NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

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

SERC Reliability Corporation

May 17, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Jason Blake, President and CEO

From: NERC Internal Audit

Date: May 17, 2022

Subject: CMEP 4A Audit - SERC

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity (RE) Compliance Monitoring and Enforcement Program (CMEP 4A) Audit.

The audit objective was 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 delegation agreements.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Manny Cancel, NERC
Lonni Dieck, SERC (Board)
Kelly Hanson, NERC
Holly Hawkins, SERC
Todd Hillman, SERC (Board)
Mark Lauby, NERC
Sonia Mendonca, NERC
Jim Robb, NERC
Janet Sena, NERC
Brian Thumm, SERC

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

SERC Reliability Corporation (SERC)
CMEP Appendix 4A Audit

Background

The **SERC Reliability Corporation** (**SERC**), is located in Charlotte, NC and is responsible for the reliability and security of the electric grid across the southeastern and central regions of the United States. This area covers approximately 630,000 square miles and serves a population of more than 91 million. It includes all or portions of Florida, Georgia, Alabama, Mississippi, Louisiana, Texas, Oklahoma, Arkansas, Missouri, Iowa, Illinois, Kentucky, Tennessee, Virginia, North Carolina, and South Carolina. SERC's footprint includes approximately 267 registered entities.

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.

Effective as of 2019, the RAM and Enforcement departments completed two separate and significant process improvement projects to improve SERC's timely resolution and mitigation of noncompliance. The groups collaborated on scope of the violations, risks, and root causes to determine required mitigation activities to remediate violations and prevent reoccurrence. In 2021, SERC's initiatives drove marked programmatic improvements. SERC processed 402 violations, a 24% reduction of violations from 2020, reducing the total inventory to 304 violations by the end of the year, and reducing the average age of inventory from 13.7 months to 10.7 months.

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 agreements.

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 utilization of monitoring tools as defined within the ROP, or directed by NERC.

SERC improved processes over the last year which led to efficiencies throughout their CMEP program. For example, SERC restructured their CMEP department in September 2021, by creating a Risk Awareness and Oversight (RAO) department to focus efforts on Inherent Risk Assessment (IRA), Entity Risk Profile (ERP), and Compliance Oversight Plans (COPs), and to ensure SERC is deploying its internal resources effectively to reduce risk to the BPS. SERC's Risk Assessment and Mitigation (RAM) department took the initiative to provide a mentor program for new RAM hires, by

shadowing a senior staff member until a probationary period ends, at which time the staff can complete work on their own, as a means of solidifying process and responsibilities. SERC has prioritized focus on Facility Ratings, as demonstrated by performing outreach, lessons learned, and virtual presentations to stakeholders across the ERO Enterprise. In addition, SERC's Data Analytics department provides dashboards which report trends and status of critical components of CMEP activities, such facility ratings, GADS/TADS/MIDAS performance, and others. This effort showcases SERC's diligence to use data as a tool for CMEP. Lastly, efficiencies were evident through improved coordination between RAM and Enforcement review of potential noncompliance, streamlining the process by eliminating backlog and aged issues.

During the course of the audit, we identified themes related to inconsistent process execution. For example, there were inconsistencies in the development of Inherent Risk Assessment (IRA), Entity Risk Profiles (ERP), and Compliance Oversight Plans (COPS); SERC's internal oversight of training and learning program objectives for CMEP staff; monitoring of industry subject matter experts conflict of interest disclosure; and SERC's evaluation of Registered Entity internal controls during registered entity audit pre-planning and planning activities. In addition, newly hired CIP auditors had a lengthy delay in completing the required NERC auditor training. These inconsistencies may negatively impact risk-based audit scoping, as well as auditor preparedness respectively.

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment
  - Regional Risk Assessment
  - Potential Non-Compliance (PNC)
  - Mitigating activities
- Compliance Oversight Plans (COPs)
  - Entity Risk Profile (ERP)
  - Internal Controls
- Enforcement activities and actions
  - Issue processing
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits, Spot Checks, Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)
- Supporting Activities
  - Methodologies and Processes
  - CMEP IP, Annual ERO Oversight Plan
  - Physical Security

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	3	0	3
Risk Assessment	0	0	0	0
COPs	0	2	0	2
Enforcement	0	0	0	0
Monitoring Tools	0	0	0	0
Supporting Activities	0	0	0	0
Total	**0**	**5**	**0**	**5**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Rating	**Observation**	**Risk**
Medium	CMEP staff auditor training was not monitored for timely completion	Associates may not be equipped to provide the subject matter expertise or demonstrate the responsibilities necessary to consistently and accurately perform CMEP duties.
Medium	Training and learning program process documentation for CMEP staff is not formalized	Staff is not effectively executing responsibilities of the role and building capabilities to grow and develop skills in critical program areas. Gaps in training of staff and ensuring adherence to training policy can lead to ineffective execution of expected performance.
Medium	COI process was not consistently applied to Industry Subject Matter Experts	Conflicts of Interest (COI) are not detected and result in undue influence over or bias over CMEP activities.
Medium	IRA-ERP-COP Inconsistencies in Peer Review	Inadequate risk oversight of the registered entities.
Medium	Evaluations of Internal Controls lacked consistency	Lack of registered entity understanding of internal controls, and lack of internal controls procedures, undermines a risk-based approach to compliance and reliability.

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
1.	**Governance: Training**	**CMEP staff auditor training was not monitored for timely completion** Auditors must complete all NERC or NERC-approved Regional Entity auditor training applicable to the Compliance Audit, per Section 3.1.5.2 of the ROP ('Foundations of Auditing' and 'Gather Quality Evidence'). Our audit identified two of three new auditors hired during the audit period that did not complete the required training timely • 21 weeks to complete training for one individual • One course remained incomplete after 14 weeks for another individual In addition, one of those new hire served on an audit team as an observer prior to completing the training per NERC procedure. Without ensuring staff completes required auditor training in a timely manner, and in conjunction with the requirements for an observer role, the individual may not be adequately prepared to execute procedures with the required knowledge or competencies. Management should ensure training is provided timely and consistent within NERC requirements for all CMEP new hires.	SERC agrees with the NERC observation that there are process improvements needed to ensure that CMEP staff auditor training is provided in a timely and consistent manner, within NERC requirements for all new hires. SERC commits to the following actions: Review and enhance processes to improve controls to validate that new hires are assigned the appropriate training and that the training is completed in the appropriate timeframe, including prior to assigning them as a member of an audit team Evaluate whether a dedicated, centralized resource is more effective and efficient than relying on separate department managers to implement the same process. This dedicated role could have the responsibility of assigning and validating	November 30, 2022	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Director of Reliability Assurance Regional Entity, Manager, Outreach & Training	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
			timely completion of all required CMEP training for new hires Whether centralized or decentralized, training program oversight will be responsible for escalating issues to management, and to maintain accurate tracking/records of all required CMEP staff training Update applicable guidance documents to reflect the method chosen for providing additional oversight to CMEP staff auditor training requirements Update audit planning process documentation to include a step that validates all audit team members have completed the required training prior to being assigned to an audit team			

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
2.	**Governance: Training**	**Training and learning program process documentation for CMEP staff is not formalized** CMEP staff should be trained on processes and tools related to their area of responsibility. SERC does not maintain formal training process documentation within each CMEP department, or in a centralized location. Without training and learning program documentation, personnel may not receive the guidance to perform their CMEP responsibilities. CMEP department's training and learning programs should include the development of formal training and learning process documentation, and the tracking of employee progress.	SERC agrees with the NERC observation that there are opportunities for improvement in documentation of training program processes. SERC commits to the following actions: Develop and maintain process documentation for a CMEP training program that includes a tracking mechanism to validate individual employee progress As noted for Observation #1, evaluate whether a dedicated, centralized resource is more effective and efficient than relying on separate department managers to implement the same process. Update applicable guidance documents to reflect the method chosen for enhancing training and learning program process documentation for CMEP staff	November 30, 2022	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Director of Reliability Assurance Regional Entity Manager, Outreach & Training	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
3.	**Governance: Conflict of Interest (COI)**	**COI process was not consistently applied to Industry Subject Matter Experts** SERC's COI and Business Ethics Policy for SERC Representatives requires that industry subject matter experts (ISMEs) disclose any COI from the time they are placed on an audit team until their involvement with the audit has completed. Of the two ISMEs assisting during the audit period, SERC was unable to provide a current COI for one individual. An actual or potential conflict of interest can increase the risk of bias and/or undue influence. SERC must ensure each ISME submits COI disclosure during the time they participate on audits in adherence to the COI and Business Ethics Policy. The policy should be updated to reflect any additional controls put in place.	SERC agrees with the NERC observation that there are opportunities for improvement to the process related to collecting and validating ISME COIs. SERC commits to the following actions: Review and enhance processes to improve controls to validate that an ISME completes a COI form prior to participating in each audit engagement they are assigned. Ensure audit planning process documentation includes a step that ensures validation that all audit team member requirements are met before participating in any engagement, including the completion of a COI form Reevaluate the protocols and safeguards surrounding ISME participation in audit engagements to ensure that such engagements do not create any appearance of a conflict of interest	November 30, 2022	Regional Entity VP, General Counsel & Corporate Secretary Regional Entity Director of Reliability Assurance	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
4.	**Compliance Oversight Plans: IRA-ERP-COP**	**IRA-ERP-COP Inconsistencies in Peer Review** The Inherent Risk Assessment, Entity Risk Profile, Compliance Oversight Plan (IRA-ERP-COP) procedure during the audit period required peer review of IRA-ERPs. A representative sample of registered entities selected within the audit period, noted the following: • 1 registered entity did not include evidence of peer review, an ERP, or a COP report • 1 ERP provided was not completed in its entirety (CMEP Implementation Plan Comparison table was not completed to demonstrate rationale for not including standards in the monitoring recommendation) The benefit of performing a peer review of IRA-ERPs is to maintain quality standards and improve performance. Without strengthening the review process, there may be inadequate risk oversight of the registered entities. SERC should ensure that there is a thorough review process in place for IRA-ERP-COPs to include determination that ERPs are filled out completely, and that each registered entity has all applicable documents reviewed and finalized. The integrity of the review process is	SERC agrees with the NERC observation that there are opportunities for improvement to the IRA-ERP-COP process to ensure consistent execution. SERC feels confident that the Risk Awareness and Oversight department that was formed in September 2021 to provide increased focus on IRA-ERP-COPs will address this observation. As SERC continues to develop the Risk Awareness and Oversight team, it commits to the following actions: Review and enhance process documentation to provide clarity on peer review expectations and validation of completeness. Ensure process documentation clearly states roles and responsibilities, preserves the objectivity and independence of the Risk Awareness and Oversight team's decision making	November 30, 2022	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Senior Manager, Risk Awareness & Oversight	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		paramount to detect and correct errors or omissions.	capability, and highlights the steps required to validate the completeness of records			
5.	**Compliance Oversight Plans: Internal controls**	**Evaluations of Internal Controls lacked consistency** Internal controls serve to minimize overall risk for failure of compliance. The Rules of Procedure and the NERC ERO Enterprise Guide for Internal Controls state that there should be a clear approach or procedure in which the Regional Entity evaluates the internal controls of a registered entity. SERC Registered Entities have varying levels of maturity with respect to Internal Controls. This was acknowledged during interviews with SERC staff, and evidenced by a registered entity sampled who was unable to respond to an internal control request for information as part of audit preplanning. SERC requested the entity develop an internal control program; however, there was no evidence of follow up or guidance/training, suggesting a lack of consistency in engaging with entities about their internal controls programs. This may result in unclear communication from SERC as to what the expectation is of a registered entity, as well as the required responses to internal control requests.	SERC agrees with the NERC observation that its program for assessing Registered Entity Internal Controls would benefit from additional consistency and documentation. SERC agrees that an enhanced approach to working with specific entities can help inform risk-based decisions about the sustainability of the individual entity's compliance program. This would also enhance the consistency of SERC's outreach in this space. SERC commits to the following actions: Evaluate potential programmatic changes, which will include the following elements: ○ identify entities with weak or no internal controls, to help SERC	February 1, 2023	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Director of Reliability Assurance Regional Entity, Senior Program Manager, Strategic Initiatives & Continuous Improvement	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		Without the consistent application of a process to review registered entity responses or questions related to internal controls, the effectiveness of the registered entity's mitigation of risk, and the opportunity to provide feedback on potential control weaknesses that may lead to non-compliance is limited. Internal controls are fundamental to a risk-based approach to ensuring reliability. Therefore, SERC should identify entities with weak or no internal controls and develop guidance or an approach to assist. This practice should exist outside the audit schedule to encourage registered entities to maintain and implement internal controls to increase the effectiveness of risk-based CMEP in ensuring reliability.	develop guidance or specific approaches for specific entities ○ increase specific awareness about internal controls deficiencies broadly across the Region and narrowly with specific entities ○ guide entities toward making appropriate decisions about the implementation of an internal controls program Evaluate opportunities to ensure consistent application of its process, and incorporate any changes necessary, as appropriate			

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.