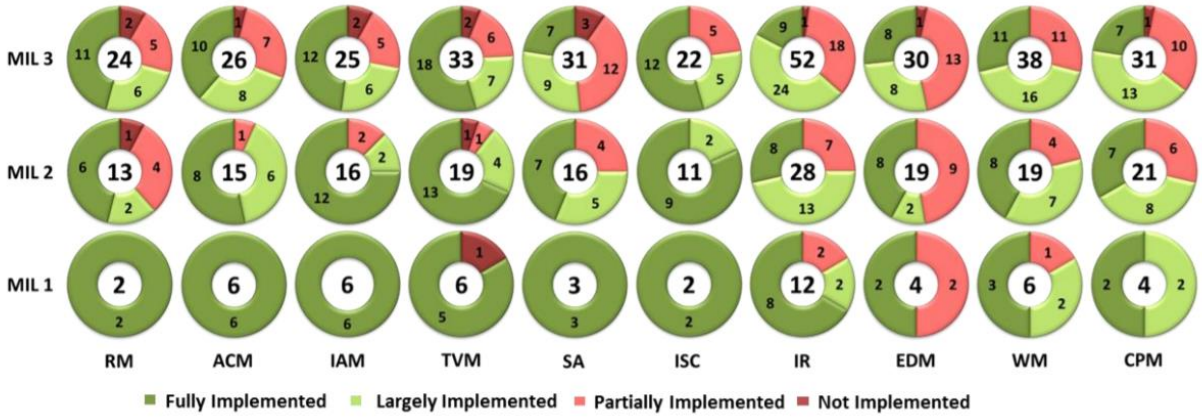


Figure 2: Utilities use the results from the ES-C2M2 self-assessment to identify gaps and formulate action plans.

	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

[5]

The Cybersecurity Evaluative Framework is very similar in structure to the ES-C2M2. Both rely heavily on questions and the assessment of qualitative data to evaluate cyber-preparedness. However, rather than a self-assessment tool, the framework has been designed for *regulators* to ask questions of utilities and assess their preparedness. In many ways, it functions like a management audit by framing questions to

[5] Source of Images: Christopher, Jason. United States Department of Energy. "Cybersecurity Capability Model Update" *Helping Utilities with Cybersecurity Preparedness: The C2M2* April 23, 2015.

utilities about processes, institutional structures, decision-making criteria, policies, etc. This is because good cyber is more about culture and the design of a system and organization on the front end than it is about one-off technological solutions.

Like the ES-C2M2, use of the framework requires in-depth analysis from a team that is familiar with core cyber concepts, and it may take several trials to feel comfortable using it. NARUC has developed mock exercises to help regulators simulate this review and get a sense of how this evaluation works in advance of its application.

Below is a step-by-step guide for regulators to use the Cybersecurity Evaluative Framework to generate and review the qualitative data from utilities. It requires users to draw from:

1) The *NARUC Cybersecurity Primer for State Regulators*
2) A separate Excel spreadsheet that accompanies the framework.

Step 1: Select 3+ Questions to Ask Utilities in Each Core Category

The framework is composed of the **12 core categories** listed below, which represent the key building blocks of good cybersecurity performance:

1. Planning: indicates that responses are not haphazard, reactive, or fragmented
2. Standards: indicates awareness of best practices and compliance with obligations
3. Reporting: indicates transparency and information sharing
4. Partnerships: indicates "strength in numbers"
5. Procurement: indicates systemic and interdependency-aware thinking
6. Personnel and Policies: indicates integration of risk management across the enterprise, including people
7. Risk Management: indicates a security perspective that addresses security over compliance
8. Implementation: this section is for more detailed responses (modifiable)
9. Response and Recovery: for if/when things go wrong
10. Process: indicates best practice awareness and continual improvement
11. Governance: indicates how reporting and transparency create accountability for performance
12. Systems and Operations: indicates that the plan is cyclical and a process, not just a one-time check-box.

To use the tool, regulators must select three or more questions to ask utilities for each of the **12 core categories**. The questions can be drawn from the 107 questions in the Primer, as they have been specifically selected to provide regulators with enough information in these categories.

For example, for Planning, regulators could select the following three questions from the Primer:

1. Does your company have a cybersecurity policy, strategy, or governing document?
2. Has your cybersecurity plan been reviewed in the last year and updated as needed?
3. Is your cybersecurity plan tested regularly? Is it tested internally or by or with a third party?

For Procurement, they could be:

1. Are cybersecurity criteria used for vendor and device selection?
2. Have vendors documented and independently verified their cybersecurity controls? Who is the verifier and how are they qualified?
3. Are there third-party providers of services whose cybersecurity controls are beyond the ability of your organization to monitor, understand, or assure? Has your organization explored whether these may create cybersecurity vulnerabilities to your operations?

Regulators should not feel confined to asking only three questions or to using the questions located in the Primer. Over time, NARUC anticipates that the tool will be adjusted and adapted to each Commission's needs and circumstances, and it has been designed with this flexibility and adaptiveness in mind.

Step 2: Collect Responses Provided by Utilities for Each Category

Based on the questions from Step 1, regulators will collect and review answers provided by utilities. To use the same example as above, sample responses for planning could look like:

1. Does your company have a cybersecurity policy, strategy, or governing document?

The company does, and it has been in place since 2009, with three subsequent revisions. We can give you a summary. The complete "For Official Use Only" version is available for "In Camera" review subject to non-disclosure agreement, at the company site. We are happy to schedule this with need-to-know commission personnel.

2. Has your cybersecurity plan been reviewed in the last year and updated as needed?

Our most recent review occurred six months ago and was accepted by the board of directors. No major revisions were required from the previous edition from 18 months ago, and only implementation specifics and schedules were adjusted.

3. Is your cybersecurity plan tested regularly? Is it tested internally or by or with a third party?

Company policy dictates that we test some components of our plan – e.g. cyber mutual assistance – as often as once per quarter. Training and response measures are tested internally twice per year. NERC compliance schedules are maintained. External audits and penetration testing is conducted annually. A full schedule is available for "in camera" commission review subject to non-disclosure agreement for need-to-know personnel at the company site.

Step 3: Use Framework to Evaluate Utilities' Preparedness in Each Core Area

As part of the review process, regulators will review utilities' answers and evaluate their preparedness in each core category. Specifically, regulators will assess where a utility is positioned across the following spectrum:

For each area provide your sense of the level of response provided by the companies:

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

Like the Maturity Indicator Levels (MILs) in the ES-C2M2, regulators will judge how far a utility has progressed in each core category. For example, to use the example of planning, regulators will attempt to assess the degree to which a utility's responses are not haphazard, reactive, or fragmented.

Is the utility completely unaware of why planning is important and/or do they dismiss the question entirely (Non-Awareness)? Are they aware of what cybersecurity planning is and why it is important, but have not planned to take any action yet (Issue Awareness Only)? Or maybe they are in the middle of implementing a plan of action, but have not finished it yet (Partial Implementation)?

The evaluation is subjective, and so the framework is not prescriptive on where one level ends and the next begins. Instead, regulators should seek to pinpoint, based on the answers they receive and the confidence they have in those answers, how far along a utility is in terms of their work in each core category and to provide guidance in prioritizing next steps.

In reviewing utility responses, regulators may have additional questions, seem unsure about how to assess a utility (is a utility at partial implementation or full implementation?), or feel unsatisfied with some answers that have been provided to them. That is why the framework includes the following two questions for each core category:

- What is your confidence in the cybersecurity preparedness based on the answers to these questions?
- What areas would you like to explore further with the company?

These follow-up questions are especially important, not only for assessing utilities' current profile or designation, but also for better understanding the full picture about a utilities' overall position with regard to cybersecurity. If answers provided by utilities are unclear or there is disagreement among the group of regulators about how to assess where they are exactly, regulators should determine what information they need to know to arrive at a consensus and reach out to utilities.

Step 4: Generate an Overall Analysis of a Utility Based on Each Core Category Assessment

Regulators should follow up on additional questions and reach a consensus on how to evaluate a utility in each of the twelve categories. At the end of this process, regulators should compile their assessments and notes. Below is an illustrative example of how some of the sections might look, with draft notes for the first two categories. The notes are by no means a model, neither in length or content, but hopefully, they serve as a representation of how a regulatory team might arrive at a specific assessment:

1. Planning: Planned Implementation

   Regulatory Notes: The utility representatives said they are drafting a plan, but they did not provide too much detail in their responses. The regulatory team wavered between evaluating their responses as "issue awareness" versus "planned implementation." Ultimately, the utility has a point person on cyber who is working on the plan, and they said they intend to bring in an outside consultant to review it later this year. With this information, the regulatory team decided upon "planned implementation," but we plan to follow up with the utility as part of the next review to get a better sense of the progress they have made in drafting and, later, implementing the plan.

2. Standards: Not Applicable

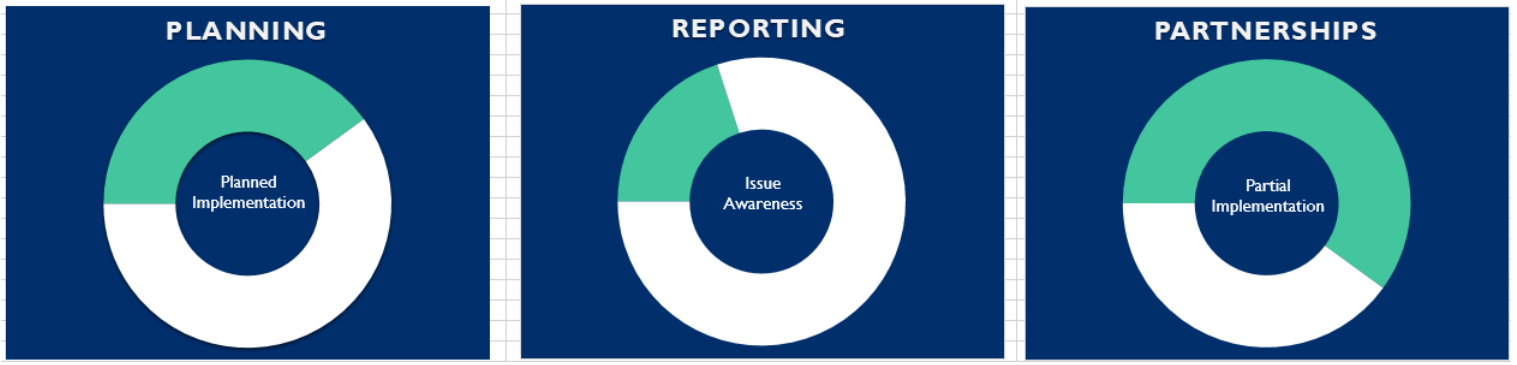
Regulatory Notes: Standards have not been adopted yet in the country, so this is not applicable. We expect to work with utilities to draft and implement baseline requirements in the next fiscal year.

Step 5: Use Tool for Visual Graphic

In the separate Cybersecurity Evaluative Framework Excel document that accompanies this document, USAID and NARUC have developed a tool to generate a visual representation of the holistic assessment from Step 4.

Regulators only have to incorporate the results from their review into the Excel spreadsheet, and a full visual graphic of all 12 categories will be generated. A snapshot of three of the categories is below:

Planning	Reporting	Partnerships
Not Applicable	Not Applicable	Not Applicable
Non-Awareness	Non-awareness/Dismissal	Non-awareness/Dismissal
Issue Awareness	Issue Awareness	Issue Awareness
Planned Implementation	Planned Implementation	Planned Implementation
Partial Implementation	Partial Implementation	Partial Implementation
Complete Implementation Iteration	Complete Implementation Iteration	Complete Implementation Iteration
Cyclical Implementation & Improvement	Cyclical Implementation & Improvement	Cyclical Implementation & Improvement
Planned Implementation	Issue Awareness	Partial Implementation



Note: this Excel format aligns with the graphics produced by the ES-C2M2 and will serve as an easy-to-understand visual representation of a utility's performance across all the core categories.

Step 6: Use the Results of the Framework to Work with Utilities in Defining Next Steps

The Cybersecurity Evaluative Framework is designed to give regulators a sense of just how prepared a utility is. While the ES-C2M2 helps utilities identify its own vulnerabilities and gaps, from which they develop an action plan, the evaluative framework can help regulators understand if utilities are indeed taking appropriate action. If such action is not being taken, the framework can serve to motivate and assist utilities in developing their own action plan around these core categories.

As such, the framework is not only a monitoring tool, but especially in countries that are just beginning their work on cybersecurity, it is also a way to begin a conversation with utilities on how best to plan and take action as part of a cyclical process of continuous improvement.

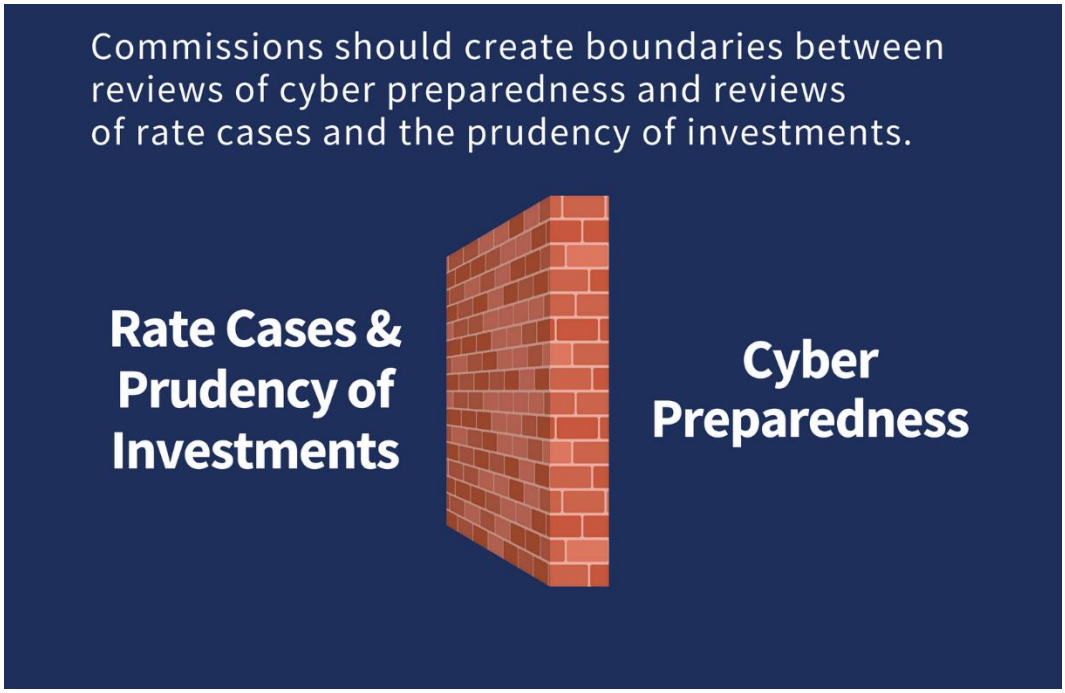
4. Context for Using Evaluative Framework

Regulators may wonder how these evaluations will work in practice. The experience of US economic regulators has been diverse, so there are no guidelines or model approach, per se. However, generally speaking, the meetings have been on-site at utilities and separated from any rate case or reviews of prudence. The two paragraphs below should help give regulators a sense of what their expectations should be in conducting initial cybersecurity reviews of utilities.

Reviews Should Be Discrete and Careful about Handling Sensitive Information

As mentioned earlier, regulators will primarily address cybersecurity in the same way they approach other issues – i.e., by asking questions and setting expectations for utilities. And yet, cybersecurity poses specific challenges requiring regulators to slightly modify their approach. First, protecting critical infrastructure tends to be an issue of national security. Therefore, regulators must ensure that sensitive information is not gathered in a context that would enable it to be publicly accessible, such as through a Freedom of Information Act request. They also must be cautious to not ask for sensitive information that they themselves cannot protect, such as utility cybersecurity plans, specific schedules, titles, and names of key employees.

The sensitivity and security concerns mean that cybersecurity should be treated as a discrete issue and separated from the context of a rate case or the review of an investment program. This is why, in the US, many regulators have opted to conduct these cyber reviews on-site at utilities, with the understanding that confidentially will be maintained and sensitive documents will be reviewed "in camera" or privately.



This separation allows utilities and regulators to have more candid and open discussions. Take, for example, rate cases, which are litigious and not necessarily conducive for cooperation and candor. They are instead venues where a question such as "do you know what time is it?" is more likely to elicit a response of "yes" as opposed to "10 o'clock." The choice to separate the two reviews is also to avoid exposing sensitive cybersecurity information to public disclosure requirements.

Setting Reasonable Expectations for Initial Cybersecurity Reviews

It should also be emphasized that utilities are likely to be at different stages of cyber maturity. The larger utilities in the US, for example, have been subject to NERC CIP standards for over a decade, while other utilities, such as smaller distribution companies, may not have given cybersecurity any consideration at all. The framework has been designed to be nimble and adaptable for regulators to use when engaging with either highly sophisticated or inexperienced utilities.

For utilities that have not given any consideration to cybersecurity, the first round of questions may have to serve as an opportunity simply to set expectations. Therefore, regulators may have temper expectations about the responses utilities provide. In such cases, the questions will allow utilities and regulators to set targets and next steps together from the outset, and the framework can then be used in future meetings to measure the progress these utilities have made according to those agreed-upon next steps.

5. Evaluative Framework

Regulators should follow the step-by-step instructions in Section 3 to use this framework.

The Cybersecurity Evaluative Framework is comprised of 12 core categories:

- **Planning**: indicates response is not haphazard, reactive, or fragmented
- **Standards**: indicates awareness of best practices and compliance with obligations
- **Reporting**: indicating transparency and information sharing
- **Partnerships**: "strength in numbers"
- **Procurement**: indicates systemic and interdependency-aware thinking
- **Personnel and Policies**: indicates integration of risk management across the enterprise, including people
- **Risk Management**: Describes a security perspective that addresses security over compliance
- **Implementation**: more detailed responses (modifiable)
- **Response and Recovery**: for if/when things go wrong
- **Process Questions**: indicate best practice awareness and continual improvement
- **Governance**: Indicates how reporting and transparency create accountability for performance
- **Systems and Operations**: indicates that the plan is cyclical and a process, not just a one-time check-box.

For each core category, provide your sense of the level of response provided by the companies:

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Planning: indicates response is not haphazard, reactive, or fragmented

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Sample Questions to Ask from the Primer

Standards: Indicates awareness of essential practices and compliance

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Sample Questions to Ask from the Primer

Reporting: indicates transparency, communications readiness, information-sharing capability

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Partnerships: indicates network-awareness, ability to draw on "strength in numbers"

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Procurement: addresses supply chain issues and investment priorities

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Personnel and Policies: indicates integration of risk management across the enterprise, including people

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Implementation: indicative of process that is cyclical, measured, and assures effectiveness

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Response and Recovery: indicates awareness of best practices for when things go wrong

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Process Questions: more detailed info about company practice (modify as appropriate)

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Governance: indicates how reporting and transparency create accountability for performance

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

Systems and Operations: indicates that the plan is cyclical and a process, not just a one-time check-box.

What level of response was provided by the company?

__ Not applicable

__ Non-awareness / dismissal

__ Issue Awareness Only

__ Planned Implementation

__ Partial implementation

__ Complete implementation iteration

__ Cyclical implementation & improvement

What is your confidence in the cybersecurity preparedness based on the answers to these questions?

What areas would you like to explore further with the company?

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
www.naruc.org