CYBERSECURITY ACCELERATOR PROGRAM™

AMERICAN PUBLIC POWER ASSOCIATION

CAP Application Guide

March 2026

Cybersecurity Accelerator Program (CAP) Application Guide

Published by the

American Public Power Association

2451 Crystal Drive
Suite 1000

Arlington, VA 22202

www.PublicPower.org

Table of Contents

Table of Contents 3
About APPA 4
Purpose of this Guide 5
Cybersecurity Accelerator Program (CAP) Overview 5
Application Process Overview 6
CAP Registration and Cost 7
Scoring Information 7
Internal Controls (IC) Section 11
Cybersecurity Governance and Training (CGT) Section 21
Cyber Incident Response (CIR) Section 26
Cyber Risk Management (CRM) Section 30
Appendix A: CAP Scoring Criteria Summary 36

About APPA

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power approximately 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 55 million people that public power utilities serve across the United States and its territories. We advise on electricity policy, grid technology and operations, and workforce development in support of safe, modern, and resilient utilities.

Purpose of this Guide

This guide provides CAP applicants with a program overview, as well as additional detail on the application process, questions, and scoring. The document offers rationale for the inclusion of each question, along with potential clarifications and associated resources, as applicable.

The guide is meant to help utilities better understand the program and grading process and provide clarity on the intent behind each question. If you have any additional questions as you are completing the CAP questionnaire, please contact CAP@PublicPower.org.

Cybersecurity Accelerator Program (CAP) Overview

CAP is intended to help participants assess and improve the maturity of their cybersecurity program over time. The CAP questionnaire addresses both information technology (IT) and operational technology (OT) security, and participants would benefit from working with both leadership and subject matter experts within their organization to complete the self-assessment. The questionnaire is based on industry-leading cybersecurity practices in four categories:

- Internal Controls
- Cybersecurity Governance and Training
- Cyber Incident Response
- Cyber Risk Management

Utilities that receive a CAP designation can demonstrate their commitment to cyber resilience to community leaders, governing board members, suppliers, and service providers. However, this initial designation is only one milestone on a journey of cyber program maturity that will continue to evolve in line with advancements in cyber threats and vulnerabilities.

In the CAP questionnaire, applicants earn points for their security practices and organizational posture in each of the four categories. The CAP assessment is intended to not only recognize utilities who have mature cyber programs, but to demonstrate what such a program might include to utilities who are less advanced.

The following sections provide a list of the specific questions and scoring criteria in each category, and Appendix A provides a summary of the point allocation across the questions.

Application Process Overview

Application Timeline (When Can I Apply?)

The initial CAP application period will open for submissions on **March 30, 2026**, and close on **June 30, 2026**. While a significant portion of the scoring occurs automatically on the online application system, the CAP Review Panel, composed of public power employees from across the country, review applications for any issues and ultimately sign off on each application's final score. The CAP Review Panel will finalize scores in **August 2026** before announcing designations at APPA's Cybersecurity and Technology Summit in **September 2026.** Based on the information provided in a utility's completed application and the utility's size, utilities that qualify for a designation may receive a Gold, Platinum, or Diamond CAP designation.

CAP Utility Size Categories (What Size Class is My Utility?)

- Small Utility: Fewer than 10,000 Customers
- Medium Utility: 10,000 – 75,000 Customers
- Large Utility: More than 75,000 Customers

Designation Levels (What Does My Score Mean?)

The score required to achieve a particular designation level is different depending on the size of the utility. **Designation documentation will clearly delineate utility size** (e.g., Platinum – Small, vs. Platinum – Medium or Platinum – Large). APPA chose this size-based approach to recognize utilities for their efforts in the context of the resources that utilities can be reasonably expected to expend on cybersecurity. For example, it is reasonable to expect that larger utilities have more resources to devote to cybersecurity and therefore require a higher score to achieve any given designation level.

	Small (<10K)	**Medium** (10-75K)	**Large** (>75K)
Diamond	90-100	95-100	98-100
Platinum	78-<90	85-<95	90-<98
Gold	66-<78	75-<85	80-<90

The size categories apply to distribution utilities, who be the majority of CAP applicants. Joint action agencies or other power-producing public power entities that participate will be considered large. Please contact CAP@PublicPower.org if you require additional guidance.

Designation Period (Once I Receive a Designation, How Long Is It Good For?)

CAP designations last for two years. For example, utilities that apply in 2026 and receive a CAP designation in September 2026 will maintain that designation through August 2028. To maintain status after that, the utility must re-apply when the 2028 application opens (early 2028) and achieve a designation in that period. If the applicant receives a CAP designation again, that will be effective in September 2028, once the previous designation expires.

CAP Registration and Cost

Application Registration (How Do I Start the Application Process?)

Prior to gaining access to the CAP application, prospective applicants must submit a registration form. APPA uses this information to create a utility account on the online application platform. In addition, the form asks for a primary contact for the utility. This individual will be the primary point of contact for all correspondence relating to the application. The Panel, potentially via APPA staff, may also contact this individual with any questions they have about the application.

Cost (Is There a Cost to Participate?)

This iteration of CAP is funded by a cooperative agreement that APPA has with the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), DE-CR0000026 – Cyber Pathways. **There is currently no cost to apply.** Future program years beyond the life of this agreement will include an application fee that corresponds with the applying utility's size.

Scoring Information

Point Values (How Do I Know What a Question is Worth?)

The sections below outline the full CAP question set, along with the associated point values.

Question Visibility (Why Can't I See All the Questions on the Platform?)

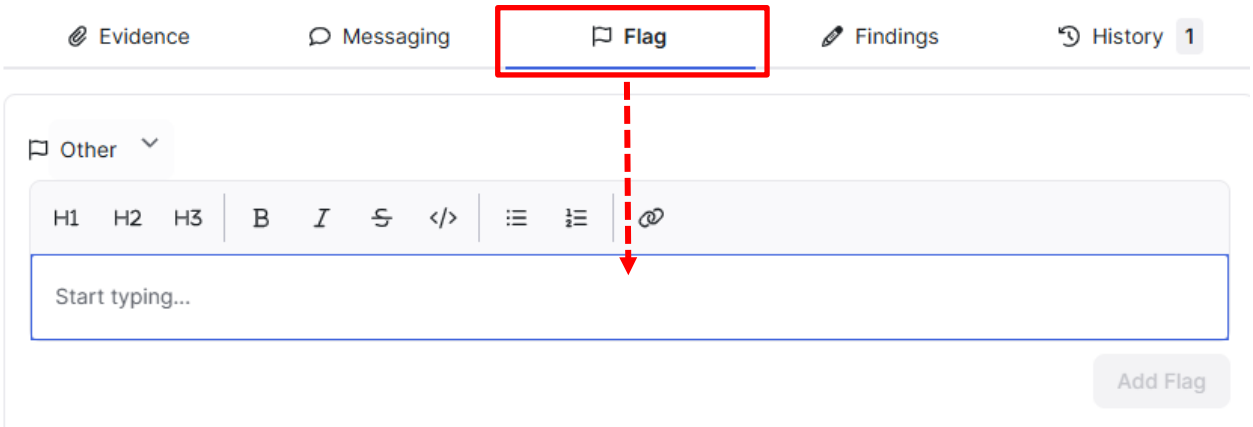
Based on the responses you select, you may not be able to see all the sub-questions listed in this guide in your questionnaire. The visibility of (and ability to get points from) a given sub-question will depend on its relationship to the initial question and your response to that question.

- Sub-questions will not be visible to you in the platform if it is not possible to answer them based on your response to the initial question. For example, if you answer "No" to "*Does your utility have password policies for IT systems?*" (CGT4), you will not see the sub-question about what those policies include (CGT4.a).
- Sub-questions that do not require a positive answer to the initial question will be visible. For example, CGT4.b asks whether your utility provides or recommends a password manager to employees; this is possible whether you have a password policy or not.

This approach minimizes the time required to complete a questionnaire while allowing each applicant the maximum opportunity to collect points. If there are any questions in this guide that are not visible based on your responses but you could credibly answer in a way that would result in additional points, please contact CAP@PublicPower.org.

Question Issues (What If I Have a Question About a Question?)

This application guide provides context on questions where CAP program staff identified the potential need for additional clarity. If there are other questions where you feel that ambiguity or lack of clarity could affect your response, please answer to the best of your ability and use the platform's "Flag" function to provide context in the associated comment box (see below).



The CAP Review Panel will review flagged questions and provide a response or otherwise resolve, as necessary. You can use the other fields (e.g., Messaging, Findings) to communicate internally about a response.

Evidence (Do I Need to Submit Documentation?)

In this iteration of CAP, there is no need to submit documentation to get points. The intent behind this approach is to minimize the burden of participating in the program. In future iterations, the Review Panel may weigh the value of requiring evidence for some questions – which can provide greater validation for CAP designations – against the increased burden for both applicants and reviewers of doing so.

CAP Review Panel (Who Reviews My Application?)

The platform automatically scores each question response based on each question's specific values. A panel of public power representatives also reviews the CAP applications. The CAP Review Panel ("the Panel") has 10 members. Two representatives from small, medium, and large systems account for six panel seats. Representatives from either a joint action agency or state/regional association fill two Panel seats. Individuals that have previously served on other APPA panels (e.g., APPA's Reliable Public Power Provider and Smart Energy Provider programs) fill the two remaining seats.

Additional Scoring Information (What Else do I Need to Know?)

Many questions begin with the words "Does your utility…" Unless the question makes a distinction about who, specifically, is conducting a given action (e.g., internal vs. external controls audit in IC13.a), "your utility" includes external partners (e.g., contractors, managed service providers) that may be performing these functions on your behalf.

Question CRM6 (or, if applicable, CRM6.a) is the last question in the questionnaire. If you the system shows that you still have questions unanswered after finishing that question, it is possible that there are one or more unanswered questions above. If so, you can click the box above the main question module that says 'Pending' and tells you the number of open questions, and it will filter to any unanswered questions.

Point Allocation (How Are Points Allocated Among the Categories?)

There are a different number of questions and points available in each category. However, to reflect their relative importance in assessing cyber program maturity, the CAP scoring process weights each category to arrive at a final score.

Category	Weight
Internal Controls	30
Cybersecurity Governance and Training	20
Cyber Incident Response	25
Cyber Risk Management	25
Total	**100**

For example, if a utility obtains 80 of 100 possible points in the Cybersecurity Governance and Training section, they will receive an 80% score in that category. Because this category makes up 20% of the total CAP application, or 20 of 100 total points, they would receive 16 points (80% of 20) for that category. A full example of a notional score is available in the table below.

Category	Score	Available	Percent	Weight	Weighted
Internal Controls	160	199	80%	30	24.1
Cybersecurity Governance and Training	78	100	78%	20	15.6
Cyber Incident Response	40	49	82%	25	20.4
Cyber Risk Management	80	89	90%	25	22.5
				Final Score	**82.6**

Note: While the “Validation score” that automatically calculates in the questionnaire platform is a good indicator of overall performance, it does not equate exactly with your official CAP score, which is the basis for designation decisions.

Minimum Category Scores (Do Category Scores Matter?)

You must score at least 50% in every category to achieve a designation. It is unlikely that applicants are sufficiently mature to obtain a score worthy of a designation while failing to score 50% in any category. However, because designations are intended to highlight utilities that are successful at implementing fundamental cybersecurity practices, failure to meet that threshold in any category would result in non-designation.

Internal Controls (IC) Section

This section contains a sequential, question-by-question review of the CAP application's Internal Controls section. The guide explains each question in this section and outlines the scoring rubric, if applicable. The section also identifies which elements of the NIST Cybersecurity Framework (CSF), Center for Internet Security (CIS) Critical Security Controls ('Controls'), DOE Cybersecurity Capability Maturity Model (C2M2), and National Association of Regulated Utility Commissioners (NARUC) Cybersecurity Baselines for Electric Distribution Systems and DER ('Baselines') may be relevant to the question.

IC1 – IT Asset Inventory

IC1. Does your utility inventory the organization's IT assets? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.AM-01; ID-AM-02	1.1	ASSET-1a:g	1.A

Having a complete and easily accessible inventory of your utility's IT assets is critical for understanding which assets in your networks you need to protect or monitor, and how best to do so. It is difficult to secure assets that you don't know exist, and these unknown connections could be the point of access for an attack.

IC1.a. How frequently do you inventory IT assets? **[up to 2 points]**

- ***Periodically*** **(2 points)**
- ***Only log known changes*** **(0 points)**

Inventorying assets on a periodic basis helps ensure greater visibility, including changes to your inventory that you were not otherwise aware of.

The questionnaire does not define a specific period, but it is important that there is a process that occurs at regular intervals.

IC2 – IT Asset Inventory

IC2. Does your utility inventory the organization's OT assets? **(8 points)**

See IC1., applied to OT.

For additional guidance, see CISA's Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators.

***IC2.a. How frequently do you inventory OT assets?* [up to 2 points]**

- ***Periodically* (2 points)**
- ***Only log known changes* (0 points)**

See IC1.a., applied to OT.

IC3 – Crown Jewel Analysis

***IC3. Does your utility identify your critical or 'crown jewel' assets?* (8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.AM-05		ASSET-1c	

In addition to knowing what assets are in your inventory, it can be helpful to identify which of those assets are the most critical.

IC4 – Data Inventory

***IC4. Does your utility inventory important data, including customer information, financial data, and internal system settings?* (8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.AM-07	3.2	ASSET-2a	2.O

A data inventory enables organizations to identify, classify, and protect sensitive data, reducing the risk of breaches and easing compliance with regulations. This inventory can also help ensure visibility, support risk assessments, and enable rapid response to incidents.

IC5 – Configuration Baselines

***IC5. Does your utility establish configuration baseline(s) for assets?* (12 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.PS-01; PR.IP-01	4.1	ASSET-3a	

Configuration baselines establish a secure, standardized foundation for systems, enabling consistent protection, rapid threat detection, and streamlined compliance. Establishing a “known good” state can help you detect unauthorized changes or other anomalies that could be early indicators of compromise. Configuration baselines can also support digital system restoration following an incident.

***IC5.a. Do you apply the configuration baseline(s) to all assets at deployment?* (2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		ASSET-3b	

Applying the configuration baselines at deployment can reduce the risk of misconfigurations, which are a common cause of breaches.

While a policy to do so is not required, that is the most common way to ensure that baselines are applied to all assets at deployment.

IC6 – Data Backup

IC6. Does your utility back up data for critical systems? (8 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.DS-11	11.1	RESPONSE-4b	2.R

Data backups are critical for ensuring business continuity, mitigating the impact of ransomware and other cyberattacks, and preserving the integrity of sensitive information. Data backups can help mitigate downtime and potential consequences of incidents, including natural disasters that impact systems physically storing your data.

IC6.a. How frequently do you perform backups? [up to 4 points]

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	11.2		

Backup frequency directly affects how much data you can recover after an incident and how much operational disruption you'll face. More frequent backups mean less data loss and faster recovery.

- ***More than once a day*** **(4 points)**
- ***Daily*** **(3 points)**
- ***Periodically, but less than daily*** **(2 points)**
- ***Ad hoc (1 point)***

IC6.b. Do you store at least one complete backup in an alternate location? (3 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	11.4	RESPONSE-4k	

Offsite backups – whether cloud-based or in a separate data center – ensure data survives even if the main location is compromised or damaged.

IC6.c. Do you maintain multiple copies of backups? (3 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	11.4		

Maintaining multiple copies of backups provides redundancy and helps ensure data availability in case a backup is corrupted, lost, or compromised. In combination with other backup best

practices, this can help mitigate against ransomware or other types of attacks where the threat actor specifically targets backups in addition to the primary data.

IC6.d. Do you store data in multiple forms of media? **(3 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	11.4		

Storing backups on multiple forms of media reduces potential single points of failure which could occur from relying on one type of media (e.g., hard drives or cloud storage). For example, even if you had multiple backups in the cloud, an attack that compromised your cloud services could make all copies unavailable.

Different forms of media also offer a variety of potential upsides, depending on need. For example, cloud backups may be most helpful for remote recovery, while local drives may offer faster restoration for on-site systems.

IC6.e. Do you encrypt backups? **(3 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	11.3	RESPONSE-4j	

Encrypting your backups helps protect them from unauthorized access, tampering, and theft.

IC6.f. How long do you retain backups? **[up to 3 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	3.4		

Longer backup retention periods provide greater protection against delayed threat detection and enable recovery from older data loss incidents. Some attackers can compromise systems and then remain relatively dormant for extended periods of time; longer retention periods increase the likelihood that you will still have backups to restore from that pre-date the initial intrusion. Historical backups can also support incident forensics in the aftermath of an attack.

- ***<30 days*** **(1 point)**
- ***1-3 months*** **(2 points)**
- ***4+ months*** **(3 points)**

IC6.g. Does your utility also backup configurations for critical systems? (4 points)

Backing up configurations for critical systems makes it easier to restore systems to a “known good” state, minimizing potential downtime following an incident, including both cyberattacks or accidental misconfiguration.

IC7 – Identity and Access Management

***IC7. Does your utility have an identity and access management (IAM) program?* (4 points)**

An IAM program helps ensure that only the right individuals and systems have access to the right resources at the right time, minimizing the risk of unauthorized access, data breaches, and insider threats.

While utilities can employ IAM practices without the existence of a specific program, establishing a program helps support and coordinate IAM-specific efforts.

***IC7.a. Does your utility create individual user accounts for people and application services that require access to:* [up to 4 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.AA-01	5.1	ACCESS-1b	2.C

Individual user accounts enable accountability and the ability to enforce access controls, reducing the risk of unauthorized activity occurring in your systems.

- ***Your IT systems (2 points)***
- ***Your OT systems (2 points)***

***IC7.b. Does your entity use multi-factor authentication (MFA) for digital access?* (4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.AA-03	6.3:6.5	ACCESS-1i	2.H

MFA is one of the most effective defenses against cyberattacks because it adds layers of protection beyond just a password, making it significantly harder for attackers to gain unauthorized access – even if they've obtained legitimate credentials. MFA is particularly effective against common, automated attacks like brute-force and credential stuffing, which rely on guessing passwords.

For additional guidance, see CISA's fact sheet on Implementing Phishing-Resistant MFA.

***IC7.b.i. What proportion of your IT systems use multi-factor authentication?* [up to 4 points]**

- ***Some IT systems?* (1 point)**
- ***Most IT systems?* (3 points)**
- ***All IT systems?* (4 points)**

'Some' is between 1-50%; 'Most' is between 51-99%; 'All' is 100%.

***IC7.b.ii. What proportion of your applicable OT systems use multi-factor authentication?* [up to 4 points]**

- ***Some OT systems? (1 point)***
- ***Most OT systems? (3 points)***
- ***All OT systems? (4 points)***

'Some' is between 1-50%; 'Most' is between 51-99%; 'All' is 100%. Unlike IT, this question specifies applicable *OT systems because some OT systems in your network may not support MFA.*

***IC7.b.iii Does your utility require multi-factor authentication for privileged accounts?* (8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	6.5	ACCESS-1h	

While MFA can help secure any system where you implement it, it is particularly important that accounts with elevated privileges use MFA because the consequences associated with compromising one of these accounts are greater than for normal users.

IC8 – Physical Access Controls for Digital Assets

***IC8. Does your utility have physical access controls to limit who is able to physically access critical or sensitive assets?* (4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.AA-06		ACCESS-3a; 3d	

Physical controls like keycards, biometrics, and security guards ensure only authorized personnel can enter sensitive areas (e.g., data centers, server rooms) that are important to your networks. Unauthorized physical access to critical or sensitive assets can result in data compromise, theft, or sabotage – including from insider threats.

IC9 – Email and Web Traffic Protections

***IC9. Does your utility use software or a service to block potentially malicious interactions? Check all that apply:* [up to 5 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	9.3:9.7	ARCHITECTURE-2g	2.M

- ***An e-mail filtering solution that blocks potentially malicious attachments* (1 point)**
- ***An e-mail filtering solution that has the ability to run suspicious attachments in a sandbox* (1 point)**
- ***An e-mail filtering solution that blocks suspicious messages based on their content or sender attributes* (1 point)**

- ***A web filtering solution which stops employees from visiting suspicious and known malicious websites*** **(1 point)**
- ***A web filtering solution that blocks suspicious or known malicious downloads*** **(1 point)**

Web and email filtering systems can protect your organization from malware, phishing, data leaks, and inappropriate content, serving as a first line of defense against both external and internal threats.

IC10 – Network Segmentation

IC10. Does your utility logically segment critical IT and OT systems? (16 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.IR-01	12.2	ARCHITECTURE-2b; 2h; 2i; 2j	2.F

Segmentation prevents threats that originate in IT systems from easily reaching OT environments. This is an essential protection, especially for OT systems that are not able to incorporate modern security features themselves. Isolating these OT assets through segmentation reduces exposure to internet-based threats and other unauthorized access. Segmentation can also allow you to limit the spread of malware or malicious traffic in the event of an incident.

An infographic highlighting the importance of IT/OT segmentation that provides some best practices for segmentation is available here.

'Critical' in this question typically refers to those systems that could impact grid operations or any other essential aspect of your business. For example, if applicable, it would certainly include any assets your organization identifies as 'crown jewels' (see question IC3.)

IC10.a. Does your utility segment systems within your IT environment? **(4 points)**

In addition to segmentation between IT and OT systems, segmentation of IT and OT networks (also known as microsegmentation) reduces the attack surface, limits lateral movement, and enforces granular access controls.

CISA has additional guidance on microsegmentation available here.

IC10.b. Does your utility segment systems within your OT environment? **(4 points)**

See IC10.a.

IC11 – Logging

IC11. Does your utility (or a third party on your behalf) log IT network activity? (4 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.PS-04; DE.CM-01	8.1;8.2	SITUATION-1a	2.T

Logging is critical for enabling many fundamental cybersecurity practices, including threat detection, incident response, and forensic analysis.

IC11.a. Does your utility (or a third party on your behalf) log OT network activity where possible? **(4 points)**

See IC11.

This question specifies logging OT network activity where possible *because some OT systems in your network may not support logging.*

IC11.b. Does your utility (or a third party on your behalf) review logs periodically? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	8.11	SITUATION-2a	

While logging network activity is critical, reviewing those logs is what turns raw data into actionable cybersecurity intelligence. Without regular analysis, logs can become digital clutter rather than an important foundation for system resilience.

IC11.c. How long do you maintain logs for key systems? **[up to 3 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	8.10		

- ***Less than one month*** **(1 point)**
- ***Between one month and a year*** **(2 points)**
- ***More than one year*** **(3 points)**

While logs can play a key role in supporting incident response, cyberattacks can play out over weeks or months. If your utility no longer has the relevant logs once you have identified a breach, it will likely complicate root cause analysis and forensics and impede the overall response effort.

IC12 – Monitoring

IC12. Does your utility have anyone (internal or external) monitoring the organization's security operations? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
DE.CM-01		SITUATION-2a	

Security monitoring enables real-time threat detection, rapid incident response, and continuous protection of networks and assets, reducing the risk of breaches and minimizing damage if attacks occur. Monitoring is essential to a proactive cybersecurity posture.

IC12.a. Does your utility have 24/7 monitoring (internal or external)? **(4 points)**

Maintaining monitoring efforts 24/7 helps reduce vulnerability to attacks that occur outside of normal business hours.

IC12.b. Do you have any automated systems (e.g., SIEM) in place to detect irregular or anomalous activity that may be indicators of a cyber incident? **(4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	13.1	SITUATION-2e; 2f	

Tools are increasingly available to support the detection of anomalous behavior and other suspicious activity. Security Information and Event Management (SIEM) tools can centralize and analyze logs from multiple network segments in a way that would be difficult – or likely impossible – for humans to replicate at scale.

IC12.b.i. Is your utility collecting data from (select all that apply): **[up to 4 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	13.2;13.3	SITUATION-2b	

- ***Endpoints*** **(2 points)**
- ***Network traffic*** **(2 points)**

Endpoint and network traffic monitoring are both essential to ensure visibility into your systems. Endpoint monitoring can provide more granular insight into what is happening on individual devices, including device compliance and user activity. Monitoring network traffic provides broader visibility across the entire environment and can detect threats before they reach endpoints. Network monitoring can be useful for identifying lateral movement and command-and-control traffic, which is particularly useful for uncovering stealthy or persistent attacks.

IC12.c. Are the people monitoring operations able to take action to resolve potential incidents in real time? **(8 points)**

Monitoring can help identify attacks but does not stop attacks without an active response. When the people (internal or external) monitoring your operations can also take action to resolve potential incidents, it can minimize the time between detection and response, and limit potential consequences of attacks on your system(s).

IC13 – Controls Audit

***13C. Does your utility test or audit the effectiveness of your cybersecurity controls?* (8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	18.1	PROGRAM-2h	1.F

Testing and auditing cybersecurity controls is essential to ensure they work as intended and identify vulnerabilities before attackers do. Without regular validation, even well-designed controls can become ineffective over time. Testing and auditing can also support risk management by providing a clear picture of your organization's risk posture and helping to identify and prioritize issues to remediate.

***IC13.a. Who performs the cybersecurity audits?* [up to 4 points]**

- ***Internal* (1 point)**
- ***Third party* (3 points)**
- ***Both internal and third party* (4 points)**

External auditors bring objectivity and expertise and can help uncover potential blind spots that internal teams have overlooked. External validation may also be important for regulatory and stakeholder requirements. However, internal testing and auditing can also be effective in supporting your cybersecurity program. Internal teams have extensive knowledge of the company's systems, can tailor tests to areas of interest, can conduct tests more frequently, and are more cost-effective. A combination of both internal and third-party audits and control testing provides the most comprehensive coverage.

***IC13.b. How frequently do you audit control effectiveness?* [up to 4 points]**

- ***Annually* (2 points)**
- ***Quarterly* (3 points)**
- ***Monthly* (4 points)**

Without regular validation, utilities risk relying on outdated or ineffective protections – potentially without knowing it. Given the evolution of cyber threats and system changes over time, even a well-designed control scheme can degrade and leave networks vulnerable.

Cybersecurity Governance and Training (CGT) Section

This section contains a sequential, question-by-question review of the CAP application's Cybersecurity Governance and Training section. The guide explains each question in this section and outlines the scoring rubric, if applicable. The section also identifies which elements of the NIST CSF, CIS Controls, DOE C2M2, and NARUC Baselines may be relevant to the question.

CGT1 – Cybersecurity Program

CGT1. Does your utility have a cybersecurity program? (8 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
GV.PO-01		PROGRAM-1a	

While individual cybersecurity practices are important, a cybersecurity program is critical because it provides a structured and centralized approach to protecting digital assets, managing risks, and ensuring business continuity in the face of evolving cyber threats.

CGT1.a. Does your cybersecurity program team have sufficient resources (personnel, funding, and tools) to achieve its goals? (2 points)

A lack of sufficient resources limits the effectiveness of any cybersecurity program.

CGT2 – Senior Management Sponsorship

CGT2. Does your utility's cybersecurity function have senior management sponsorship? (8 points)

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
GV.RR-01		PROGRAM-2a; 2c; 2d	

It is important for senior executives to treat cybersecurity as a critical business imperative rather than just an IT issue. This buy-in typically indicates that the organization's leadership actively supports, funds, and enforces security initiatives, ensuring they align with overall business strategies and risk management goals. Senior management sponsorship of cybersecurity work helps ensure strategic alignment, resource prioritization, and organizational accountability, transforming security from a technical concern into a fundamental organizational priority.

CGT3 – Roles and Responsibilities

***CGT3. Does your utility have formally assigned roles and responsibilities for cybersecurity?* (8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
GV.RR-02		WORKFORCE-3a:d	

Formally assigning roles and responsibilities for cybersecurity ensures accountability, improves coordination, and strengthens your organization's ability to prevent, detect, and respond to threats. Without clear ownership, security efforts can become fragmented, inconsistent, or neglected.

***CGT3.a. Does your utility perform background checks or other methods of personnel vetting for employees and contractors with cybersecurity responsibilities?* (4 point)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		WORKFORCE-1c	

Because individuals with cybersecurity responsibilities often have access to sensitive systems, data, and infrastructure, trust alone isn't enough. Verification is important for reducing insider threats and ensuring organizational security.

CGT4 – Password Policy

***CGT4. Does your utility have password policies for IT systems?* (2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	5.2	ACCESS-1d	

Weak or inconsistent password practices are one of the most common entry points for attackers. Password policies define and enforce requirements that can help reduce the risk of unauthorized access, protecting sensitive data and systems from cyber threats.

***CGT4.a. Do these policies include (select all that apply):* [up to 12 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
			2.A:C

- ***Minimum requirements for user-generated passwords* (4 points)**
- ***Use of unique passwords* (4 points)**
- ***A requirement to change default passwords in systems and applications* (4 points)**

Minimum requirements for user-generated passwords can help ensure that users create strong, hard-to-guess passwords that can reduce the likelihood of successful brute-force or credential-stuffing attacks. Requiring unique passwords across different systems limits attackers' ability to use compromised credentials for one system to gain unauthorized access to many.

Default passwords are often published in manuals or online forums, which are easily accessible by threat actors. These default credentials tend to be widely known and easily exploited. A requirement to change default passwords removes some potential low-hanging fruit for attackers.

CGT4.b. Does your utility provide or recommend a password manager to employees? (2 points)

Password managers simplify compliance with password policies by helping users generate complex passwords, autofill those passwords to avoid memorizing (or writing down) each one, and ensure unique passwords for all accounts.

CGT4.c. Does your utility have password policies for OT systems, where applicable? (2 points)

See CGT4. And CGT4.a.

CGT5 – Access Control Policy

***CGT5. Does your utility have a cyber access control management policy for IT systems?* (8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.AA-05	6.1	ACCESS-2a	

Access control policies can help ensure that only authorized users can access specific systems, data, and resources. By using role-based access controls and ensuring users can only access what is necessary for them, you can minimize the potential consequences of account breaches, insider threats, or human error.

***CT5.a. Does your utility have a cyber access control management policy for OT systems?* (8 points)**

Access control is also critical for OT systems, given the potential for unauthorized access to disrupt or physically damage grid infrastructure.

***CT5.b. Does your utility have a policy for revoking access when no longer needed?* (4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	6.8	ACCESS-2b; 1f	2.D

Access that lingers beyond its purpose creates unnecessary risk. When employees change roles or leave the organization, or when contractors are no longer performing work, you should

promptly revoke accesses associated with their account to reduce potential entry points for attackers and prevent unauthorized use.

CT5.c. How frequently do you review access permissions to ensure policy compliance? **[up to 3 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	6.8	ACCESS-2h	

- ***Less than annually*** **(0 points)**
- ***Annually*** **(1 point)**
- ***Quarterly*** **(2 points)**
- ***Monthly*** **(3 points)**

Like a control audit, periodically reviewing access permissions to ensure compliance can help reduce privilege creep and misaligned access, reducing the risk of malicious or unintentional unauthorized access.

CGT6 – Information Sharing

CGT6. Does your utility share cybersecurity information with relevant organizations (e.g., E-ISAC, APPA, MS-ISAC, CRISP, ETAC)? **(4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		THREAT-1i	

Sharing threat intelligence helps build collective resilience against increasingly sophisticated cyberattacks. When organizations share relevant information with the community, it allows others to detect and respond to threats faster and more effectively.

CGT7 – Training for Cybersecurity Employees

CGT7. Does your utility provide role-based cybersecurity training to employees with cybersecurity responsibilities? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.AT-02	14.9	WORKFORCE-4a; 4f	2.J

Role-based cybersecurity training tailors education to the specific risks, responsibilities, and tools that each employee encounters, making training more relevant, effective, and actionable. Tailoring training to specific roles and responsibilities can help focus information on practical, job-specific scenarios.

CGT7.a. Does your utility also provide role-based cybersecurity training to contractors? **(2 points)**

Contractors may have similar access to your organization's networks and systems and can similarly benefit from role-specific training, where applicable.

CGT8 – Cybersecurity Awareness Training

CGT8. Does your utility provide cybersecurity awareness training to all employees? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
PR.AT-01	14.1-14.8	WORKFORCE-4d	2.I

Cybersecurity awareness training empowers employees to recognize and respond to threats, reduces human error, and strengthens an organization's overall security posture. Training helps employees avoid common pitfalls, including falling for phishing or social engineering schemes and mishandling sensitive data.

CGT8.a. How often do you conduct training? **[up to 3 points]**

- ***At least quarterly*** **(3 points)**
- ***Annually*** **(2 points)**
- ***Less than annually*** **(1 point)**

One-time training isn't enough to build lasting vigilance among employees. Cyber threats evolve constantly, and most employees need regular refreshers to stay alert, informed, and prepared.

CGT8.b. How frequently do you incorporate any testing (e.g., simulated phishing attacks)? **[up to 3 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		WORKFORCE-4e	

- ***Monthly*** **(3 points)**
- ***Quarterly*** **(2 points)**
- ***Annually*** **(1 point)**
- ***Less than annually*** **(0 points)**

If you do not incorporate any testing, select 'less than annually.'

Testing of basic cybersecurity skills taught in awareness training helps transform passive learning into active defense, helping employees practice real-world scenarios, reinforce knowledge, and build instinctive responses to threats.

CGT8.c. Does your utility also provide cybersecurity awareness training to all contractors (or verify that contractors otherwise receive awareness training)? **(1 point)**

Contractors that have access to your systems and networks should have similar cyber awareness training to your employees, whether your organization provides that training or they receive it elsewhere.

Cyber Incident Response (CIR) Section

This section contains a sequential, question-by-question review of the CAP application's Cyber Incident Response section. The guide explains each question in this section and outlines the scoring rubric, if applicable. The section also identifies which elements of the NIST CSF, CIS Controls, DOE C2M2, and NARUC Baselines may be relevant to the question.

CIR1 – Incident Declaration

CIR1. Does your utility have criteria in place to assess whether cybersecurity events constitute an incident? **(4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
DE.AE-08	17.9	RESPONSE-2d	

Having clear criteria to assess when a cybersecurity event constitutes an incident is essential for timely, consistent, and effective response. Applying these criteria ensures that your organization can distinguish between routine anomalies and serious threats, enabling appropriate action and resource allocation.

CIR1.a. Does your utility have established criteria for when it must report a cyber incident to relevant regulatory or other bodies? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
RS.CO-03		SITUATION-3d; RESPONSE-2g; RESPONSE-3c	4.A

Knowing when your organization needs to report a cyber incident to relevant stakeholders can ensure compliance with external requirements and support consistent decision-making.

CIR2 – Cyber Incident Response Plan

CIR2. Does your utility have a cyber incident response plan? **(24 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
RS.MA-01	17.4	RESPONSE-3d	2.S

While security controls are critical for protecting your organization's networks and systems, it is equally important to have a robust plan in place to manage cyber incidents if they occur. A cyber incident response plan is essential for handling incidents quickly and effectively to minimize potential consequences.

APPA has guidance available on developing an incident response plan and many of the elements you might want to include, available in the Cyber Incident Response Playbook.

CIR2.a. Does that plan include roles and responsibilities for specific personnel in cyber incident response? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	17.5	RESPONSE-3a	

Defining roles and responsibilities in the plan helps ensure clarity and coordination during a crisis, and can help avoid duplicating – or worse, neglecting – important tasks. Pre-defined roles and responsibilities can also support accountability in the incident response process.

CIR2.b. Does that plan include processes for tracking and logging progress? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		RESPONSE-2f	

Tracking and logging progress during a cyber incident ensures that every action or decision taken is documented, coordinated, and reviewable. Doing so provides visibility and accountability and can help both during the incident response and the post-incident review.

CIR2.c. Does that plan identify third parties that your utility might call on to support response efforts? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		RESPONSE-3j	

For incidents that exceed your organization's ability to respond in a timely or effective manner, it is important to reach out to trusted partners to support your response effort. This may include contractors and service providers, cyber mutual assistance program participants, APPA, and government partners at the local, state, or federal level.

CIR2.d. Does that plan include emergency contact information for internal and/or external points of contact? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	17.2		

Including and maintaining emergency contact information is crucial for rapid communication, coordination, and escalation in a crisis. When time is critical, knowing who to call and how to reach them can make a meaningful difference in the incident's outcome.

CIR2.e. Does that plan include a playbook or guideline of recommended actions for certain scenarios? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	17.3		

Including recommended actions can provide step-by-step guidance tailored to specific types of incidents, helping to ensure fast, consistent, and effective response under pressure. Consistency in response approaches can reduce errors, reduce uncertainty about appropriate courses of action, and solidify best practices. Playbooks can also support incident response training and exercises.

CIR2.f. Does that plan have processes and procedures specific to responding to incidents in your OT system(s)? **(2 points)**

Incidents involving OT systems will likely have different considerations than an IT-only breach. Outlining relevant OT-specific steps or requirements can improve responses to such incidents.

CIR2.g. How frequently does your utility exercise that response plan?

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	17.7	RESPONSE-3g	

- ***Annually*** **(3 points)**
- ***Every two years*** **(2 points)**
- ***Less than every two years*** **(1 point)**
- ***Never*** **(0 points)**

Exercising your incident response plan helps turn theory into practice, helping your team respond swiftly, confidently, and effectively if a real cyber incident occurs. Exercises can also identify potential gaps in response plans and can support the process of updating them to meet your organization's needs. Exercising the plan at least annually helps team members understand their specific roles and responsibilities in an incident, which can improve their ability to respond if one occurs.

CIR3 – Cybersecurity Integration into Business Continuity

CIR3. Is cybersecurity and cyber incident response part of your utility's continuity of operations (COOP), business continuity, or disaster recovery planning? **(4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		RESPONSE-4a; 4d	5.A

In today's threat environment, cyber threats can disrupt critical functions just as severely as natural disasters or other system failures. Integrating cyber incident response planning into broader COOP or business continuity planning ensures your organization is treating digital threats with the same urgency and consideration as physical disruptions.

Cyber Risk Management (CRM) Section

This section contains a sequential, question-by-question review of the CAP application's Cyber Risk Management section. The guide explains each question in this section and outlines the scoring rubric, if applicable. The section also identifies which elements of the NIST CSF, CIS Controls, DOE C2M2, and NARUC Baselines may be relevant to the question.

CRM1 – Threat Management

CRM1. Does your utility gather information on threats (e.g., threat actors and common tactics, techniques, and procedures) and review it for applicability to your organization? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.RA-02; ID.RA-03		THREAT-2b	3.A

Threat intelligence helps your organization detect and prevent attacks before they occur by identifying emerging tactics, techniques, and procedures used by threat actors. This information can also help your cybersecurity team understand the current threat landscape and prioritize defensive actions accordingly.

CRM1.a. How does your utility approach managing threats (including strengthening security protections, increasing monitoring activities, and/or raising awareness throughout the organization)? **[up to 2 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
		THREAT-2d	

- ***Policy*** **(2 points)**
- ***Ad hoc*** **(0 points)**

A threat management policy provides a structured framework for identifying, assessing, and responding to cyber threats and can help ensure consistent, proactive, and effective protection across the organization.

CRM2 – Vulnerability Management

CRM2. Does your utility gather information on vulnerabilities and review it for applicability to your assets and systems? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines

ID.RA-01	7.1	THREAT-1a; 1b	1.E

The vulnerability management process is crucial for proactively identifying, prioritizing, and remediating vulnerabilities before they can be exploited. Because you cannot control the intent and capability of attackers (threats), vulnerability management is the only way to reduce the likelihood of facing a cyber incident.

CRM2.a. Does your utility proactively scan for potential vulnerabilities? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	7.5; 7.6	THREAT-1c; 1f	

Proactively scanning for potential vulnerabilities can help your organization identify and remediate vulnerabilities in a timely manner. A proactive approach helps provide ongoing visibility into your security posture and can help track improvement over time.

CRM2.a.i. How frequently does your utility conduct vulnerability scans? **[up to 3 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	7.5; 7.6		

- ***At least weekly*** **(3 points)**
- ***Monthly*** **(2 points)**
- ***Quarterly*** **(1 point)**
- ***Less than quarterly*** **(0 points)**

A greater frequency of scanning increases the chances that you will identify potential vulnerabilities before an attacker can exploit them.

CRM2.b. How does your utility approach managing applicable vulnerabilities (e.g., patching or other changes)? **[up to 2 points]**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
	7.2; 7.7; 16.6	THREAT-1d	

- ***Policy*** **(2 points)**
- ***Ad hoc*** **(0 points)**

A vulnerability management policy provides a structured, repeatable approach to identifying, assessing, and mitigating vulnerabilities. A formal policy can help ensure timely identification and remediation of vulnerabilities.

CRM3 – Cyber Risk Assessment and Prioritization

CRM3. Does your utility identify and assess cybersecurity risks to your organization? **(12 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.RA-05		RISK-2a; 3a	

Cyber risk assessment involves a thoughtful consideration of how different risks – a function of threats, vulnerabilities, and consequences – could result in unwanted outcomes for your organization. This process often involves a qualitative or quantitative comparison of risks, which allows for prioritization of mitigation efforts and resources.

At a basic level, many risk assessments will plot individual risk entries as a function of likelihood (which considers threats and vulnerabilities) and consequence. The graphic below provides an example of a basic heat map your utility might use to categorize risks.

Likelihood	Very Likely	Low	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	High	Extreme
	Possible	Low	Low	Medium	High	Extreme
	Unlikely	Low	Low	Medium	High	High
	Very Unlikely	Low	Low	Low	Medium	High
		Negligible	Minor	Moderate	Major	Catastrophic
	Consequence					

For more information on how to conduct risk assessments for your utility, APPA has developed a Risk Management Toolkit for Public Power Utilities.

CRM3.a. Does the risk assessment process include the identification of critical assets and systems? **(8 points)**

In addition to identifying the greatest risks to your organization, you can leverage the risk assessment process to identify which assets and systems are most essential to your organization's operations and would result in the greatest consequences if disrupted.

CRM3.a.i. Does your utility prioritize resources and risk management activities for those assets and systems? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.RA-06		RISK-4b	

This process also supports risk-based prioritization of mitigation efforts and resource allocation. By prioritizing resources to mitigate risks to your most critical assets and systems, public power

utilities can apply their potentially limited resources in a way that will have the greatest impact in terms of reducing your cyber risk.

***CRM3.b. Does your utility manage those risks with some combination of acceptance, transference, avoidance, or mitigating activities?* (4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.RA-06		RISK-4a	

Your organization may not be able to mitigate every identified risk. However, there are three other potential options for managing risks: transference, avoidance, and acceptance.

- *Transference:* Shifting the impact of the risk to a third party (e.g., purchasing cyber insurance or outsourcing data storage to a secure cloud provider).
- *Avoidance:* Eliminating the activity or condition that gives rise to the risk (e.g., choosing not to store sensitive data online to avoid the risk of a data breach).
- *Acceptance:* Acknowledging the risk and choosing to proceed without additional controls (e.g., accepting the risk of using legacy systems due to budget constraints).
- *Mitigation:* Taking steps to reduce the likelihood or consequence of a given risk (e.g., implementing additional controls).

Some combination of these strategies is necessary to manage the broad range of risks your utility is likely facing.

CRM4 – Third Party Cybersecurity Vetting

***CRM4. Does your utility vet third-party suppliers for potential cybersecurity risks?* (12 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
ID.RA-10; GV.SC-06	15.5	THIRD-PARTIES-2d	1.I

Third-party suppliers of software, hardware, firmware, or managed services can become entry points into your networks and systems for attackers. A single weak link in your supply chain can provide attackers with access to your networks and systems, exposing your entire organization.

Using security questionnaires and audits, requiring relevant reports and certifications, including cybersecurity clauses in contracts, and conducting period reviews can all help reduce third party risks. However, even some of the largest providers may be susceptible to compromise and make you vulnerable to third-party risks as a result.

***CRM4.a. Does your utility have established cybersecurity requirements for third-party service providers?* (2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
GV.SC-05		THIRD-PARTIES-2a	

While cybersecurity requirements cannot guarantee that incidents will not occur, ensuring that providers meet industry standards can help reduce the risk of third-party compromise.

CRM4.b. Does your utility have established cybersecurity requirements for third-party product (e.g., hardware, software, firmware) providers? **(2 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
GV.SC-05		THIRD-PARTIES-2b	

See CRM4.a.

CRM4.c. Does your utility conduct any vendor, equipment, or software risk assessments before procuring IT or OT systems or services? **(2 points)**

Conducting risk assessments as a part of the procurement process can help ensure that new systems or services align with your organization's security, operational, and compliance requirements. Separate from ongoing efforts to assess risks associated with trusted third parties, it is important to conduct point in time assessments to understand the potential new risks to your system from incorporating new vendors, equipment, or software.

CRM5 – Third Party Risk Assessment

CRM5. Does your utility assess potential cybersecurity risks from the compromise of a third-party provider? **(8 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
GV.SC-07	15.3; 15.6	RISK-2k	

Third-party providers often have access to your systems or data and play important roles in sustaining your day-to-day operations. As a result, the compromise of a third-party provider you rely on can either greatly increase your own cyber risk or, if the provider is offline, could potentially leave you without critical software or services. Identifying these risks and introducing compensating controls is essential for reducing your organization's potential exposure.

CRM6 – Insider Threat

CRM6. Does your utility monitor for indicators of potential malicious activity (e.g., unauthorized remote access, repeated failed access attempts, communication with known malicious websites or IP addresses)? **(4 points)**

NIST CSF	CIS Controls	DOE C2M2	NARUC Baselines
DE.CM-03		SITUATION-2d; ACCESS-2i	2.G

Because insider threats have some level of trusted access, their activity within your networks may not trigger traditional security alerts. However, there are some technical and behavioral indicators that could provide early warning signs of malicious intent or activity. Monitoring for these indicators can help reduce the risk of insider threats, which could result in data breaches or impacts on operations.

CRM6.a. Does your utility have a cyber-specific insider threat program? **(2 points)**

A cyber insider threat program helps detect, prevent, and respond to threats originating from within your organization, whether intentional or accidental. Insiders often have trusted access, making them uniquely capable of causing significant harm if not properly monitored and managed.

Appendix A: CAP Scoring Criteria Summary

Category	Question	Subject of Question	Maximum Point Value
Internal Controls (30%)	IC1	IT Asset Inventory	10
	IC2	OT Asset Inventory	10
	IC3	Crown Jewel Analysis	8
	IC4	Data Inventory	8
	IC5	Configuration Baselines	14
	IC6	Data Backup	31
	IC7	Identity and Access Management	28
	IC8	Physical Access Controls for Digital Assets	4
	IC9	Email and Web Traffic Protections	5
	IC10	Network Segmentation	24
	IC11	Logging	13
	IC12	Monitoring	28
	IC13	Controls Audit	16
		Category Total	**199**
Cybersecurity Governance and Training (20%)	CGT1	Cybersecurity Program	10
	CGT2	Senior Management Sponsorship	8
	CGT3	Roles and Responsibilities	12
	CGT4	Password Policy	18
	CGT5	Access Control Policy	23
	CGT6	Information Sharing	4
	CGT7	Training for Cybersecurity Employees	10

Appendix A: CAP Scoring Criteria Summary (continued)

Category	Question	Subject of Question	Maximum Point Value
	CGT8	Cybersecurity Awareness Training	15
		Category Total	**100**
Cyber Incident Response (25%)	CIR1	Incident Declaration	6
	CIR2	Cyber Incident Response Plan	39
	CIR3	Cybersecurity Integration into Business Continuity	4
		Category Total	**49**
Cyber Risk Management (25%)	CRM1	Threat Management	10
	CRM2	Vulnerability Management	15
	CRM3	Cyber Risk Assessment and Prioritization	32
	CRM4	Third Party Cybersecurity Vetting	18
	CRM5	Third Party Risk Assessment	8
	CRM6	Insider Threat	6
		Category Total	**89**