NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL EXECUTIVE SUMMARY

CMEP Regional Entity Audit (Appendix 4A)

Consolidated Executive Summary

October 13, 2022

RELIABILITY | RESILIENCE | SECURITY




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

To: Sonia Mendonca, Senior Vice-President and General Counsel
Jim Robb, President and CEO

From: NERC Internal Audit

Date: October 13, 2022

Subject: Regional Entity Compliance Monitoring and Enforcement Program Audit

****

Enclosed is a consolidated Executive Summary of Internal Audit's observations related to Compliance Monitoring and Enforcement Program (CMEP) 4A Audits performed at the six Regional Entities.

The audit objective was to assess the Regional Entities' implementation of the NERC CMEP and determine whether the program effectively meets the requirements under the Rules of Procedure (ROP) Section 400, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements placed in the CMEP IP.

This Executive Summary provides additional context and summarizes broad themes from the observations described in greater detail in the individual audit reports already issued to each Regional Entity. It is intended to aid NERC, working within the ERO Enterprise collaboration structure, in pursuing enhancements to the implementation of the CMEP and notes actions that NERC CMEP management has agreed to undertake in connection with the observations. It is not intended to modify the management action plans (MAPs) adopted in the individual Regional Entity audit reports.

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

CC: Jim Albright (TexasRE)
Jason Blake (SERC)
Manny Cancel
Charles Dickerson (NPCC)
Melanie Frye (WECC)
Tim Gallagher (ReliabilityFirst)
Kelly Hanson
Mark Lauby
Sara Patrick (MRO)
Janet Sena
Mechelle Thomas

EXECUTIVE SUMMARY

CMEP Appendix 4A Audit – Consolidated Observations and Recommendations

Background

NERC, as the Electric Reliability Organization (ERO), established the Compliance Monitoring and Enforcement Program (CMEP) to facilitate the "ongoing monitoring of user, owner and operator compliance with Reliability Standards." The North American Bulk Power System (BPS) is monitored by the following six Regional Entities with corresponding boundaries: Midwest Reliability Organization, Northeast Power Coordinating Council, ReliabilityFirst, SERC Reliability Corporation, Texas Reliability Entity, and Western Electricity Coordinating Council. Included in the Appendix is an illustrative view of each Regional Entity footprint and CMEP staff for comparison at the time of audit.

In February 2015, the ERO Enterprise adopted a risk-based approach to the implementation of the CMEP in accordance with the Reliability Assurance Initiative (RAI), approved by Federal Energy Regulatory Commission (FERC). Significant components of the risk-based CMEP entailed developing Inherent Risk Assessments (IRAs), focusing efforts and reliance on evaluating the effectiveness of an entity's internal controls, deploying the compliance exception process to record and mitigate risks without formal enforcement action, and implementing a self-logging program for eligible registered entities to consolidate self-reporting of minimal risk noncompliance to be processed as compliance exceptions. This approach improved processing time of minimal to moderate risk noncompliance and broadened NERC and Regional Entity use of entity-specific risk assessments to determine audit scope and frequency. Over the past few years, NERC and the Regional Entities have implemented CMEP improvements, such as a single CMEP information system, Align, and enhancements to tools integral to effective monitoring, such as Compliance Oversight Plans (COPs), to establish a transparent CMEP oversight strategy for a registered entity with assigned monitoring tools and intervals based on a comprehensive assessment of risk.

NERC oversees each Regional Entity that has been delegated authority to, among other things, implement an effective CMEP. The objective of this oversight is to ensure that the Regional Entity carries out its obligations under the CMEP effectively, and in accordance with the Rules of Procedure (ROP) and the terms of the Regional Delegation Agreement (RDA), and to ensure consistency and fairness of the Regional Entity's execution of the CMEP.

In accordance with ROP Section 402.3.1 and Appendix 4A, the NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC CMEP and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC ROP, and the corresponding annual CMEP Implementation Plan (IP).

As a result of a directive in the FERC Order on the Five-Year Performance Assessment issued on January 19, 2021, NERC Internal Audit independently planned and performed audits of each Regional Entity's implementation of the CMEP. The audits were executed under the leadership of NERC Internal Audit resources, supplemented through staff augmentation through partnership with a leading audit firm, and conducted with observers from FERC and the Compliance and Certification Committee (CCC). The audit findings and recommendations have been shared with NERC and the six Regional Entities, and management action plans have been developed to address process, control, and compliance observations. Further, we look forward to completing our independent audit of the NERC CMEP in accordance with Section 406 of the ROP, which will further inform our overall observations and conclusions to collectively improve the CMEP.

Audit Summary

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 an evaluation of the Regional Entity's approach to and application of the risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC. The audit scope did not specifically include NERC's oversight responsibilities over the Regional Entities' implementation of the CMEP. However, we acknowledge these responsibilities and understand that NERC staff leading CMEP functions intend to work collaboratively with the Regional Entities to address the observations summarized below as part of the continued improvement of the CMEP.

Our observations did not detect significant noncompliance with the ROP. Specific deviations were identified, communicated within the respective Regional Entity audit reports, and should not be implied in other observations and conclusions. Furthermore, our conclusions underscore a need to enhance NERC oversight activities to continue to drive greater adoption of the risk-based methodology, further harmonization of processes, and more effective use of monitoring tools across the ERO Enterprise.

We concluded that all Regional Entities demonstrated the capability and access to data, tools, guidance and templates to perform CMEP administration and activities, which include the consistency and harmonization of processes and tools enabled by the ERO Enterprise implementation of Align. In addition, while local innovations and enhancements provide a more integrated approach to CMEP oversight, planning, scheduling, and execution of monitoring activities, the Regional Entities and NERC should consider a common path to use the full functionality of Align and standard processes, tools and templates to support more consistency in the implementation of the CMEP. This common path will drive consistency of the CMEP risk-based oversight strategy by identifying, assessing and mitigating risks guided by common processes and use of standard tools and templates that ensure reliability and security.

During the course of our evaluation, we identified several best practices across the Regional Entities, as well as opportunities to improve the implementation of the CMEP and related processes. These best practices were attributed to the Regional Entities' strong leadership and focus on the most optimal structure, subject matter expertise and innovations necessary to administer an effective CMEP. Best practices consisted of locally designed, developed and implemented automated tools to represent registered entities within the Regional Entity footprint, to more effectively evaluate risk, plan and schedule monitoring activity, and analyze, or retain performance data relevant to determining the appropriate oversight strategy, monitoring activities, tools and associated monitoring intervals. In addition, the majority of the Regional Entities implemented Entity Risk Profile ("ERP") tools and processes as a mechanism to capture inherent risks changes, and incorporate and refresh performance data and results of monitoring activity to inform annual planning.

Our audit approach and procedures included a comprehensive evaluation of each Regional Entity's application of a risk-based oversight strategy and use of monitoring tools such as periodic risk assessments and analyses, IRAs, COPs, Compliance Audits, Self-Certifications, Spot Checks, Self-Logging and Periodic Data Submittals (PDS) to establish compliance monitoring intervals. Furthermore, core CMEP governance activities included a review of the depth and breadth of training and learning programs administered across the CMEP, including Regional Entity focus on the importance of creating understanding of, and demonstrating proficiency with internal controls as a critical component to risk-based oversight. Additional governance activities included: an understanding of complaint and investigation processes, review of complaints received and investigations performed during the period of the audit, and oversight performed to ensure independence over CMEP activities related to Regional Entities operating with hybrid boards.

A significant area of opportunity in the evolution of the ERO Enterprise's risk-based approach is to move the oversight approach to a holistic framework, inclusive of an ongoing assessment of all registered entities (e.g.,

accounting for all assets within their respective footprint and impact to the BPS) beyond functions subject to a three year audit requirement and to achieve greater balance in the use of use of monitoring tools with sufficient rationale for monitoring intervals to ensure the effectiveness of the CMEP in promoting reliability and security.

Elements of the CMEP oversight strategy, application of tools, and use of approved templates vary from Regional Entity to Regional Entity. Also, the application of a risk based approach is defined differently by each Regional Entity as illustrated with variation in scope, frequency, and execution of monitoring activities, such as Compliance Audits, performance of Self-Certifications focused on Critical Infrastructure Protection (CIP) or Operations and Planning (O&P) Reliability Standards, and half of Regional Entities' applying a concept of a "guided self-certification" which equates to a limited scope audit. Additionally, tools integral to the execution of a risk-based oversight strategy and the establishment of monitoring tools and intervals, such as IRAs and COPs, were developed and refreshed inconsistently across Regional Entities.

To illustrate aspects of the variations in risk-based oversight strategy, and use of program tools and templates, several visual representations are included in Appendix A on page 10, within the Consolidated Executive Summary. These are provided to aid NERC and the Regional Entities in working towards further consistency and are not intended as separate or additional observations or findings.

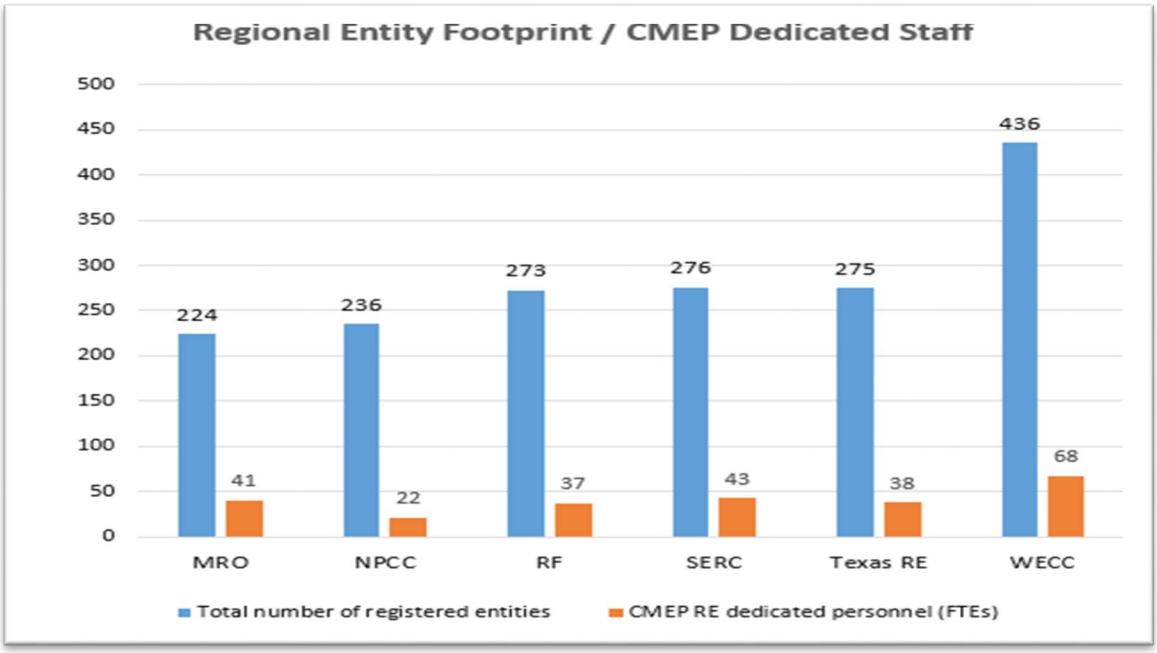
Aggregated Observations (Inclusive of the six Regional Entities)	
Observation	**Management Action Plan (MAP) Summary**
IRAs • Risk-based approach to developing and refreshing IRAs is primarily influenced by registered entities with BA/RC/TOP functions and the associated ROP requirement for a Compliance Audit at least once every three years • Registered entities ranked as low risk entities generally did not have an IRA developed until 2+ years after registration • Frequency for refreshing IRAs was inconsistent across the Regional Entities; some based on annual or semi-annual risk assessments/questionnaires, changes in registration, and performance considerations from planned monitoring activity • Templates varied across Regional Entities, including the performance risk analyses and risk summaries • Evidence of management review/approval was inconsistent	NERC Compliance Assurance will collaborate with Regional Entities to collect the Regional risk-based IRA development and refresh processes • As appropriate, NERC Compliance Assurance will work with the Regional Entities to develop a consistent approach across ERO Enterprise Align release 4.5, currently scheduled for November 2022, will address future template concerns as Align will be the tool for IRA development and summarization. NERC Compliance Assurance will monitor: • IRA completion and report results to the BOTCC; and • Registered entity IRA refresh processes and gauge current to expected progress
COPs • Approximately 55% of registered entities have a COP • Refresh frequency varied across Regional Entities; refreshes occurred before a Compliance Audit, or after, and in some cases were not refreshed until two years after an audit • Templates and development processes vary across the Regional Entities without specific guidelines for when to complete or refresh a registered entity's COP • Evidence of management review/approval was inconsistent	NERC Compliance Assurance will collaborate with Regional Entities to collect the Regional risk-based COP development and refresh processes • As appropriate, NERC Compliance Assurance will work with the Regional Entities to develop consistent approach across ERO Enterprise Align release 4.5, currently scheduled for November 2022, will address future template and approval process concerns as Align will be the tool for COP development NERC Compliance Assurance will monitor: • COP completion and report results to the BOTCC; and • Registered entity COP refresh processes and gauge current to expected progress

Compliance Audits • Audit Notification Letters did not effectively communicate scope and varied in comparison to COPs • Differentiation between on-site and off-site audit approaches varied across the Regional Entities	Align audit functionality automates a consistent ERO Enterprise approach for audit scope and audit notification. The audit pilot program is extended through 2Q 2023. NERC Compliance Assurance will collaborate with Regional Entities to evaluate: • Regional Entity justification documentation of audit scope and COP variations; and • Regional Entity approaches to on-site and off-site audits NERC Compliance Assurance will continue to monitor: • ROP audit scope and notification requirements; and Regional Entity audit approaches for on-site and off-site audits
Self-Certifications • 50% of REs apply a concept of "guided self-certifications", which share many characteristics of a limited scope audit; evidence of compliance is required and in some cases 100% reviewed by Regional Entity staff • Scope of Self-Certifications vary across Regional Entities; some focus only on CIP, while some include both CIP and O&P • Process or guidance for recording Potential Noncompliance (PNC) identified during Self-Certifications is not defined, resulting in significant delays in recording and reporting PNCs in a few cases	NERC Compliance Assurance will collaborate with Regional Entities to evaluate: • Regional Entity implementation of self-certification principles (Review timelines and PNC creation); and • Regional Entity processes for identified possible noncompliance during self-certification engagements NERC Compliance Assurance will monitor potential noncompliance submitted through the self-certification process to ensure timely submittal
Internal Controls • Understanding and awareness of internal controls is inconsistent across Risk Assessment and Mitigation (RAM) and Compliance Monitoring and Enforcement personnel, including compliance auditors and techniques to evaluate during audit engagements • Evaluation of internal controls within monitoring activities or programs is inconsistent; compliance audits, self-logging, self-certifications and COPs • Absence of specific training, guidance and learning programs that reinforce the importance of internal controls within a risk-based oversight model consistent with industry leading governance, risk and control (GRC) frameworks and standards	NERC Compliance Assurance will continue to work with ERO Enterprise staff, the RPMG and its Internal Controls Task Force, and others as needed, to develop additional guidance and/or training on internal controls, including: • Consistent internal controls identification, documentation, and assessment approach by Regional Entities during CMEP activities; and • Holistic Regional Entity approach for applying and sharing internal control information. NERC Compliance Assurance will periodically monitor Regional Entities implementation of developed internal control guidance/training.

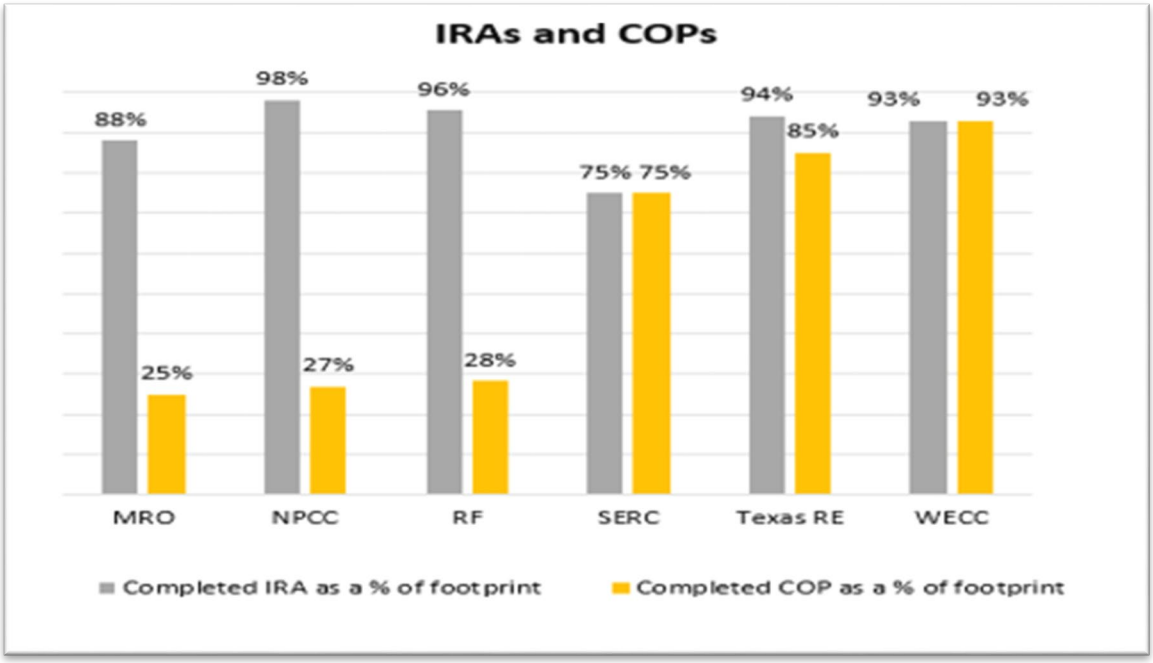
Enforcement Processes • Undocumented and inconsistent "triage" processes for PNC handling; backlogs occurred with PNCs captured in off-line format as minimal risk and not entered into system with timely reporting and disposition according to ROP • Monitoring activities and tools varied across Regional Entities related to handling of Open Enforcement Actions	NERC Enforcement will continue ongoing activities with the ERO Enterprise Enforcement Group (EG) to explore best practices for eliminating backlogs. NERC Enforcement is already seeing Regions adopting the best practices of other Regions NERC Enforcement will work with the EG to consider developing meaningful metrics for processing enforcement matters NERC Enforcement will also continue quarterly meetings with each Regional Entity to discuss caseloads and strategies for resolving older cases
Self-Logging • Participation in the program is on average at a nominal 8% of all registered entities within the ERO Enterprise • Promotion of the program and benefits is not understood or endorsed by the Regional Entities; 50% of Regional Entities do not differentiate between self-logging and self-reporting, minimizing the benefit of the program • Program application processes are inconsistent across the Regional Entities in terms of requirements and qualifications for eligibility according to ROP	NERC Enforcement will work with the EG to reevaluate the program in light of recent FERC orders NERC Enforcement will conduct a Self-Logging oversight activity in 2023, to evaluate, among other things, any potential improvements to the program considering the confines of FERC orders
Complaints and Investigations • In a two-year period, approximately 6 complaints were logged and 3 investigations across all Regional Entities • Handling, communication and resolution of anonymous complaints was inconsistent between Regional Entities and NERC • Disposition of complaints was premature in some cases and did not adequately address reported internal control issues that may contribute to violation of Reliability Standards	NERC Compliance Assurance will collaborate with Regional Entities to collect and assess Regional Entity Complaint and Investigation processes for: • Consistency across the ERO Enterprise; • Efficiency; • Thoroughness; and • Communication process
Training and Learning Programs • A process to designate and track required training of auditors and lead auditors was not in place, making it difficult to verify that required training occurred prior to audit engagements and/or on a stated frequency • Evidence of more comprehensive lead auditor training was lacking	The Align tool, Learning Management system, or regional tools are, or will be used, to capture required auditor training completion NERC Compliance Assurance will continue to provide required Auditor training, as well as periodically perform oversight to ensure regional audit staff training are adequately documented, tracked, and current

Appendix A – CMEP Data Visualizations (Illustrative)

CMEP Registered Entity Footprint by Regional Entity in comparison to CMEP Staff

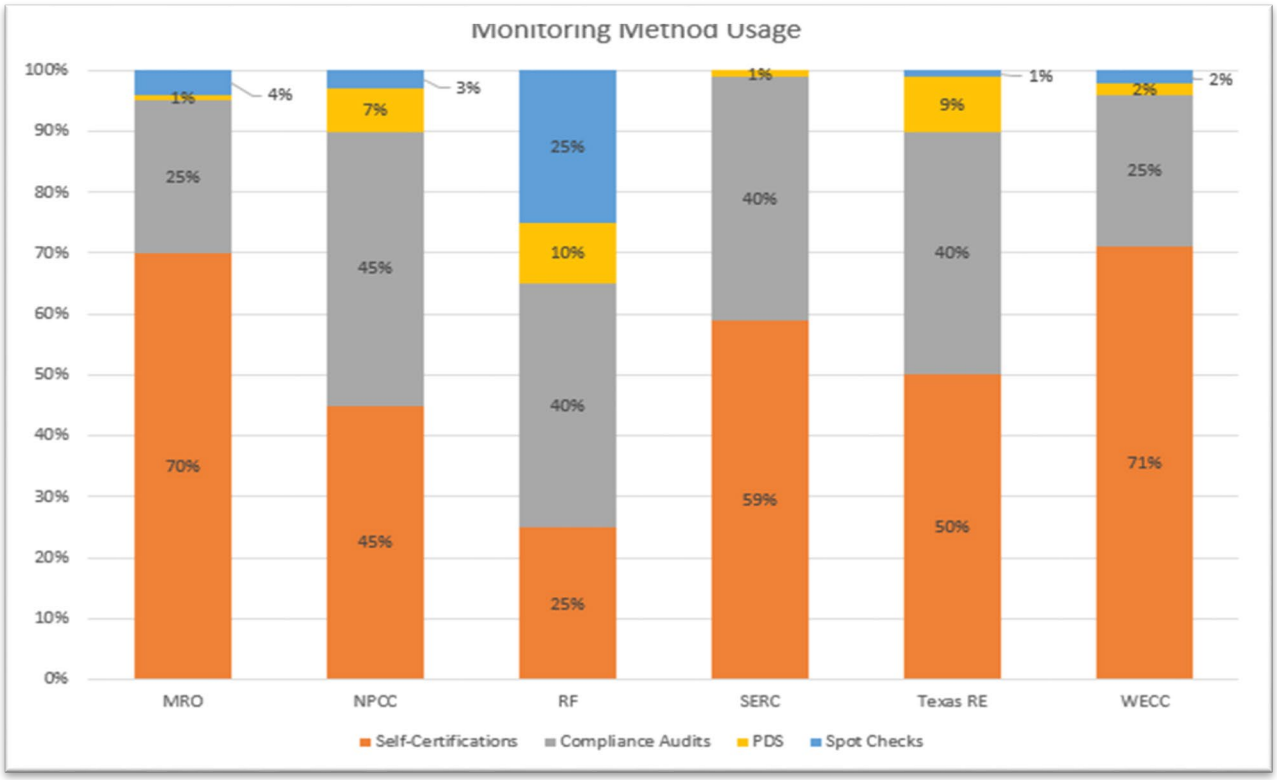


CMEP IRA and COP development as a percentage of total registered entities in Regional Entity footprint

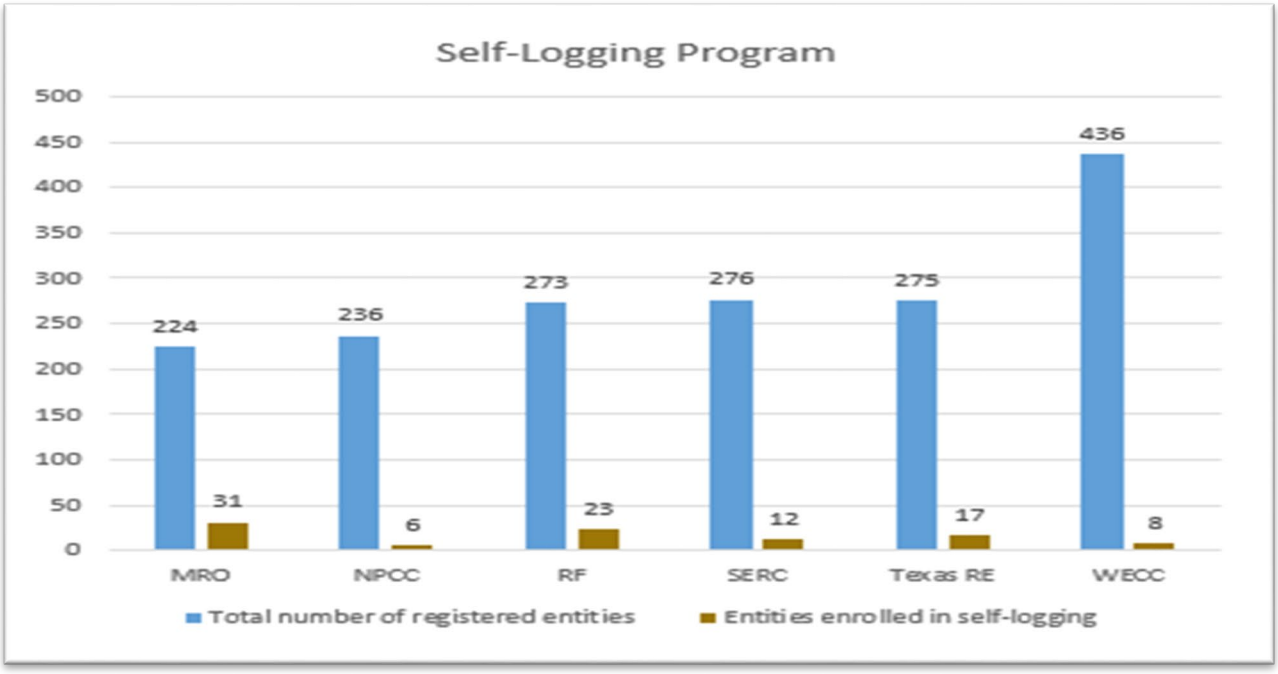


Appendix A – CMEP Data Visualizations (Illustrative) – con't

CMEP - Tool Usage



Self-Logging Program Enrollment



Appendix B

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, ROP requirements, and discussions with members of management and relevant stakeholders, 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 governing NERC Board 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.