

**NERC**

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

FINAL REPORT

# Regional Entity Compliance Monitoring and Enforcement Program (CMEP 4A) Audit

## Texas Reliability Entity, Inc. (Texas RE)

Date: August 31, 2022

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE  
Suite 600, North Tower  
Atlanta, GA 30326  
404-446-2560 | [www.nerc.com](http://www.nerc.com)



## EXECUTIVE SUMMARY

### Texas RE CMEP Appendix 4A Audit

#### Background

The **Texas RE**, is a Texas 501(c) (3) non-profit corporation that is the Regional Entity for the area of Texas served by the Electric Reliability Council of Texas (ERCOT). Through a Delegation Agreement with the North American Electric Reliability Corporation (NERC), which is approved by the Federal Energy Regulatory Commission (FERC), Texas RE is authorized to develop, monitor, assess, and enforce compliance with NERC Reliability Standards, develop regional standards, and assess and periodically report on the reliability and adequacy of the bulk power system in the ERCOT region. Texas RE is independent of all users, owners, and operators of the BPS.

There are approximately 293 registered entities in Texas RE's footprint. The membership sectors are: System Coordination and Planning, Transmission and Distribution, Cooperative Utility, Municipal Utility, Generation, and Load-Serving and Marketing.

Texas RE provides a robust program to oversee and ensure reliability of the ERCOT Interconnection, which covers approximately 75 percent of Texas' land area and 90 percent of its electricity load. The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Program, which is required at least once every five years.

Texas RE has participated in periodic self-certifications related to its CMEP and activities up to the period of this engagement. The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

#### Audit Summary

The audit objective is to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreement.

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC.

Throughout the audit, Texas RE staff were both accommodating and responsive to requests from IA, and their diligence and professionalism were appreciated.

Noteworthy remarks to Texas RE's CMEP program are as follows:

- Texas RE CMEP Engage tool is a comprehensive in-house software platform tool that serves well for maintaining IRA, COP, performance considerations, and other CMEP monitoring activities.
- Texas RE thoroughly tracks CMEP staff training and education.
- The multi-year audit schedule is a holistic resource for tracking audit and self-certification activity across the RE footprint. The tracker captures scheduling from 2006 to 2030, and includes each entity’s registered functions, NERC ID (i.e. NERC Compliance Registry #), MRRE LRE/ARE designation, and COP monitoring interval.

During the course of the audit, we identified themes related to inconsistent process execution. For example, we noted the exclusion of applicable NERC CMEP IP risk elements into compliance oversight plans and audit scoping; a deviation from the COP procedure; and long-term compliance monitoring intervals for some lower-risk registered entities.

The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Period and Scope	Observation Summary				
The period under review was January 1, 2020 through December 31, 2021.	<u>Ratings</u>				
The scope included the following:	<b>Area</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>	<b>Total</b>
<ul style="list-style-type: none"> <li>• Governance/Regional Delegation Agreements (RDA)                             <ul style="list-style-type: none"> <li>○ Compliance Registry - CMEP Contacts</li> <li>○ Conflict of Interest (Board and Employees)</li> <li>○ Training</li> </ul> </li> </ul>	Governance	0	0	0	0
<ul style="list-style-type: none"> <li>• Risk Assessment/Risk Categories/Factors/Elements                             <ul style="list-style-type: none"> <li>○ Inherent Risk Assessment</li> <li>○ Regional Risk Assessment</li> <li>○ Potential Non-Compliance (PNC)</li> <li>○ Mitigating activities</li> </ul> </li> </ul>	Risk Assessment	0	1	0	1
<ul style="list-style-type: none"> <li>• Compliance Oversight Plans (COPs)                             <ul style="list-style-type: none"> <li>○ Entity Risk Profile (ERP)</li> <li>○ Internal Controls</li> </ul> </li> </ul>	COPs	0	1	0	1
<ul style="list-style-type: none"> <li>• Enforcement activities and actions                             <ul style="list-style-type: none"> <li>○ Issue processing</li> <li>○ Disposition determination</li> <li>○ Penalty processes/assessments</li> </ul> </li> </ul>	Enforcement	0	0	0	0
<ul style="list-style-type: none"> <li>• Compliance Monitoring Processes and Tools                             <ul style="list-style-type: none"> <li>○ Compliance Audits, Spot Checks, Self-Reports, Self-Logging, Self-Certifications</li> <li>○ Periodic Data Submittals (PDS)</li> </ul> </li> </ul>	Monitoring Tools	0	0	1	1
<ul style="list-style-type: none"> <li>• Supporting Activities                             <ul style="list-style-type: none"> <li>○ Compliance Audits, Spot Checks, Self-Reports, Self-Logging, Self-Certifications</li> <li>○ Periodic Data Submittals (PDS)</li> </ul> </li> </ul>	Supporting Activities	0	0	0	0
<ul style="list-style-type: none"> <li>• Supporting Activities                             <ul style="list-style-type: none"> <li>○ Methodologies and Processes</li> <li>○ CMEP IP, Annual ERO Oversight Plan</li> <li>○ Physical Security</li> </ul> </li> </ul>	<b>Total</b>	<b>0</b>	<b>2</b>	<b>1</b>	<b>3</b>

<b>High/Medium/Low-Risk Rated Observations</b> <i>(High, medium, and low risk observations require a management action plan)</i>		
Rating	Observation	Risk
Medium	Exclusion of relevant CMEP IP Risk Element Standards and Requirements from Entities' Compliance Oversight Plans was not justified or supported through documented rationale	Excluding NERC CMEP IP Risk Element Standards and Requirements from an applicable entity's COP results in reduced or incomplete monitoring; potential for risks to be unmitigated and/or lead to non-compliance, adversely impacting reliability and security.
Medium	Adherence to local policy for development of COPs is not followed.	An oversight strategy is not defined, along with the appropriate monitoring tools and interval to manage risk.
Low	Compliance monitoring category levels for lower risk entities in COPs did not reconcile to the audit schedule prepared by Texas RE. Several entities with category 5 designations were scheduled for 8-year intervals.	Inconsistent application of the ERO Enterprise Oversight strategy and lack of support or rationale for changes reduce the effectiveness of CMEP in ensuring reliability and security across all entities within its footprint in a risk-based manner.

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
1.	Risk Assessment Rules of Procedure; Section 400.401.6 Risk Elements	<p><b>Exclusion of relevant CMEP IP Risk Element Standards and Requirements from Entities' Compliance Oversight Plans was not justified or supported through documented rationale</b></p> <p>Review of the COPs created in the audit period against the CMEP IP Risk Elements applicable standard and requirements identified that multiple COPs exclude standards and requirements that should apply to the entity.</p> <ul style="list-style-type: none"> <li>Five entities had a total of 34 applicable Standards and Requirements excluded with no clear action for monitoring or oversight plan.</li> </ul> <p>As noted in the "Conducting Inherent Risk Assessments" DESK 10.18, the COP is used to "create a scope for an upcoming engagement, Risk Staff will consult the COP for the list of Requirements selected for active oversight". In addition, the "COP process uses this information to create a COP consisting of all Requirements applicable to the entity, the monitoring methods available for oversight, and the monitoring interval for the entity". The CMEP IP 2020 states that "notably, the implementation plan is not intended to be a representation of just "important" Reliability Standards requirements; rather, it is intended to reflect the ERO</p>	Texas RE appreciates the auditors' observation regarding the opportunity to enhance Texas RE's policies and procedures for documenting its review of, inclusion or exclusion, and proposed monitoring for CMEP IP Risk Elements. To address this observation, Texas RE will adopt process enhancements to improve Texas RE's documented justifications when it elects to exclude the Requirements associated with applicable Risk Elements from Appendix B of the registered entity's COP.	October 31, 2022	<p>Regional Entity Director, O&amp;P Compliance and Risk Assessment</p> <p>Regional Entity Manager, Risk Assessment</p>	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		<p>Enterprise’s prioritization within its CMEP based on its inputs and to communicate to registered entities to bring collective focus within their operations to address each prioritized risk”. This illustrates the importance of the risk element standards being prioritized, monitored, and included for oversight action.</p> <p>There are no procedures or protocols to ensure that the identified NERC CMEP IP Risk Elements for the year are included in the COP for the applicable entity.</p> <p>Failure to review or properly assess NERC CMEP IP Risk Elements and their applicability to a registered entity’s compliance oversight could result in detecting risks and threats to the bulk power supply system.</p> <p>Either create or include in policy and procedures documentation of a direct review of NERC CMEP IP Risk Elements, how they are assessed and then included or excluded, and their monitoring for applicable entities.</p>				
2.	<p><b>Compliance Oversight Plan (COPS)</b></p> <p><b>ROP RE Risk-based compliance</b></p>	<p><b>Adherence to local policy for COP development is not followed</b></p> <p>Development and refreshing of COPs based on other significant performance considerations and monitoring activities</p>	<p>Although Texas RE believes the entity in question has elements of a COP in place, Texas RE acknowledges the audit team’s observation regarding the importance of timely development and</p>	<p>December 31, 2022</p>	<p>Regional Entity Director, O&amp;P Compliance and Risk Assessment</p>	<p>Medium</p>

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
	oversight 403.10	<p>doesn't necessarily lead to development of refreshing of a COP.</p> <p>A COP was not developed for a registered entity that experienced significant performance considerations from the period of 2018 to present.</p> <ul style="list-style-type: none"> <li>• Two anonymous complaints were filed in 2019</li> <li>• Physical Security Event in 2019</li> <li>• Unannounced audit in 2020</li> </ul> <p>Texas RE's 'Developing Compliance Oversight Plans Procedure' states Texas RE develops a COP for every Registered Entity in its region, and staff stated a COP will be developed for each newly registered entity within six months. Triggers may result in refreshing a COP, such as a change in one or more performance considerations impacting the risk category and subsequently the oversight strategy.</p> <p>Texas RE provided a 2018 IRA Summary Report, and Internal Work Papers (2021 IRA Risk Factor Analysis, and Risk Performance Data spreadsheet) to the audit team. A COP serves both internal and external parties, and Texas RE was not able to provide evidence of articulating the oversight strategy to the entity since 2018, although performance considerations changed.</p>	<p>updating entity COPs as conditions warrant and per our internal COP procedure. Texas RE is in the process of implementing a risk-based schedule for revising COPs to use the current ERO COP template, and that risk-based schedule anticipates that in 2022 Texas RE will refresh the COP for the registered entity at issue to reflect the most current facts and circumstances in advance of the registered entity's next scheduled compliance engagement.</p> <p>To address the observation more generally, Texas RE will adopt process improvements to include creating or refreshing a COP using the most current ERO COP template in advance of future unscheduled Compliance Audits.</p>		Regional Entity Manager, Risk Assessment	



Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		<p>While Texas RE’s COP interval scheduler indicated a COP would be developed in 2020, the target date was moved to end of 2022 ahead of the 2023 guided self-certification.</p> <p>The current oversight strategy may not accurately represent a risk-based approach, or designating the proper monitoring tools and intervals without a relevant COP based on consideration of multiple performance considerations (i.e. Culture of Compliance events).</p> <p>Risk management should ensure that IRAs and COPs are developed according to internal procedures, leveraging the most current ERO Enterprise guidance, tools and templates.</p>				
3.	<b>Compliance Monitoring Rules of Procedure; Section 400.3.1 Compliance Audits</b>	<p><b>Compliance Monitoring Intervals for Low-Risk Registered Entities</b></p> <p>Six of seven lower-risk registered entities sampled were designated as Category 5 in their respective COPs, yet Texas RE’s audit schedule tracker indicates 8-year monitoring intervals, with no compliance monitoring tools utilized in the interim.</p> <p>The NERC Compliance Oversight Plan Process Enhancements guidance (November 13, 2020), includes for the oversight strategy, that Category 5, lower inherent risk without demonstrated positive performance should be monitored</p>	<p>Texas RE appreciates the audit team’s observation. To address the audit team’s recommendations, Texas RE will review other Regional Entities’ processes for capturing periodic changes to entity inherent risk, as well as demonstrated positive performance. Based on this review, Texas RE will consider process improvements that are a fit for the Texas RE footprint’s unique characteristics, including Texas RE’s access</p>	October 31, 2022	<p>Regional Entity Director, O&amp;P Compliance and Risk Assessment</p> <p>Regional Entity Manager, Risk Assessment</p>	Low

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		<p>between 5-7 years. Category 6, lower inherent risk with demonstrated positive performance at 6+ years.</p> <p>To extend compliance monitoring of registered entities beyond 7 years without intermittent monitoring can increase risk to reliability and security. In addition, COP monitoring categories should reflect the appropriate monitoring interval, along with associated department tracking mechanisms.</p> <p>Texas RE should monitor lower-risk entities in between long interval engagements by capturing evidence of demonstrated positive performance on Reliability Standards that are applicable to the entity. An example would be an annual risk questionnaire to all registered entities, with responses due and appropriate follow up and monitoring, in line with a risk-based monitoring approach. In addition, Texas RE should ensure that it develops clear, documented justifications if monitoring intervals are extended for lower-risk entities.</p>	<p>to real-time performance data within the Texas Interconnection that may obviate the need to request certain performance information and data directly from registered entities via a questionnaire.</p> <p>In addition, Texas RE will adopt process improvements to ensure that Texas RE develops clear, documented justifications if monitoring intervals are extended for lower-risk entities. These process improvements will include a periodic reassessment of the justification during the period between compliance engagements in situations in which Texas RE has elected to extend entity intervals, including a reassessment of the entity's overall Compliance Oversight Plan</p>			

## Appendix

### Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

### Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.