NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2019 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 2.2

August 2019

RELIABILITY | RESILIENCE | SECURITY



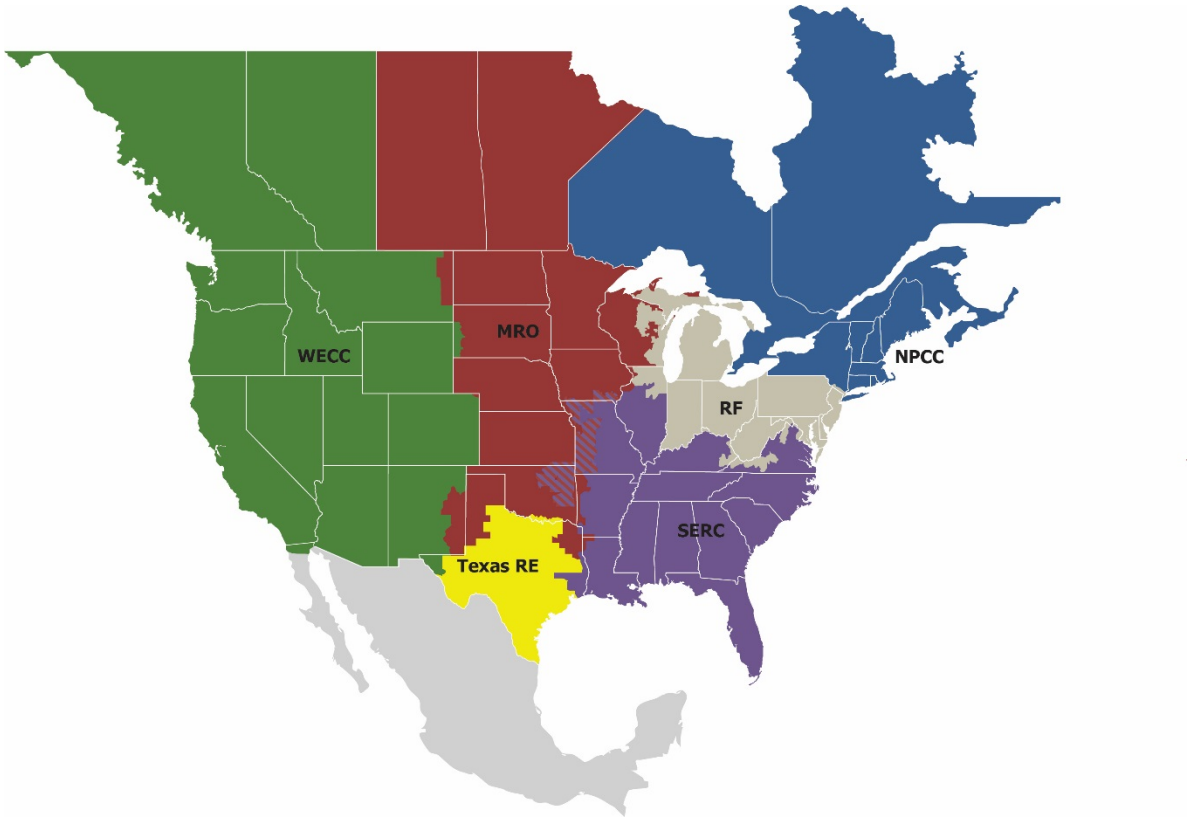

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Revision History

Version	Date	Revision Detail
Version 1.0	September 2018	• Release of the 2019 ERO CMEP Implementation Plan. The ERO CMEP IP is the NERC- only portion of the CMEP Implementation Plan and does not include Regional Implementation Plans.
Version 2.0	November 2018	• Updated with the seven Regional Entities' 2019 CMEP IPs in Appendices A1 – A7.
Version 2.1	November 2018	• Non substantive edits were made to Appendix A4.
Version 2.2	August 2019	• Updated to reflect the dissolution of the FRCC RE.

Introduction

Purpose

The Electric Reliability Organization (ERO) Enterprise[1] Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) is the annual operating plan used by the ERO Enterprise in performing CMEP responsibilities and duties. The ERO Enterprise executes CMEP activities in accordance with the NERC Rules of Procedure (ROP) (including Appendix 4C), their respective Regional Delegation Agreements, and other agreements with regulatory authorities in Canada and Mexico.

The ROP requires NERC to provide an IP to the Regional Entities (REs) on or about September 1 of the preceding year.[2] REs must submit their IPs to NERC for review and approval on or about October 1. RE IPs provide:

- details on Regional Risk Assessment processes and results;
- reliability Standards and Requirements associated with Regional Risk Assessment results;
- the Regional Compliance Monitoring Plan, which includes the annual audit plan; and
- other key activities and processes used for CMEP implementation.

The ERO Enterprise maintains a consolidated IP that provides guidance and implementation information common to NERC and the REs.

Implementation Plan

The ERO Enterprise consolidated IP uses a streamlined format that eliminates redundant information, improves transparency of CMEP activities, and promotes consistency among the RE-specific IPs. This format provides ERO-Enterprise-wide guidance and implementation information while preserving RE differences by appending RE-specific IPs to supplement the overall ERO Enterprise IP. The RE-specific IPs describe risk assessments that identify the risks that the REs will consider as part of their monitoring activities for registered entities.

NERC is responsible for collecting and reviewing the RE IPs to help ensure REs provide appropriate and consistent information on how they conduct CMEP activities. NERC monitors RE progress of CMEP activities against the RE IPs throughout the year and reports on CMEP activities in a year-end annual CMEP report.[3]

During the implementation year, NERC or an RE may update their portions of the IP. Updates may include, but are not limited to, the following: changes to compliance monitoring processes; changes to RE processes; or updates resulting from a major event, FERC order, or other matter. REs submit updates to the NERC Compliance Assurance group, which reviews the updates and makes any needed changes. When changes occur, NERC posts a revised plan on its website and issues an announcement.

RE-specific IPs are due to NERC for annual review and approval on or about October 1. NERC will review the RE-specific IPs and include them in this document in Appendix A (1–7).

[1] The ERO Enterprise is comprised of NERC and the seven Regional Entities, which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the EROs' statutory obligations to assure the reliability of the North American BPS.
[2] NERC ROP, Section 403 (Required Attributes of RE Compliance Monitoring and Enforcement Programs).
[3] ERO Enterprise Annual CMEP Reports available at http://www.nerc.com/pa/comp/Pages/AnnualReports.aspx

Significant CMEP Activities

The following ongoing activities impact the ERO Enterprise's CMEP implementation.

Program Alignment

Greater alignment across the ERO Enterprise can help maintain focus on the most significant risks to reliability using aligned practices in the monitoring and enforcement of compliance with the Reliability Standards. The ERO Enterprise Program Alignment Process is an opportunity to improve alignment throughout the ERO Enterprise by identifying approaches to ensure consistency and leverage ongoing efforts across the ERO Enterprise. The NERC Compliance and Certification Committee (CCC) Alignment Working Group (AWG) works with NERC, as needed, to aid in framing anonymously submitted issues and reports its work to the CCC.

Program Alignment consists of the following:

- **Track**: Identify and capture issues
- **Triage**: Classify, analyze, and prioritize
- **Transparency**: Post and report

The program's overall elements of success are capturing and centralizing all reported issues, encouraging industry participation to help define the issues with real examples, responding in a timely manner, and providing the appropriate level of transparency to industry. The ERO Enterprise implements this program through documented processes owned and facilitated by NERC.

Compliance Guidance

A key factor in the success of compliance monitoring and enforcement of mandatory Reliability Standards rests on a common understanding among industry and ERO Enterprise CMEP staff of how compliance can be achieved and demonstrated. For many Reliability Standards, this is straightforward. For others, a variety of approaches may achieve the same objective. The Compliance Guidance process provides such a mechanism through the ERO Enterprise endorsement of Implementation Guidance and the development of CMEP Practice Guides.

Implementation Guidance is developed by industry and vetted through prequalified organizations. For an organization to become prequalified, a member of that organization must submit an application to the CCC. Vetted examples can then be submitted to the ERO Enterprise for endorsement, and the example would be given deference by the ERO Enterprise during CMEP activities with consideration of facts and circumstances if endorsed. Implementation Guidance would not prescribe the only approach to implementing a Reliability Standard, and registered entities would be allowed to choose alternative approaches that better fit their situation. Draft Implementation Guidance will be posted on NERC's website on the Compliance Guidance page[4] while it is being considered for ERO Enterprise endorsement. Once the Implementation Guidance is endorsed, it will be moved to the ERO Enterprise-Endorsed Implementation Guidance section. Draft Implementation Guidance that does not receive ERO Enterprise endorsement will be removed, and the document in the Non-Endorsed Implementation Guidance section will be updated with the rationale.

CMEP Practice Guides are developed by the ERO Enterprise to reflect the independent, objective, professional judgment of ERO Enterprise CMEP staff, and at times may be initiated following policy discussions with industry stakeholders. Following development, the CMEP Practice Guides are posted for transparency on the NERC website.

[4] Compliance Guidance available at http://www.nerc.com/pa/comp/guidance/Pages/default.aspx

Throughout 2019, the ERO Enterprise will continue to review and act on Implementation Guidance documents submitted by industry as well as to evaluate the need for (and develop, where appropriate) CMEP Practice Guides. NERC publicly posts Implementation Guidance and CMEP Practice guides on the Compliance Guidance website.

Coordinated Oversight of Multi-Region Registered Entities

The ERO Enterprise offers coordinated oversight for Multi-Region Registered Entities (MRREs)[5] to streamline the compliance monitoring and enforcement activities for the registered entities that use, own, or operate assets in areas covering more than one RE territory.

REs will coordinate their oversight responsibilities for MRREs in coordinated oversight by designating one or more Lead RE (LRE) to each MRRE or a group of MRREs. The LRE is selected based on BPS reliability considerations and the registered entity's operational characteristics. The selected LRE works collaboratively with the remaining Affected REs, known as AREs, and informs NERC of activities as appropriate. Coordinated oversight for MRREs is flexible and voluntary for MRREs.

The ERO Enterprise Guide for Coordinated Oversight of MRREs contains additional details on the process, including criteria for inclusions and roles and responsibilities.

Southwest Power Pool (SPP) RE Dissolution

On May 4, 2018, the Federal Energy Regulatory Commissions (FERC) approved the dissolution of Southwest Power Pool RE.[6] The dissolution resulted in the transfer of registered entities from SPP RE to MRO and SERC effective July 2018. NERC, MRO, and SERC initiated transition activities in 2018, and registered entities transferred to MRO and SERC will follow applicable regional processes and the 2019 Regional Implementation Plans.

Additionally, to facilitate the transition from SERC as the CEA for the registered functions of SPP, NERC will act as the CEA for SPP for two years following the termination effective date for the SPP Regional Delegation Agreement. To execute CEA activities, NERC will follow the NERC ROP and other existing processes and procedures used by REs to implement the CMEP. Throughout the 2019 implementation year, NERC will consider the ERO Enterprise risk elements, as well as applicable risks typically considered when conducting risk-based compliance monitoring.

Florida Reliability Coordinating Council (FRCC) RE Dissolution

On April 30, 2019, the Federal Energy Regulatory Commissions (FERC) approved the dissolution of the Florida Reliability Coordinating Council RE.[7] The dissolution resulted in the transfer of registered entities from FRCC RE to SERC effective July 1, 2019. NERC and SERC initiated transition activities earlier 2019, and registered entities transferred to SERC will follow applicable regional processes and the updated 2019 SERC Regional Implementation Plan (Appendix A4).

[5] Coordinated Oversight of MRRE Program Development and Implementation, available at MRRE Coordinated Oversight Program

[6] FERC Order granting approvals in connection with the dissolution of the SPP RE located here: https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Granting%20Approvals%20in%20Connection%20with%20the%20Dissolution%20of%20the%20SPP%20RE.pdf

[7] FERC Letter Order granting approvals in connection with the dissolution of the FRCC RE located here: https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/FRCC%20Dissolution%20Order.pdf

Risk-based Compliance Monitoring and Enforcement

Compliance monitoring and enforcement must be "right-sized" based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of noncompliance. A risk-based approach is necessary for a proper allocation of resources and to encourage registered entities to enhance internal controls, including those focused on the self-identification of noncompliance.

The ERO Enterprise Risk-Based CMEP focuses on identifying, prioritizing, and addressing risks to the BPS to focus resources where they are most needed and likely to be the most effective.

Risk-based Compliance Monitoring

Risk-based compliance monitoring involves the use of the ERO Enterprise Risk-Based Compliance Oversight Framework (Framework). The Framework focuses on identifying, prioritizing, and addressing risks to the BPS, enabling each RE to direct resources where they are most needed. REs are responsible for tailoring their monitoring (i.e., monitoring tools and the frequency and depth of monitoring engagements) of registered entities through use of the Framework. This process is described in more detail in the ERO Enterprise's Risk-Based CMEP.[8]

As reliability risk is not the same for all registered entities, the Framework examines BPS risk of registered entities (both collectively and individually) to determine the most appropriate CMEP tool to use when monitoring a registered entity's compliance with NERC Reliability Standards. The Framework also promotes an examination into how registered entities operate, and tailors compliance monitoring focus to areas that pose the greatest risk to BPS reliability. The Framework elements are dynamic and are not independent; rather, they are complementary and interdependent.

The IP contains the ERO Enterprise risk elements, which provide guidance to REs in the preparation of their RE IPs. REs are expected to consider regional risks and specific circumstances associated with individual registered entities within their footprints when developing compliance oversight plans. The process for identifying ERO Enterprise and RE risk elements, and their associated areas of focus, is explained later in this document.

The REs determine the type and frequency of the compliance monitoring tools (e.g., offsite or onsite audits, spot checks, or self-certifications) that are warranted for a registered entity based on reliability risks. The Inherent Risk Assessment (IRA) involves a review of potential risks posed by an individual registered entity to the reliability of the BPS.[9] An IRA considers factors like assets, systems, geography, interconnectivity, and overall unique entity composition. In considering such factors, an IRA is not limited by the risk elements and associated areas of focus identified in the 2019 ERO Enterprise CMEP IP. Rather, the IRA considers multiple factors to focus oversight to entity-specific risks and results in the identification of the Reliability Standards and Requirements that should be monitored.

When developing specific compliance oversight plans for registered entities in their footprints, the REs also take into account prior compliance history, mitigating activities associated with prior noncompliance, and any information obtained through the processes outlined in the ERO Enterprise Guide for Internal Controls.[10] As a result of the Internal Control Evaluation (ICE), and other considerations, the REs may further refine the focus of compliance monitoring activities for a given entity and may, for example, limit the depth or focus of testing for a given area.

Periodic Data Submittals

Registered entities provide the required information to the CEA, either NERC or the REs, in accordance with the NERC ROP and CMEP. For the 2019 implementation year, NERC and the REs developed a consolidated schedule for

[8] Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program
[9] ERO Enterprise Guide for Compliance Monitoring
[10] ERO Enterprise Guide for Internal Controls

the ERO Enterprise. The purpose of this schedule is to provide registered entities a consistent list of required Reliability Standard Periodic Data Submittals throughout the ERO Enterprise, and includes RE-specific data submittal schedules as well. NERC and the REs may also request data or information under Sections 800 or 1600 of the NERC ROP; these data requests are not included on this schedule.

Compliance Assessments for Events and Disturbances

An important component of the ERO Enterprise's risk-based approach to compliance monitoring is voluntary participation in the Compliance Assessment (CA) Process by registered entities after an event or disturbance. Through the Event Analysis Process, the ERO Enterprise promotes a culture of reliability and security excellence that encourages an aggressive and critical self-review and analysis of operations, planning, and critical infrastructure performance.

The CA Process is a complementary review of the event focused on the evaluation of compliance with Reliability Standards. A registered entity completes a CA by reviewing the facts and circumstances of an event or disturbance, identifying relevant Reliability Standards and Requirements, evaluating compliance with these Reliability Standards and Requirements, and self-reporting any potential noncompliance. RE compliance staff also assess significant events and disturbances to increase awareness of reliability risks that may guide further compliance monitoring activities.

Registered Entity Responsibilities in the CA Process

The registered entity Compliance Assessments constitute a major element of the overall CA Process. The ERO Enterprise encourages registered entities to perform a voluntary, systematic CA in response to all system events and disturbances. Registered entities are encouraged to share the CA with the RE for all Category 2-and-above events, and any Category 1 and uncategorized events that were significant and could help to increase awareness of reliability risks. Registered entities should use the Sample Compliance Assessment Report template (Appendix B of this document) when performing a CA. In addition to the completed CA template, registered entities should provide to the RE sufficient event information, such as the Brief Report or Event Analysis Report, so the RE may thoroughly understand the event.

Registered entities that follow the process above to evaluate systematically their own compliance performance, self-report potential noncompliance, and address reliability issues, demonstrate the effectiveness of their internal controls and their commitment to a culture of compliance. Registered entities that demonstrate strong internal controls and a robust culture of compliance that mitigates risk to the BPS may be afforded some recognition by way of reduced levels and frequency of compliance monitoring activities. Mitigating credit for these actions is also considered during the enforcement of a noncompliance. Such credit may be available to the registered entity for comprehensive CAs that clearly demonstrate a systematic review of applicable Reliability Standards and, as appropriate, self-reporting.

Regional Entity Responsibilities in the CA Process

REs play a key role in the CA Process as their familiarity and direct contact with the registered entities enable them to affect the CA Process Outcome in a significant and positive manner. REs should take measures to promote the development and submittal of Compliance Assessments for Category 2-and-above events by the registered entities, working closely with the registered entities to ensure that the Compliance Assessments are complete, timely, and accurate, and that they create a clear picture of all significant elements of the event. REs will review system event reports and CA reports provided by registered entities and may use a risk-based approach to prioritize these evaluations. However, the REs will conduct a Regional Compliance Evaluation (RCE) for all Category 2-and-above events. The RE should also examine lower category events that indicate the need for closer evaluation. As part of its independent evaluation of the CA, the RE may request additional information from the registered entity if it is needed to understand the event. The subsequent RCE is therefore based on a complete understanding of the event from the directly involved registered entities and reflects any required compliance follow-up.

The scope of RCEs and the manner in which the REs and NERC evaluate, process, and respond to these reviews should reflect the significance of the event. Events described as "Category 2 and above" typically constitute significant challenges to BES reliability and may stem from violations of or gaps in the Reliability Standards. Consequently, prompt completion of the RE RCE is critical to ensure any deficiencies are quickly identified and corrected. The RE will share the RCE and CA with NERC staff.

Risk-based Enforcement

The ERO Enterprise's risk-based enforcement defines, communicates, and promotes desired entity behavior to improve the reliability of the BPS. Specifically, risk-based enforcement allows the ERO Enterprise to focus on higher risks to the reliability of the BPS while maintaining the ERO Enterprise's visibility into potential noncompliance, regardless of the level of risk they pose. NERC has transitioned its oversight activities to align with the Risk-Based CMEP, allowing the ERO Enterprise to focus on issues that pose greater risk to reliability. NERC staff conducts qualitative reviews on a continuing basis on various aspects of the Risk-Based CMEP to evaluate the effectiveness of CMEP strategies and program execution. In addition, these reviews identify and incorporate best practices and guidance for REs.

Enforcement Philosophy

The ERO Enterprise continues to refine its risk-based enforcement philosophy. The ERO Enterprise's risk-based enforcement philosophy generally advocates reserving formal enforcement actions for those issues that pose a higher risk to the reliability of the BPS. The risk of a noncompliance is determined based on individual facts and circumstances, including any compensating or mitigating factors that existed during the pendency of the noncompliance. The ERO Enterprise works with registered entities to ensure timely remediation of potential risks to the reliability of the BPS and to prevent recurrence of the noncompliance. The enforcement process allows parties to address risks collaboratively and promote increased compliance and reliability through improvement of programs and controls at the registered entities.

For issues posing a minimal risk to the BPS, NERC and the REs may exercise appropriate judgment whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes as Compliance Exceptions. The availability of streamlined treatment of minimal-risk noncompliance encourages prompt identification and correction of issues by registered entities, and the efficient mitigation of such issues in the enforcement process. As such, while self-identified minimal risk noncompliance is more than likely not going to be subject to a financial penalty, registered entities are encouraged to establish robust internal controls to prevent, detect, and correct noncompliance. This approach allows the ERO Enterprise to oversee the activities of registered entities in a more efficient manner and to focus resources where they result in the greatest benefit to reliability.

An inherent element of a risk-based approach to enforcement is accountability of registered entities for their noncompliance. No matter the risk of the noncompliance, the registered entity still bears the responsibility of mitigating that noncompliance and working to prevent recurrence. Based on the risk, facts, and circumstances associated with that noncompliance, the RE decides on an appropriate disposition track–inside or outside of an enforcement action–as described above. The RE also determines whether a penalty or sanction is appropriate for the noncompliance.

Penalties and sanctions are generally warranted for some moderate risk violations and most, if not all, serious risk violations (e.g., loss of load, CIP program failures). Penalties and sanctions are also frequently assessed when repeated noncompliance of the same or similar Reliability Standard constitutes an aggravating factor. In addition to the use of significant penalties to deter undesired behavior, the ERO Enterprise also incents desired behaviors. Specifically, REs may offset penalties to encourage valued behavior. Valued behaviors that may mitigate penalty

amounts include registered entity cooperation, accountability (including acceptance of responsibility for violations), a culture of compliance, and self-identification of noncompliance.

REs may also grant credit in enforcement determinations for certain actions undertaken by registered entities for improvements that increase reliability and security. For example, REs may consider significant investments in tools, equipment, systems, or training made by registered entities–beyond those typically used in the industry or otherwise planned or required for compliance or mitigation–as an offset for proposed penalties in enforcement determinations. REs do not award credits or offsets for actions or investments undertaken by a registered entity that are required to mitigate the noncompliance or meet the Requirements of future Reliability Standards.

2019 ERO Enterprise Risk Elements

Process for Risk Elements and Associated Areas of Focus

As noted above, the ERO Enterprise utilizes the Framework to identify risks to the reliability of the BPS, as well as, mitigating factors that may reduce or eliminate a given reliability risk. As such, NERC identifies risk elements using data including, but not limited to: compliance findings; event analysis experience; data analysis; and the expert judgment of NERC and RE staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee). NERC uses these risk elements to identify and prioritize interconnection and continent-wide risks to the reliability of the BPS. These identified risks, as well as risks to the reliability of the BPS identified by each RE for its footprint, will be used by REs to focus monitoring activities.

For the purpose of the IP, areas of focus highlight ERO-Enterprise-wide and RE-specific risks that merit increased focus for compliance monitoring that may become a part of an individual registered entity's monitoring activities. The areas of focus do not represent the exclusive list of important or relevant Reliability Standards or Requirements, nor the entirety of the risks that may affect the reliability of the BPS. Rather, REs will consider the risk elements and areas of focus to help prioritize compliance monitoring efforts.

When developing entity-specific compliance oversight plans, REs consider local risks and specific circumstances associated with individual registered entities. The compliance oversight plan also takes into account the unique compliance history of each registered entity, along with both the timing of and the results of any prior compliance monitoring, when determining which compliance monitoring tools will be used for future monitoring for each registered entity. The compliance oversight plan focuses on a complete picture of reliability risks associated with a registered entity along with various mitigating factors, such as past performance or the presence of effective internal controls, to determine the appropriate compliance monitoring tool(s) for registered entities.

As a result, a particular registered entity's scope of monitoring may include more, fewer, or different Reliability Standards than those outlined in the ERO and RE CMEP IPs. The determination of the appropriate CMEP tools may be adjusted as needed within a given implementation year. Additionally, NERC and the REs have the authority to monitor compliance with all applicable Reliability Standards whether they are identified as areas of focus to be considered for compliance oversight in the annual IP or are included in an RE's oversight plan for a registered entity.

NERC followed the risk element development process to review and reassess the 2018 risk elements to determine applicability for 2019.[11] Although the IP identifies NERC Standards and Requirements to be considered for focused compliance monitoring, the ERO Enterprise recognizes by using the Framework and risk-based processes that REs will develop a focused list of NERC Reliability Standards and Requirements specific to the risk a registered entity poses. Therefore, a particular area of focus under a risk element does not imply 1) that the identified Reliability Standard(s) fully addresses the particular risk associated with the risk element, 2) that the identified Reliability Standard(s) is only related to that specific risk element, or 3) that all Requirements of a Reliability Standard apply to that risk element equally. Subject to NERC monitoring, REs will consider the ERO Enterprise risk elements, along with RE risk elements, when conducting compliance monitoring activities and assessing compliance with identified Reliability Standards and Requirements.

Risk Element Results

The 2019 risk elements are included in Table 1 below and reflect a maturation of the risk-based approach to compliance monitoring. As regional entities become more knowledgeable about their entities and understand the

[11] Appendix C, ERO Enterprise Guide for Compliance Monitoring, available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Guide%20for%20Compliance%20Monitoring.pdf

risks that they represent and mitigate, risk elements can be more focused on discrete issues that NERC encourages prioritization in the coming year.

NERC identified the risk elements listed below using the risk element development process,[12] which considers data, reports, and publications that identify reliability risks which translate into compliance monitoring. This includes the risks noted in the Reliability Issues Steering Committee's (RISC) report,[13] the State of Reliability Report,[14] the Long-Term Reliability Assessment, publications from the RISC, special assessments, the ERO Enterprise Strategic Plan, and ERO Event Analysis Process insights.

Areas of focus are provided for each of the risk elements. The areas of focus do not represent the exclusive list of important or relevant Reliability Standards or Requirements, nor do the areas of focus encompass the entirety of the risks that may affect the reliability of the BPS. Rather, REs will consider the risk elements and areas of focus to help prioritize compliance monitoring efforts. Standards identified as areas of focus that will become inactive during 2019 have been identified along with the succeeding version of the Reliability Standard, or area of focus, in each of the corresponding risk element tables listed below.

Table 1: Comparison of 2016-2018 Risk Elements and 2019 Risk Elements[15]

2016-2018 Risk Elements	2019 Risk Elements
Critical Infrastructure Protection	Improper Management of Employee and Insider Access
Extreme Physical Events	Insufficient Long-Term Planning Due to Inadequate Models
Maintenance and Management of BPS Assets	Insufficient Operational Planning Due to Inadequate Models
Monitoring and Situational Awareness	Spare Equipment with Extended Lead Time
Protection System Failures	Inadequate Real-time Analysis During Tool and Data Outages
Event Response/Recovery	Improper Determination of Misoperations
Planning and System Analysis	Inhibited Ability to Ride Through Events
Human Performance	Gaps in Program Execution

Improper Management of Employee and Insider Access

The protection of critical infrastructure remains an area of significant importance. This risk element establishes a focus on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.[16] Regardless of the sophistication of a security system, there is potential for human error. Compliance monitoring should seek to understand how entities manage the risk of how many people have access and the complexity of the tasks the people are asked to perform. If security has increased the difficulty in performing

[12] ERO Enterprise Guide for Compliance Monitoring; October 2016
[13] ERO Reliability Risk Priorities; February 2018
[14] NERC *State of Reliability 2018*, available at https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_2018_SOR_06202018_Final.pdf
[15] The risk elements below are not a comprehensive list of all risks to the reliability of the BPS. The Reliability Standards, requirements, and associated functions for each area of focus may be updated throughout the year to reflect new versions of the Reliability Standards that become effective.
[16] ERO Reliability Risk Priorities; February 2018

personnel's normal tasks, personnel will look for ways to circumvent the security to make it easier to perform their job. On the other hand, when complex tasks are replaced with automation, focus should be on whether the learning curve of setting up the automation correctly was mitigated.

Harvesting credentials and exploiting physical and logical access of authorized users of BES facilities and Cyber Systems (BCSs) pose a major risk to systems that are used to monitor and control the BPS. This risk is particularly enhanced due to the fact that the target here is privileged and non-privileged users who have authorized unescorted access who has unprecedented level of access to critical aspects of BES. By actively and covertly employing social engineering techniques and phishing authorized users can be tricked to harvest credentials and gain access.[17]

Improper access of employees can lead to BCSs being compromised and is a major risk to systems that are used to monitor and control the BPS. Based on the results of NERC's Remote Access Study, many systems used to operate the BES rely on remote access technologies. Remote access refers to the ability to access a system, application, or data from a remote location. Remote access can take one of two forms: 1) human- or user-initiated remote access, referred to as Interactive Remote Access in NERC's CIP Reliability Standards; or 2) automated system-to-system access. Registered entities frequently use Interactive Remote Access technologies to enable remote users to operate, support, and maintain control systems networks and other BES Cyber Systems. Among other things, providing for remote access enables users to efficiently access Cyber Assets to troubleshoot application software issues and repair data and modeling problems that cause application errors. These remote access technologies–while important for efficiently operating, supporting, and maintaining Cyber Assets, including those for control systems–could open up attack vectors. If not properly secured, remote access could result in unauthorized access to a registered entity's network and control systems with potentially serious consequences. For instance, an attacker could breach an environment via remote access by deliberately compromising security controls to obtain privileged access to critical systems. Although registered entities generally do not rely on Internet-facing systems to operate and monitor the BES, malicious actors have demonstrated capabilities to infiltrate systems that are not Internet-facing, such as systems designed to run autonomously with minimal human interaction and other mission-critical applications that are used to perform supervisory control that, if misused, could result in serious reliability issues. Additionally, a compromised device that is allowed to remotely access a Cyber Asset can serve as a gateway for cyber-criminals to attack networks.

The identified area's risks can be mitigated through awareness and technical controls. Entities need to enhance security awareness to include specific topics on social engineering and insider threat. By implementing detection and monitoring tools as technical controls insider threat incidents can be prevented proactively. Further, a formalized insider threat management program in place can vastly reduce the associated risk.

Areas of Focus

Table 2: Improper Management of Employee and Insider Access

Standard	Requirements	Entities for Attention	Asset Types
CIP-004-6	R1, R2, R3, R4	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Back up Control Centers Control Centers Data Centers Generation Facilities Substations

[17] US-CERT TA18-074A

Table 2: Improper Management of Employee and Insider Access			
Standard	**Requirements**	**Entities for Attention**	**Asset Types**
CIP-005-5	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-006-6	R1, R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-007-6	R2, R3, R5	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-010-2	R1, R2, R3, R4	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-011-2	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations

Insufficient Long-Term Planning Due to Inadequate Models

Planning and system analyses are performed for the integration and management of system assets. This includes the analyses of other emerging system issues and trends (e.g., significant changes to the use of demand-side management programs, the integration of inverter-based resources and variable energy resources, changes in load characteristics, increasing dependence on natural gas deliverability for gas-fired generation, increasing uncertainty in nuclear generation retirements, and essential reliability services). NERC's annual *Long-Term Reliability Assessment*[18] forms the basis of NERC's assessment of emerging reliability issues. The ERO continues to raise

[18] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_12132017_Final.pdf

awareness on inverter-based resource performance through NERC alerts[19] and industry outreach. Compliance monitoring should seek to understand how entities manage the risk of planning in this changing environment.

Insufficient long-term planning can lead to increased risks to reliability. Adequately modeled planning cases become increasingly critical as a changing resource mix, deployment of new technologies, etc., affect the risk to BPS reliability. For instance, the models should reflect if the power electronic controls of utility-scale inverter-based resources, such as PV resources, give these resources the ability to provide both real and reactive power. As stated in the 2018 RISC report,[20] since the rate of change of the resource mix is increasing, planners will place more emphasis on interconnection-wide studies that require improvement to and integration of regional models. In addition, enhancements to models will be needed to support probabilistic analysis to accommodate the energy limitations of resource additions (such as variable renewable resources). Resource adequacy must look beyond the calculation of reserve margins that assume actual capacity available during peak hours.

Areas of Focus

Table 3: Insufficient Long-Term Planning Due to Inadequate Models

Standard	Requirements	Inactive/Future Enforcement Date *(if applicable)*	Entities for Attention
FAC-002-2	R1, R2, R3, R4, R5	n/a	Planning Coordinator Transmission Planner Transmission Owner Distribution Provider Generator Owner
MOD-032-1	R2	n/a	Balancing Authority Generator Owner Resource Planner Transmission Owner Transmission Service Provider
MOD-033-1[21]	R1, R2	n/a	Planning Coordinator Reliability Coordinator Transmission Operator
TPL-001-4	R1, R2, R3, R4	n/a	Planning Coordinator Transmission Planner

Insufficient Operational Planning Due to Inadequate Models

Insufficient operational planning can lead to increased risks to reliability. More comprehensive dynamic load models will be needed to sufficiently incorporate behind-the-meter generation and distributed load resources such as demand-side management programs. One of the ways in which the industry can better understand the system is by monitoring load characteristics and the changing nature of load due to DER. The NERC Load Modeling Task Force developed a reliability guideline that provides Transmission Planners (TPs) and Transmission Owners (TOs) with insights into end-use load behaviors and how to capture them in the composition of dynamic load models.[22]

[19] https://www.nerc.com/news/Documents/Inverter%20Alert%20Announcement.pdf
[20] ERO Reliability Risk Priorities; February 2018
[21] Per Implementation Plan, the first studies will be performed in 2019.
[22] NERC Modeling Improvements Initiative Update; May 2018

Additional studies have similarly shown a need to more accurately understand and model inverter-based resource characteristics. NERC has identified adverse characteristics of inverter-based resources in two separate Alerts. [23,24] With the recent and expected increases of both utility-scale solar resources and distributed generation, the causes of a sudden reduction in power output from utility-scale power inverters needs to be widely communicated and addressed by the industry. Entities with increasing inverter-based resources should be aware and addressing this within their models.[25]

Areas of Focus

Table 4: Insufficient Operational Planning Due to Inadequate Models

Standard	Requirements	Inactive/Future Enforcement Date *(if applicable)*	Entities for Attention
MOD-032-1	R2	n/a	Balancing Authority Generator Owner Resource Planner Transmission Owner Transmission Service Provider
MOD-033-1[26]	R1, R2	n/a	Planning Coordinator Reliability Coordinator Transmission Operator
TOP-003-3	R1, R2	n/a	Balancing Authority Transmission Planner
TPL-001-4	R1, R2, R3, R4	n/a	Transmission Planner

Spare Equipment with Extended Lead Time

As the BPS ages, less-than-adequate infrastructure maintenance is a reliability risk that continues to grow. The RISC report identifies that the failure to maintain equipment is a reliability risk exacerbated when an entity either does not have replacement components available or cannot procure needed parts in a timely fashion. The failure to properly commission, operate, maintain, prudently replace, and upgrade BPS assets generally could result in more frequent and wider-spread outages, and these could be initiated or exacerbated by equipment failures.

Spare equipment strategy is an important aspect of restoration and recovery. The strategy should encompass identifying critical spare equipment as part of a national or regional inventory. The strategy should also account for the transportation and logistics requirements for replacing critical assets. An improved spare equipment strategy or plan will lead to better planning and possibly faster response times for restoration and recovery. A spare equipment strategy can help strengthen the resiliency for responding to potential physical threats and vulnerabilities.[27]

Areas of Focus

[23] Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings; June 2017
[24] Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings - II; May 2018
[25] NERC Modeling Notification: Recommended Practices for Modeling Momentary Cessation Distribution; April 2018
[26] Per Implementation Plan, the first studies will be performed in 2019.
[27] CIP-014-2 Guidelines and Technical Basis, Requirement R5

Table 5: Spare Equipment with Extended Lead Time			
Standard	**Requirements**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
CIP-014-2	R1, R5	n/a	Transmission Owner
TPL-001-4	R2.1.5	n/a	Planning Coordinator Transmission Planner

Inadequate Real-time Analysis during Tool and Data Outages

Without the right tools and data, operators may not make decisions that are appropriate to ensure reliability for the given state of the system. NERC's *ERO Top Priority Reliability Risks 2014-2017* notes that "stale" data and lack of analysis capabilities contributed to the blackout events in 2003 ("August 14, 2003 Blackout") and 2011 ("Arizona-Southern California Outages"). Certain essential functional capabilities must be in place with up-to-date information available for staff to use on a regular basis to make informed decisions.

Specifically, entities are to be encouraged to have realistic plans to continue real-time analysis during outages of tools, loss of data, or both. The 2018 RISC report[28] identifies that loss of situational awareness can be a precursor or contributor to a BPS event. This risk element is made more important in situations where planning models may not keep pace with increasing BPS complexity and accurately reflect area specific dependencies on inverters, natural gas, or other items identified in the other 2019 risk element "Planning Representing Area Specific Dependencies and Characteristics". Forecasting BPS resource requirements to meet customer demand is becoming increasingly difficult due to the penetration of DER which can mask the customer's electric energy use and the operating characteristics of distributed resources without sufficient visibility.

Compliance monitoring should understand the plan and the capability and feasibility of the entities skilled workforce to implement the plan within a reasonable time frame. Monitoring should include a keen eye on events and the human evaluation rather than simply looking at RTCA scans. RTCA is a tool to help achieve the intent of these requirements, but RTA is the human evaluation of computer generated results. While the two are linked in this process, simply having RTCA running in the background does not constitute an assessment of the system.

The ERO Enterprise is seeking to understand how registered entities are implementing their obligations related to Real Time Assessments and may engage targeted efforts in 2019 to understand these implementations, including through Self-Certifications.

Areas of Focus

Table 6: Inadequate Real-time Analysis during Tool and Data Outages			
Standard	**Requirements**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
IRO-008-2	R4	n/a	Reliability Coordinator
TOP-001-4	R13	n/a	Transmission Operator

[28] ERO Reliability Risk Priorities; February 2018

Improper Determination of Misoperations

Protection systems are designed to remove equipment from service so the equipment will not be damaged when a fault occurs. Protection systems that trip unnecessarily can contribute significantly to the extent of an event. When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary. Such coordination errors occurred in the Arizona-Southern California Outages (see recommendation 19),[29] the August 14, 2003 Blackout (see recommendation 21),[30] and the Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015 (see recommendation 2).[31]

Furthermore, a protection system that does not trip–or is slow to trip–may lead to the damage of equipment (which may result in degraded reliability for an extended period of time), while a protection system that trips when it should not can remove important elements of the power system from service at times when they are needed most. Unnecessary trips can even start cascading failures, as each successive trip can cause another protection system to trip.

The 2018 RISC report[32] includes a key point that the ERO Enterprise, the impacted organizations, and the respective forums and trade organizations should perform post-event reviews to capture lessons learned and how to reduce the impact of future events. These reviews will be incomplete if not every event is noticed because the relay operations were not reviewed by qualified personnel. The report also identifies the risk posed by the increasing complexity in protection and control systems, further emphasizing the importance of a skilled workforce analyzing events and relay operations.

Areas of Focus

Table 7: Improper Determination of Misoperations

Standard	Requirements	Inactive/Future Enforcement Date *(if applicable)*	Entities for Attention
PRC-004-5(i)*	R1, R3	n/a	Generator Owner Transmission Owner

Inhibited Ability to Ride through Events

Generating plant protection schemes and their settings should be coordinated with transmission protection, control systems, and system conditions to minimize unnecessary trips of generation during system disturbances.[33]

Increased implementation of inverter-based resources has brought a focus on this issue. The ERO continues to raise awareness on inverter-based resource performance through NERC alerts[34] and industry outreach. Compliance monitoring should seek to understand how entities manage the risk of resource availability in this changing environment.

Areas of Focus

[29] See Arizona-Southern California Outages on September 8, 2011
[30] See Final Report on the August 14, 2003 Blackout
[31] See Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015
[32] ERO Reliability Risk Priorities; February 2018
[33] Considerations for Power Plant and Transmission System Protection Coordination, July 2015
[34] https://www.nerc.com/news/Documents/Inverter%20Alert%20Announcement.pdf

Table 8: Inhibited Ability to Ride Through Events			
Standard	**Requirements**	**Inactive/Future Enforcement Dates *(if applicable)***	**Entities for Attention**
PRC-019-2	R1	n/a	Transmission Owner Generator Owner
PRC-023-4	R1, R2, R6	n/a	Transmission Owner Generator Owner Planning Coordinator
PRC-024-2	R1, R2	n/a	Generator Owner
PRC-025-2	R1	n/a	Transmission Owner Generator Owner

Gaps in Program Execution

The ERO Enterprise has observed an increase in FAC-003-3 R2 violations resulting in vegetation contacts. These violations result from vegetation management programs that have less than adequate procedures to address identified problems or that fail to adapt to changing conditions, e.g., increased precipitation that accelerates vegetation growth.[35]

Change management weaknesses have also led to significant violations related to Facility Ratings and maintenance of Protection System devices. Some registered entities have Facility Ratings based on inaccurate equipment inventories, or ratings are not being updated during projects or following severe weather. Where records are not kept up to date, inaccurate models and damaged equipment can result. Failing to keep accurate inventories of equipment, following asset transfers, addition of new equipment, or mergers and acquisitions, is also causing incomplete Protection System Maintenance and Testing Programs that jeopardize the functionality of the equipment to respond to faults or disruptions on the electric system.

[35] *See* Notices of Penalty filed May 31, 2018 in FERC Docket Nos. NP18-11-000, NP18-12-000, and NP18-13-000.

Areas of Focus

Table 9: Gaps in Program Execution			
Standard	**Requirements**	**Inactive/Future Enforcement Dates *(if applicable)***	**Entities for Attention**
FAC-003-4	R1, R2, R3, R5, R6, R7	n/a	Generator Owner Transmission Owner
FAC-008-3	R6	n/a	Generator Owner Transmission Owner
PRC-005-6	R3	n/a	Generator Owner Transmission Owner

Regional Compliance Monitoring Plans

Based on RE consideration and assessment of ERO Enterprise risk elements and Regional Risk Assessments, each RE will provide details on its regional compliance monitoring plan. The regional plans include planned compliance monitoring activities for Compliance Audits, Spot Checks, Self-Certification, and Periodic Data Submittals. REs consider risk elements, both ERO-wide and Regional, entity-specific risks, and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with NERC Reliability Standards. These Regional compliance monitoring plans are included in Appendices A1 through A7 of this plan.

Regional Risk Assessments

In addition to considering ERO Enterprise risk elements, REs perform a Regional Risk Assessment to identify risks specific to their Region and footprint that could potentially impact the reliability of the BPS. After determining Region-specific risks identified for monitoring priority, REs will also identify the related NERC Reliability Standards and Requirements associated with those risks to focus monitoring activities. The standards and requirements identified for RE risk elements are not intended to be a static list that must be examined during all compliance monitoring activities (e.g., scoping for a Compliance Audit). Rather, the risk elements identified by the RE will serve as input when determining registered entity compliance oversight plans and considered when scoping entity-specific compliance monitoring engagements, like audits.

In the process of reviewing ERO risk elements to compile Regional Risk Assessments, REs are expected to

- gather and review RE-specific risk reports and operational information (e.g., interconnection points and critical paths, system geography, seasonal/ambient conditions, etc.);
- review and categorize potential RE-specific risks for compliance monitoring; and
- identify associated Reliability Standards and Requirements for IRAs, review of internal controls, and ultimately the compliance oversight plan.

The RE IPs will describe the Region-specific risks that result from the Regional Risk Assessment. The RE IPs should explain how REs identified risks that affect their footprints, including the reasons any ERO risk elements identified above are not included or applicable to the RE footprint. Although each RE will consider risk elements, and may use similar risk considerations, the output of the Regional Risk Assessments may differ as a result of RE characteristics and the uniqueness of each RE's footprint. REs are encouraged to align their RE risk elements with the ERO risk elements as much as possible since RE risk elements should be viewed as incremental to the ERO risk elements. Additionally, like ERO risk elements, Region-specific risk elements are not meant to reflect a comprehensive list of risks to the BPS. Rather, Region-specific risks are the focus risk areas for monitoring for a given implementation year.

NERC Oversight of RE Compliance Monitoring

NERC collects and reviews the RE IPs prior to posting the final version of the ERO CMEP Implementation Plan. NERC oversight of the RE IPs will focus on how the REs conducted Regional Risk Assessments and how the assessments' results serve as an input into the overall compliance monitoring plans for registered entities.

While REs should document all processes, conclusions, and results used to develop registered entities' compliance oversight plans, they will not need to obtain prior approval from NERC on oversight plans. However, REs should maintain supporting documentation to supplement NERC's review.

NERC oversight and regular training will help ensure that all processes discussed herein are implemented in a consistent manner throughout the ERO Enterprise.

Appendix A1: Midwest Reliability Organization (MRO) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the MRO as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

MRO has been actively participating in an ERO Enterprise initiative to revise the Compliance Oversight Plan (COP) process. As part of this initiative MRO is developing and prototyping new regional procedures for developing COPs. In an effort to improve alignment throughout the ERO Enterprise[36], MRO will adopt the ERO Enterprise COP Report template that was developed as part of this ERO Enterprise initiative by the end of the second quarter of 2019.

Other Regional Key Initiatives & Activities

As part of the Annual IP, MRO staff will periodically sample Compliance Exceptions, including those submitted through Self-Logging, to verify that the mitigating activities have been completed. The sample will come from only those Compliance Exceptions that have been identified by a registered entity as already mitigated or Compliance Exceptions that have a planned mitigation date that has passed.

Regional Risk Assessment Process and Results

MRO's risk-based compliance monitoring efforts begin with assessments of risk at the ERO, Regional, and individual entity levels. In the annual ERO Enterprise CMEP IP, a set of continent-wide risks called ERO Risk Elements and their associated NERC Reliability Standards and Requirements are identified. While the Risk Elements are not a comprehensive list of all risks to the reliability of the BPS, they typically reflect the risks identified by the ERO as top-priority reliability risks as well as the Reliability Issues Steering Committee's (RISC) ERO Priorities. Utilizing the ERO Risk Elements as a starting point, a comprehensive review of Region-specific risks called the Regional Risk Assessment (RRA) is performed by MRO staff, with input and review by MRO stakeholder organizational groups, focusing on reliability risks specific to the MRO footprint. The RRA allows staff and entity SMEs to consider the ERO-identified risks at the regional level and serves as an opportunity to provide feedback to the ERO for risks that have been identified for the MRO regional footprint. This process includes factors and considerations such as footprint and registered entity characteristics, geography, event analysis and misoperations, compliance history, and security considerations.

The 2019 MRO Regional Risk Assessment discusses many key risks, some of which have already resulted in recommended action for NERC or MRO and its stakeholder organizational groups. Each year, MRO conducts and publishes the RRA to identify and review risks posed to the BPS, and ensure the Reliability Standards and requirements are grouped into Performance Areas that are relevant and justified in order to best monitor those risks. The Performance Areas, in conjunction with the ERO Risk Elements, form the basis for MRO's compliance monitoring activities as a starting point for performing Inherent Risk Assessments, and culminating in the development of an entity's Compliance Oversight Plan. In addition, MRO staff seek to translate key findings and recommendations into region-specific feedback for risk assessment and mitigation activities, standards development, and other process improvements.

Regional Risk Elements and Areas of Focus

The 2019 MRO RRA did not identify any additional regional Risk Elements or Areas of Focus to add to the suite of ERO Risk Elements. In order to ensure that the ERO Risk Elements as well as any significant risks recognized by the MRO RRA are addressed through a risk-based approach to compliance monitoring, MRO has developed Performance Areas. Performance Areas organize requirements according to the activities performed by entities in order to promote

[36] ERO Enterprise Program Alignment Process

reliable operations of the BPS and simplifies the process of identifying those requirements that MRO plans to monitor in order to effectively address identified risks. The 2019 MRO Performance Areas list is available on MRO's website. Each Performance Area includes a description of the identified risk and a list of associated requirements that address those risks.

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the Annual Audit Plan that lists all planned audits for registered entities during the 2019 implementation year. The Annual Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

MRO's 2019 Compliance Audit Plan is located here: 2019 MRO Compliance Audit Plan on the MRO website. Throughout the implementation year, MRO may make updates to the 2019 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts spot checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the NERC ROP.

For 2019, MRO will continue with the use of Self-Certifications. As part of the Self-Certification process, registered entities will provide MRO with supporting evidence to substantiate determinations.

Self-Certifications are intended to provide MRO with reasonable assurance of compliance based upon the results of the registered entity's assessment. Where appropriate, MRO may utilize the Self-Certification instead of Compliance Audits or Spot Checks as the monitoring tool for specific NERC Reliability Standards and Requirements. The Self-Certification process helps improve the effectiveness of oversight and increase efficiency by relying on the work of registered entities in meeting compliance requirements.

Part of the process of relying upon the work of others includes MRO performing a review of the work and evidence supporting the Self-Certification results. MRO may re-perform the work, in part, to verify the accuracy of the Self-Certification determinations. In the event that further substantiation is needed, MRO staff may request additional evidence or include the applicable NERC Reliability Standards and Requirements in a subsequent Compliance Audit. The overall goal of the Self-Certification process is to provide reasonable assurance that the entity meets compliance with the applicable NERC Reliability Standards and Requirements.

As shown in Table A2.1, Self-Certifications will be performed over the implementation period (January 1 to December 31) on a quarterly basis for an identified baseline set of NERC Reliability Standards that have been identified both

through the RRA process and through an entity's IRA. An entity will receive a Self-Certification for a specific requirement if that entity's IRA, and analysis performed within the entity's COP, identifies that requirement as being one that should be monitored through a Self-Certification. In other words, the input used by MRO to make this decision for each entity is based on a registered entity's specific inherent risk to the BPS, its compliance history, and other performance considerations. MRO will apply professional judgement, for entities who have yet to receive a completed IRA and/or COP, in determining the entity's inclusion in a given Self-Certification.

MRO registered entities who have received a COP may notice a change in MRO's 2019 Self-Certification schedule. MRO's review of the MRO Regional Risk Assessment, ERO risk elements and areas of focus have led to this change. A FAC-003-4 Self–Certification was added to Quarter 2 of 2019 and a FAC-008-3 Self-Certification was added to Quarter 4 for 2019 to address risks identified through this review. To accommodate this effort, PRC-005-1.1b/6 and PRC-019-2 were transitioned to be monitored through Audits and PRC-015-1 R1 was removed because it is scheduled for retirement.

The intent of the quarterly frequency is to:

- Disperse the workload (allows sufficient time for completion and review) and
- Promote continuous self-monitoring of compliance.

Table A1.1: 2019 Self-Certification Schedule

Standard	Requirement	Quarter
CIP-002-5.1a	R1,R2	Q1
EOP-008-1	R1,R7	Q1
FAC-003-4	R3,R6,R7	Q2
EOP-005-2	R1,R9,R14	Q3
FAC-008-3	R3,R6	Q4

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the ERO Enterprise 2019 Periodic Data Submittal.

Compliance Outreach

Table A1.2: Compliance Outreach Activities

Outreach Activity	Anticipated Date
MRO Newsletter	Six times a year
MRO Hot Topics	Periodically as needed
MRO Webinars	Periodically as needed
MRO Reliability Conference	Twice a year (Spring and Fall)
MRO Security Conference	Fall 2019
MRO Compliance Monitoring and Enforcement Program (CMEP) Conference	Fall 2019
Registered entity HEROs outreach events	At request of the entity
MRO Risk-Focused Conference or Training	Annually

Appendix A2: Northeast Power Coordinating Council (NPCC) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the NPCC as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- NPCC will continue to offer formal O&P Internal Control Evaluations to all entities on the 2019 audit schedule.
- NPCC will also offer to perform CIP Internal Control Evaluations on entities that have already had their initial CIP Version 5 audit.
- NPCC will refresh existing IRA's and use the 2019 ERO and NPCC Implementation Plans to develop Compliance Oversight Plans (COPs) for its 2019 monitoring engagements.

Other Regional Key Initiatives & Activities

- In 2019, NPCC will continue with a cyber-security and physical security outreach program for volunteering entities.

Regional Risk Assessment Process and Results

NPCC considers the Risk Elements identified in the ERO CMEP Implementation Plan and the Risk Factors identified in the ERO Guide for Compliance Monitoring to identify important reliability risks within NPCC's footprint. If NPCC concludes that any of the ERO Risk Elements are not relevant reliability risks within NPCC's footprint, NPCC will provide documented rationale.

NPCC determines whether any additional regional risks specific to the NPCC footprint, but sufficiently different from the risks identified in the ERO Implementation Plan, should be added as Regional Risk Elements into the NPCC Implementation Plan. Input into Regional Risk Element determination can take the form of Enforcement trends, audit team observances, ERO or Regional events, issues raised by NERC or stakeholder groups, etc. Often, additional regional risks specific to the NPCC footprint may be categorized within a NERC identified Risk Element and would not likely require an additional Regional Risk Element.
In the event NPCC identifies an additional Regional Risk Element that is not included in the ERO CMEP Implementation Plan, NPCC will provide justification and documentation regarding the additional Regional Risk Element.

In the development of the standards and requirements that appear in this regional plan, NPCC considered the 2019 ERO Risk Factors and other tangible Bulk Electric System (BES) attributes such as entity functional registration, transmission assets, Remedial Action Schemes, black start plans and facilities, generation assets, role of Under Frequency Load Shedding (UFLS) , Enforcement trends, historical events, etc.

NPCC did not expand the requirements under ERO Risk Elements.

NPCC identified three Regional Risk Elements for 2019.

Regional Risk Elements and Areas of Focus

The table below contains NPCC Regional risk elements, for focus during 2019, based on the NPCC's Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of a registered entity's compliance oversight plan (COP).

Table A2.1: Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Improper BES Cyber System Classification	In order to verify proper classification of BES Cyber Systems, and ensure appropriate protections are applied, NPCC will review select entities for compliance to CIP-002-5.1.	CIP-002-5.1, R1, R2
Improper UFLS Settings	Although rarely used, UFLS schemes owned by the TO and DP are an extremely important aspect in limiting the extent of major disturbances. This is especially true in NPCC which has transmission corridors that are of the radial nature. As such, NPCC has a regional UFLS standard and will focus on the design and implementation of UFLS programs which are key in order to prevent a total system blackout like those that occurred in 1965, 1977, and 2003. In addition, the proper underfrequency settings at the GO directly correlate to the success of the UFLS program.	PRC-006-NPCC-1 R4 (TO, DP) R7 (TO, DP) R13 (GO)
Failure to Report Generator Capabilities	Accurate generator capabilities are necessary for the planning and operation of a reliable bulk electric system. This Standard is the leading non-compliance issue in the NPCC footprint on 2018. While the violations were not deemed to be highly impactful individually, the high number of non-compliance issues is a concern.	MOD-025-2, R1, R2

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The NPCC Compliance Monitoring Plan includes the 2019 Compliance Audit Plan that lists all planned audits for registered entities during the 2019 implementation year. The 2019 Compliance Audit Plan, located on NPCC's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2019 Compliance Audit Plan for NPCC is located here: Audit Schedules. Throughout the implementation year, NPCC may make updates to the 2019 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

NPCC conducts spot checks based on a registered entity's COP, or at RE discretion at any time. NPCC may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. NPCC will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

NPCC determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. NPCC will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced notice according to the NERC ROP.

NPCC will conduct Self-Certifications for Entities that have Low Impact BES Cyber Systems to ensure that the entity has completed its assessment of cyber assets properly. As shown in the table below, NPCC will perform Self-Certifications on a quarterly basis in 2019, with a 45-day advance notice given to the entity. The entity will receive the notice of the requirement covered by the Self-Certification and will be instructed to submit their compliance documentation into the NPCC compliance portal. Only a subset of the entities registered for the function that applies to the chosen requirement will receive the Self-Certification notification in the particular quarter.

Table A2.2: Self-Certification Schedule

Quarter 1			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	January 22	March 8
Quarter 2			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	April 15	May 30
Quarter 3			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	July 15	August 29
Quarter 4			
Standard	**Requirement**	**Notification Date**	**Due Date**
CIP-002-5.1a	R1, R2	October 15	November 29

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. NPCC follows the ERO Enterprise 2019 Periodic Data Submittal posted here: Periodic Data Submittals.

Compliance Outreach

Table A2.3: Compliance Outreach Activities

Outreach Activity	Anticipated Date
Spring and Fall Workshops – NPCC holds semi-annual workshops as a primary mechanism for outreach to registered entities.	May 2019 November 2019
Introduction to NPCC for Beginners – NPCC provides an introductory class for those new to CMEP activities prior to the May and November workshops.	May 2019 November 2019

Table A2.3: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Physical Security Information Exchange Sessions - The sessions take place at the May and November workshops and address NPCC Awareness Programs, Security Strategies, and subjects such as CIP-014 implementation, and evolving physical threats to the electric industry.	May 2019 November 2019
CIP and O&P Internal Controls Evaluation (ICE) Outreach Session – The sessions will take place at the May and November workshops to provide awareness and promote participation in the program. It will provide NPCC's purpose, approach and implementation of the voluntary ICE process, including expectations, tools, education/examples, best practices, deliverables, and feedback into Risk-Based CMEP.	May 2019 November 2019
Cyber Security Outreach for Non-Nuclear Generators – This will provide guidance to non-nuclear sites on all facets of their on-site cyber security.	Throughout 2019
Physical Security Outreach for Non-Nuclear Generators – This will provide guidance to non-nuclear sites on all facets of their on-site physical security.	Throughout 2019
Individual Meetings with Registered Entities – NPCC will meet with registered entities for specific CMEP related issues if requested and warranted.	
CDAA – NPCC will issue announcements via CDAA (the NPCC Compliance Portal) informing registered entities of CMEP aspects.	
Webinars – NPCC will conduct CMEP related webinars as needed. NPCC conducts pre-ICE webinars for all participants.	
FAQs – NPCC will post FAQs on an as needed basis.	
Compliance Guidance Statements – NPCC may issue Compliance Guidance Statements to offer clarification on the compliance approach associated with the NERC Rules of Procedure, NERC Reliability Standards, or NPCC Regional Reliability Standards.	
Registered Entity Surveys – NPCC will issue surveys to registered entities on an as needed basis. Such surveys have included acquiring registration data, BES element data, workshop content preferences, etc.	
Website – The NPCC website provides information in the areas of Standards, Registration, Compliance Monitoring, and Compliance Enforcement.	

Appendix A3: ReliabilityFirst Corporation (ReliabilityFirst) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the ReliabilityFirst as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

ReliabilityFirst will support the ERO Program Alignment initiative, and follow and perform the ERO Risk-Based Compliance Oversight Framework described in the ERO Enterprise Compliance Monitoring Enforcement Program CMEP IP. The 2019 ERO Enterprise CMEP IP identifies a number of new Risk Elements and Areas of Focus, which provide a starting point for ReliabilityFirst's risk analysis and COP development. However, the 2019 ERO Enterprise CMEP IP recognizes that it does not include the complete set of risks that may affect the Bulk Power System (BPS) which Regional Entities are expected to consider—local risks and specific circumstances associated with individual registered entities within their footprint—when developing COPs.

To account for such risks and circumstances, ReliabilityFirst performed a Regional Risk Assessment (RRA), which identified potential risks within the ReliabilityFirst region. ReliabilityFirst may monitor additional NERC Reliability Standards and Requirements associated with these risks. ReliabilityFirst also has the discretion to add, subtract, or modify Standards and Requirements in its COPs for individual registered entities as it deems necessary based on the individual registered entity IRA and COP development.

ReliabilityFirst monitors FERC and NERC activities, system events, and events in the ReliabilityFirst Region. Based on these monitoring activities, ReliabilityFirst may modify its CMEP IP throughout the year to address and mitigate situational awareness and reliability, security and resiliency issues as they arise.
ReliabilityFirst will continue to use a risk-based enforcement approach consistent with the ERO Enterprise. To that end, ReliabilityFirst will exercise professional judgment in enforcement by using streamlined dispositions for qualified minimal and moderate risk noncompliance. Penalties will generally be reserved for situations involving serious risk violations or programmatic failures.

ReliabilityFirst will continue to utilize self-logging for qualified registered entities, and will continue to verify completion of only a sample of mitigating activities associated with self-logged noncompliance.

Additionally, where ReliabilityFirst has confidence in a registered entity's internal compliance program as a result of positive performance on an ICE, ReliabilityFirst may narrow the audit scope and audit periodicity to reflect the compliance maturity of the registered entity. To support a strong culture of compliance and to demonstrate robust internal controls, registered entities are encouraged to continually perform self-assessments of their compliance programs and internal controls on an ongoing basis.

ReliabilityFirst will notify registered entities of the NERC Reliability Standards and Requirements for which they will be monitored via any of the following means: posting of the Compliance Monitoring Schedule for Data Submittals; the Audit Notification Letter; the Spot Check Notification Letter; the Self-Certification notification; and the IRA report which address the registered entities tailored COP.

Other Regional Key Initiatives & Activities

Self-Certifications

ReliabilityFirst will perform Self-Certifications as needed throughout 2019. A Self-Certification requires an entity to submit their supporting documentation to substantiate their self-assessment. The Self-Certifications for a registered entity will be based upon the specific COP resulting from the registered entity's IRA and or identification of any

additional ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls in the year.

Annual Compliance Monitoring Plan

ReliabilityFirst developed a process to be used by the ReliabilityFirst (RF) Compliance Monitoring Department (CoMo), with input from Risk Analysis and Mitigation Department (RAM) in creating an annual plan for compliance monitoring engagements and activities. The process of annually creating the monitoring plan is a risk-based approach for all compliance oversight, while optimizing the use of ReliabilityFirst resources. The plan, because is it risk based, is also an effective method of mitigating those risks that are associated with standards across the RF footprint. The annual plan may also result in more frequent touch points (e.g. compliance oversight activity) for those entities deemed to have a high risk profile. This process provides a framework to be used in developing the Regional annual plan for compliance monitoring by taking into account an entity's individual Compliance Oversight Plan, their Inherent Risk Assessment results, and their operational performance, etc.

The Entity COP and RF Annual Compliance Monitoring Plan can be subject to change throughout the year as other regional or entity risks are identified. As a result of this process, this plan will be reviewed and updated at least on an annual basis to ensure it correlates with the ERO, regional and entity risks.

Regional Risk Assessment Process and Results

The Regional Risk Assessment identifies risks within the ReliabilityFirst Region that could potentially impact the reliability of the BPS. To accomplish the RRA, ReliabilityFirst utilizes a cross-functional team of internal SMEs (the RRA Team) to review and analyze information and data to determine the highest-priority risks to the ReliabilityFirst region. The types of region-specific information and data the RRA Team reviews includes, but is not limited to: US Population & Census Data, Event Analysis Data (e.g., OE-417 and EOP-004 reports and Lessons Learned), Generation Availability Data System (GADs), Transmissions Availability Data System (TADS), Misoperations, Load Analysis, Locational Marginal Pricing, System Operating Limits (SOL), Interconnection Reliability Operating Limits (IROL), Interconnection Points, Cyber Security data, Physical Security data, and data on Threats and Vulnerabilities. After a period of information gathering, analysis, and decision making, the RRA team develops the results of the RRA in the form of ReliabilityFirst Risk Elements and Risk Areas.

ReliabilityFirst may include additional detail on the Risk Elements and their associated NERC Standards and Requirements in the registered entity-specific COPs.

The Regional Risk Assessment is performed annually, but may be updated more frequently as necessary. As new and emerging threats and risks are identified, system events take place, and compliance monitoring activities are performed, ReliabilityFirst will update the Regional Risk Assessment to keep current with potential issues, threats, and risks.

Regional Risk Elements and Areas of Focus

The 2018 ReliabilityFirst Regional Risk Assessment explored and analyzed the following risk areas: Cyber Security Emerging Threats, Information/Asset Security, Audit Findings and Risk, IROLs, Situational Awareness, Transmission, Generation, Wind Generation, Changing Generation Mix, Protection System Misoperations, Planning/Modeling, Event Response, Environmental Factors, and Emerging Risks.

As a result, the 2018 ReliabilityFirst Regional Risk Assessment identified the Regional Risk Elements listed in Table A4.1 below. ReliabilityFirst will assess these Regional Risk Elements and engage entities as appropriate throughout 2019 in order to address these risks. The RRA also identified some potential Regional Risks that have no associated standards and requirements as Areas of Focus. These Regional Risks will be further evaluated, and other techniques

available to ReliabilityFirst (i.e. Assist Visits, Appraisals, Workshops, Reliability and Compliance Open Forum Calls, Targeted Outreach, etc.) will be used to drive entity behavior and activities towards mitigating those risks.

ReliabilityFirst also reviewed the 2019 ERO Risk Elements with associated Areas of Focus and concurs with the specified NERC Reliability Standards and Requirements. ReliabilityFirst did not determine a need to expand on the 2019 ERO Risk Elements and Areas of Focus.

As new Risk Elements and Areas of Focus are identified and validated, their information will be communicated and implemented in future revisions of the ReliabilityFirst CMEP Implementation Plan per the Implementation Plan revision process outlined by NERC.

Table A3.1: Regional Risk Elements

Regional Risk Element	Justification	Associated Standard and Requirement(s)
Forced Transmission Outages of single or multiple lines in close proximity	ReliabilityFirst is identifying this Regional Risk Element due to an increased volume of unrecoverable capital-project transmission outages for reinforcements due to the generation retirements in the RF region. The risk to the BPS associated with forced transmission outages increases due to the number of facilities already out of service for both maintenance and capital projects. While maintenance outages are typically shorter and can be recovered, the capital project outages are often longer and cannot be recovered quickly, making the system less resilient during a storm or following a misoperation. ReliabilityFirst has seen instances of forced outages in conjunction with previously scheduled outages forcing entities to take emergency actions to recover.	TOP-002-4 R1-R7

Table A3.1: Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Resource Reserve Margin	Planning Reserve Margins (PRM) are designed to provide an amount of generation capacity that, after accounting for planned and unplanned outages, will reliably supply expected demand. Coupled with probabilistic analysis, calculated planning reserve margin requirements have been an industry standard used by planners for decades as an indication of resource adequacy. RF is comprised of two markets that procure generation to satisfy the required PRM in different ways. One registered entity offers a forward looking market that procures generation for the future at increasing amounts as the planning cycle moves forward. The capacity costs and resource requirements provide the market signals for new generation to be built. Another ReliabilityFirst registered entity operates a voluntary capacity market to procure resources for the Electric Distribution Companies (EDC). EDCs can also procure required resources on their own. With this entity's PRM falling below their requirement in 5 years, the entity may not be providing the proper signal to the Generator Owners and Operators to build capacity to meet further needs. This will limit the options for this entity's system operators have to operate the BPS in the future. ReliabilityFirst is identifying this as a Regional Risk Element for 2019.	BAL-502-RF-03 R1-3
IROL Exceedances	ReliabilityFirst is identifying this Regional Risk Element since M-8 of the 2018 ERO State of Reliability Report (page 160) indicates hundreds of IROL exceedances (<30 minutes) in the Eastern Interconnect in 2016/2017. With ReliabilityFirst in the Eastern Interconnect, it believes this identified risk needs to be monitored in order to raise entity awareness. An IROL exceedance could be one contingency away from possible cascade, uncontrolled separation, and/or instability.	EOP-011-1 R1-R6 IRO-009-2.1 R1-R4 TOP-001-4 R1, R3, R4, R7, R8,R9

Table A3.1: Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Identifying IROL-like conditions (Situational Awareness of possible cascade, uncontrolled separation, and/or instability beyond pre-determined IROL's).	ReliabilityFirst is identifying this Regional Risk Element due to frequent category 1h.v events (i.e. State Estimator Outages) in conjunction with unrecoverable capital-project transmission outages for reinforcements due to the generation retirements in the RF region. Reliability Coordinator and Transmission Operator situational awareness tools such as Voltage and Transient Stability Analysis plus Cascading Analysis require the State Estimator to be converging. With an increase in unrecoverable scheduled outages, additional analysis is needed following a forced outage to determine if the next contingency will lead to cascading, uncontrolled separation, and/or instability before emergency actions are implemented.	IRO-002-5 R1-R6 IRO-008-2 R1, R3, R4, R5, R6 TOP-001-4 R8, R9

Table A3.2: Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Insufficient Long-Term Planning Due to Inadequate Models	ReliabilityFirst is expanding the ERO risk element to monitor this since RF is aware of its RTO generation retirement list plus new generation in queue. For example, ReliabilityFirst is experiencing coal/nuclear generation retirements along the Great Lakes plus the increase of natural gas generation due to the Marcellus shale in Pennsylvania. Furthermore, Changing Generation mix (coal/nuclear retirements plus subsidies) is addressed within the 2018 DOE and FERC Rulings. Themes include inertia, misoperations, capacity, frequency response, inverter based technology, etc. Based on these facts, Regional awareness is a focus to understand how changing generation mix impacts both reliability and resiliency within the ReliabilityFirst region.	BAL-003-1.1 R1-R4 BAL-502-RF-03 R1-R3 EOP-005-2 R1.4,R6,R7,R9 EOP-005-3 R1,R6,R8 (4/1/19) MOD-001-1a R1-R9 PRC-019-2 R1-R2 PRC-024-2 R1-R4 PRC-025-2 R1 PRC-026-1 R2,R3,R4 TPL-001-4 R1-R8 VAR-002-4.1 R1-R6

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2019 Compliance Audit Plan that lists all planned audits for registered entities during the 2019 implementation year. The 2019 Compliance Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2019 Compliance Audit Plan for this RE is located on ReliabilityFirst's website. Throughout the implementation year, the RE will may make updates to the 2019 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts spot checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the NERC ROP.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2019 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website.

Compliance Outreach

Table A3.3 Compliance Outreach Activities

Outreach Activity	Anticipated Date
ReliabilityFirst Newsletter - The ReliabilityFirst Newsletter provides registered entities with news and information relating to reliability activities.	Bi-monthly throughout the year.
Monthly Compliance Update Letter - The ReliabilityFirst Monthly Compliance Update Letter provides registered entities with any changes made to the Compliance Monitoring Schedule and the due dates for compliance submittals.	Monthly throughout the year.
ReliabilityFirst Website - The ReliabilityFirst website provides compliance and technical materials to support compliance program performance. There is also an area titled the Knowledge Center where ReliabilityFirst is committed to sharing our expertise, and leveraging the expertise of our entities, to advance industry practices surrounding risk identification, mitigation, and prevention.	Monthly throughout the year.
Workshops/Seminars/Webinars - ReliabilityFirst Reliability workshops/seminars or webinars will be scheduled to assist the registered entities in the understanding of their responsibilities to satisfy compliance to the Reliability Standards throughout the year.	Semi-annual (Baltimore, MD: May 1-3, 2019 and Independence, OH: October 1-3, 2019.

Table A3.3 Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
CIP Outreach and Awareness – ReliabilityFirst will conduct CIP outreach, including training and education engagements, to ensure that registered entities have confidence in their implementation of the CIP Standards and Requirements. These engagements will primarily be conducted as Workshops and Webinars.	Sessions are held as requested by our registered entities, built into the workshop material and or addressed though our Assist Visit program.
Periodic Reports - ReliabilityFirst will provide Periodic Reports to its registered entities identifying compliance related activities that the registered entities continue to struggle with. These reports will be posted on the ReliabilityFirst website.	Periodically throughout the year.
Reliability and Compliance Open Forum Calls - ReliabilityFirst has instituted a monthly conference call to provide an open forum for registered entities to call and voice concerns, ask questions, and to gain information about upcoming items. The calls are also used to share reliability issues, trends, and information related to existing or emerging risks. These calls were previously called our Open Compliance Calls, but in 2018 we are repurposing these calls to focus on reliability and compliance issues.	Monthly throughout the year.
Assist Visits - ReliabilityFirst has instituted a program whereby a registered entity may request a one-on-one or small group meeting where guidance on compliance related activities can be provided. These Assist Visits can be in the form of a conference call, web meeting, or on-site visit. Topics can range from helping a registered entity become more familiar with compliance related material and activities, to special guidance and education when either the registered entity or ReliabilityFirst believes the registered entity needs special attention or additional help.	As requested by our registered entities.
CIP Low Impact Focus Group - The CIP Low Impact Focus Group consists of entities in the ReliabilityFirst footprint who are responsible for compliance for low impact BES Cyber Systems. The group holds monthly meetings to discuss various topics, and holds periodic webinars with featured speakers. The goals of the group include the following: • Assist registered entities with CIP low-impact assets • Communicate lessons learned from high- and medium-impact entities • Communicate lessons learned from other Regions • Provide a forum for general questions • Provide a forum to communicate good practices	Monthly throughout the year.

Appendix A4: SERC Reliability Corporation (SERC) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the SERC as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

NERC Compliance Monitoring Enforcement Program (CMEP) tools used by SERC in 2019 will include Compliance Audit, Spot Check, and Self-Certification. SERC will focus its resources on higher risk items identified primarily through entity-specific Inherent Risk Assessments (IRAs). SERC will continue to consider an outreach component to on-site compliance audits, as well as assessing any internal controls. During the on-site week, the entity may engage SERC compliance audit staff to address approaches and ask questions in both the Operating and Planning (O&P) and Critical Infrastructure Protection (CIP) compliance areas. SERC continues to enhance its Frequently Asked Questions process, where SERC subject matter experts (SMEs) address questions asked by entities.

Reviews of internal controls during Compliance Monitoring activities will continue to mature throughout 2019. SERC completed IRAs for all registered entities in its footprint by the end of 2017, and intends to refresh each registered entity's IRA at least every three years, or more frequently as appropriate, based on certain risk-based triggers. SERC will continue to develop a registered entity's Compliance Oversight Plan (COP) based on the risks identified during the IRA process, entity performance data, and regional trends.

SERC continues to look for ways to strengthen reliability, reduce risk to the Bulk Electric System (BES), and promote a culture of reliability excellence. In past compliance engagements, SERC Compliance Monitoring staff identified discrepancies between Facility Ratings and the ratings used in system operations. SERC will review operational ratings and compare those ratings to the Facility Ratings developed in accordance with Registered Entity Facility Rating methodologies. SERC will continue to conduct asset reviews in the field by inspecting substations and generating facilities, verifying that Equipment Ratings used to develop Facility Ratings match the actual equipment in the field. In addition, these ratings will be verified in planning and operations models and in Energy Management Systems (EMS) during control center tours. Failure of registered entities to properly develop and apply Facility Ratings can produce incorrect System Operating Limits (SOLs) and lead to BES equipment damage.

Other Regional Key Initiatives & Activities

SERC continues to support its Industry Subject Matter Expert (ISME) program, in which SERC audit teams occasionally use volunteers employed by Registered Entities in the SERC Region to supplement both O&P and CIP compliance audit teams. The program approach focuses on identification, qualification, and assignment of ISMEs to match the technical resource needs of the specific compliance audits. Information about SERC's ISME program is available on the SERC website.

SERC gained an additional 11 Registered Entities in our footprint as a result of Southwest Power Pool (SPP) RE's recent dissolution. On April 30, 2019, FERC approved the dissolution of the FRCC RE, and the transfer of 35 registered entities in the FRCC footprint to SERC took place on July 1, 2019. The FRCC registered entities transferring to SERC should follow the revised Regional CMEP IP for SERC. These consolidations affected SERC staffing, and has necessitated some additions to SERC's CMEP staff. SERC strategic CMEP planning will continue to focus on rigor and effectiveness to address potential challenges associated with Regional consolidation.

SERC will continue to promote and support the Multi-Regional Registered Entity (MRRE) program in 2019. As a Lead Regional Entity (LRE), SERC will lead efforts related to all aspects of the CMEP. The LRE coordinates and conducts creation and revisions of a Registered Entity's IRA with input from each Affected Regional Entity (ARE), and determines the appropriate Compliance Oversight Plan (COP). This coordinated oversight should eliminate

unnecessary duplication of compliance monitoring and enforcement activities. In addition, as the ARE, SERC will continue to collaborate and coordinate with the LREs to ensure IRAs, compliance monitoring, and enforcement activities include SERC Regional considerations.

Regional Risk Assessment Process and Results

Reliable operation of the bulk power system (BPS) is crucial. SERC recognizes that protecting the reliability of the electric grid in the SERC Region is the responsibility of its members with SERC's support. Achieving a secure and reliable grid requires registered entities to remain diligent about reliability and resiliency within their service areas. SERC is responsible for assisting registered entities in identifying Regional reliability risks and coordinating reliability-related activities throughout the Region.

SERC has coordinated efforts with its stakeholders to develop and implement a continuous program of Regional assessment of potential reliability risks to the SERC Region BPS. The SERC Regional Reliability Risk Assessment program is a robust, centralized process for analyzing, prioritizing, addressing, and communicating significant risks and risk-controlled initiatives.

The program's objective is to improve BPS reliability through a coordinated effort of a cross-functional organization that identifies, analyzes, prioritizes, and addresses reliability risks. In conformance with the ERO risk-based CMEP, the SERC process consists of the following major activities:

- Identify or nominate risks
- Determine time horizon (i.e., immediate, next-day, operational, seasonal, and long-term)
- Assess and rank risk:
  - Determine the consequence or severity impact(s)
  - Determine the probability of occurrence
  - Assign High, Medium, or Low from the Risk Assessment Matrix
  - Prioritize risks
  - Store the information in the Risk Registry
- Develop risk control initiatives
- Monitor and reevaluate risk impact

SERC's Reliability Risk Team (RRT) is a major participant in the program. The RRT is responsible for identifying risks based on the probability of occurrence and severity of impact. SERC's RRT identified three different areas of risk:

- Operational Risk(s)
- Engineering Risk(s)
- Critical Infrastructure Protection (CIP)

SERC also identified risk elements within each group. These identified risk elements align with the ERO-wide risk elements:

- Critical Infrastructure Protection
- Severe Weather Events
- Protection System Failures/Improper Misoperation Determination
- Planning and System Analysis/Gaps in Data Management

As new and emerging threats and risks are identified, system events occur, and compliance monitoring activities are performed, SERC's RRT will update the Regional Reliability Risk Assessment program to include current potential issues, threats, and risks. In addition, as SERC performs IRAs of its registered entities, SERC will review potential risks to BPS reliability posed by individual registered entities.

The coordination among the SERC registered entities, SERC technical committees, SERC staff, neighboring system personnel, and other members of the ERO is vital to the understanding and analysis of potential major reliability issues. In 2015, SERC implemented its Integrated Risk Management (IRM) program. The IRM process addresses SERC's need to gather and analyze data to support risk-based techniques. SERC determined the best method to support this initiative is through uninhibited sharing of data across SERC program areas. The objective of the IRM is to support risk-based compliance monitoring and enforcement by defining and deploying sound business policies, procedures, and process tools across all SERC departments to implement a comprehensive integrated risk management program.

SERC, through its members and staff, is heavily engaged with NERC and its initiatives. SERC's risk management programs enable it to focus compliance monitoring oversight activities on those NERC Reliability Standards which, if violated, would pose the greatest risk to the reliable operation of the SERC portion of the BPS.

Regional Risk Elements and Areas of Focus

The table below contains the regional risk elements, and expended ERO risk elements, for focus during 2019 based on the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of a registered entity's compliance oversight plan (COP).

Table A4.2: SERC Regional Risk Elements

Regional Risk Element	Justification	Associated Standard and Requirement(s)
Severe weather events and impacts on transmission and generation	The SERC Region historically has experienced severe weather events, such as hurricanes and tornados. These events usually create system contingencies beyond existing planning criteria. However, emergency procedures and other operating standards still apply. Over the years, the Region has identified this risk and emphasized system preparedness through the assessment of SERC Performance Information for Identifying Potential Reliability Risk, as well as through the NERC Reliability Assessment reporting process. SERC is also focusing on operational risks, such as deficient entity response and performance, identified during severe weather events. It is important from an operational perspective to consider proper operation of the system during these events, with respect to balancing resources and demand, and necessary communication capabilities.	BAL-002-2(i), R1, R2, R3 BAL-005-0.2b, R7 COM-002-4, R1, R6, R7 EOP-005-2, R1 (EOP-005-3, R1 in effect 4/1/19) EOP-006-2, R1, R7, R8, R9, R10 EOP-008-1, R1, R2, R4, R7 EOP-011-1, R2, R3, R4, R6

Table A4.2: SERC Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Power System Coordination and Modeling	The following can introduce risk to the reliable operation of the BPS in the SERC Region: • Increased use of the BPS in a manner for which the system was not originally designed • Inadequate operating experience • Insufficient coordinated studies • Insufficient coordinated operations • Uncertainty of resources and resource mix • Available generator ability to adequately respond to frequency changes SERC's unique Planning Coordinator (PC) structure necessitates coordination throughout the SERC Region. Many of the PCs in the SERC Region coordinate with multiple entities. Performing modeling without appropriate coordination would risk the validity of SERC study performance.	FAC-014-2, R5 MOD-027-1, R2 PRC-001-1-1.1(ii), R3, R4, R5 PRC-019-2, R1 TOP-002-4, R4 VAR-002-4.1, R1, R3
Underfrequency Load Shedding (UFLS) Schemes	The SERC UFLS Regional Standard is to establish consistent and coordinated requirements for the design, implementation, and analysis of UFLS programs among applicable SERC registered entities. The Regional Standard adds specificity not contained in the NERC Standard for development and implementation of the UFLS scheme in the SERC Region that effectively mitigates the consequences of an under-frequency event.	PRC-006-SERC-02, R1, R2, R3, R4, R5, R6
Loss of Major Application (EMS/SCADA, Communications Capability)	SERC has seen an increase around events resulting in unplanned EMS/SCADA outages in the last two years. These event durations are exceeding 30 minutes with loss of communications and control, limiting system visibility. Also, testing of data exchange capability is important to ensure proper functionality and to help prevent possible unplanned outages.	COM-001-3, R12 EOP-008-1, R5, R6 TOP-001-4, R9, R21, R24

Table A4.2: SERC Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Critical Infrastructure Protection	The area of critical infrastructure protection remains an area of significant importance. SERC continues to focus in this area due to the risk of cyber security controls for BES cyber systems being compromised and leading to unauthorized electronic access to those systems; introduction of widespread malware; improper management of employee and insider access; and extreme physical events including sabotage, attacks, and vandalism. In addition, some SERC registered entities have not yet been audited on the CIP-014-2 physical standard.	CIP-004-6, R5 CIP-005-5, R1 CIP-007-6, R1 CIP-014-2, R1, R2, R3, R4, R6
Maintenance and Management of BPS Assets (Improper Misoperation Determination)	SERC is expanding the NERC area of focus around "Improper Misoperation Determination," based on operational risks and trends in misoperations in SERC.	PRC-004-5(i), R2, R4

The table below contains former FRCC regional risk elements and areas of focus for 2019. In consideration of these regional specific risks, SERC will include these as focus areas that will be considered in risk-based reliability assurance, **for former FRCC regional entities only**, for the remainder of 2019.

Table A4.2: 2019 FRCC Regional Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Extreme Physical Events	The Florida peninsular geography, along with its susceptibility to hurricanes and limited connections to the Eastern Interconnect, increases the risk that an event may occur which can result in system restoration from Blackstart Resources. Florida's susceptibility to hurricanes increases the risk of a control center being inoperable. The Florida peninsular geography, along with its susceptibility to hurricanes, limited connections to the Eastern Interconnect and the existence of a significant RAS that could result in islanding increase the risk of an island event occurring.	CIP-009-6, R2 EOP-005-3, R8, R15 PRC-006-3, R8, R9
Dependence on RAS Schemes	The Florida region has RAS separation schemes that could impact a major portion of the Florida peninsular if they do not operate as planned.	PRC-016-1, R1, R2

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how an RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2019 Compliance Audit Plan that lists all planned audits for registered entities during the 2019 implementation year. The 2019 Compliance Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2019 Compliance Audit Plan for this RE is located on SERC's website. Throughout the implementation year, the RE will may make updates to the 2019 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts spot checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the NERC ROP.

SERC also utilizes Self Certifications. The results of an entity's Inherent Risk Assessment (IRA) determine the need for Self-Certifications. Low-risk Standards and Requirements are primarily the focus of the Self-Certification monitoring method, although for a small entity, high or medium risk Standards and Requirements could come into scope as well. Self-Certification forms require the inclusion of supporting evidence to provide reasonable assurance of compliance. This process could also include questions and/or data requests.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2019 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website.

Compliance Outreach

Table A4.3 Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Outreach Events SERC outreach events occur throughout the year to accommodate the training and education needs of registered entities. Planned events, listed here, with specific themes will also feature compliance and reliability topics of importance at the time of the event. SERC staff post event details on the Upcoming Events page of the SERC website, which can be accessed through the Event Calendar on the home page or under Outreach > Events Calendar. Outreach events are promoted in the monthly SERC Transmission newsletter and email notifications; and reminders are sent to primary and alternate compliance contacts for all registered entities within the SERC Region footprint. Open Forum Webinar SERC 101 Webinar Spring Compliance Seminar (Charlotte, NC and WebEx) Small Entity Seminar Open Forum Webinar Open Forum Webinar CIP Compliance Seminar (Charlotte, NC and WebEx) Fall Compliance Seminar (Charlotte, NC and WebEx)	 Jan 28, 2019 Feb 18, 2019 Mar 5-6, 2019 Mar 6, 2019 May 6, 2019 Jul 29, 2019 Sep 17-18, 2019 Oct 8-9, 2019
Focused Workshops and Webinars Supplemental focused events scheduled on an as-needed basis provide outreach and training for new or revised Reliability Standards, targeted groups of registered entities based on functional registration, and ERO initiatives.	As needed throughout the year
FAQ & Lessons Learned SERC staff subject matter experts address technical questions received from registered entities, and then post the responses on the website, along with lessons learned, to share information and best practices. These items, listed by topical categories, are posted on the SERC website under Outreach / FAQ & Lessons Learned.	Available throughout the year

Table A4.3 Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
SERC Transmission Newsletter SERC distributes its SERC Transmission newsletter to registered entities within the Region each month and posts it on the SERC website. It is also distributed throughout the ERO Enterprise to those who request a subscription. Articles contain links to scheduled outreach information for both SERC and NERC events, along with other topics helpful to maintaining BPS reliability.	Distributed monthly and available throughout the year on the SERC website
SERC 101 The SERC 101 webpage is available under Outreach. It features links to basic compliance information on the FERC, NERC, and SERC websites in one convenient location. A sample of the links includes information such as the Energy Policy Act (EPAct) of 2005 and the FERC Reliability Primer on the FERC site; the ROP and Reliability Standards information on the NERC site; and Assistance, Registration and Certification, and Compliance Enforcement information on the SERC site.	Available throughout the year
SERC Compliance Portal SERC registered entities submit Self-Certifications, Self-Reports, Mitigation Plans, and Data Submittals via the SERC Portal. Feedback from targeted surveys allows SERC to incorporate enhancements based on the needs of the users, and outreach events include training on upgrades and enhancements.	Available throughout the year
Dedicated Email In-Boxes Appropriate SERC staff monitor dedicated email in-boxes established for questions from stakeholders. The Contact Us link is accessible from any page of the SERC website, and features a list of topics along with the email address link to submit questions. A sampling of the topics includes compliance issues and situational awareness/events analysis. SERC responds to emails within 24 hours. When a response will take longer than 24 hours, SERC sends an acknowledgement email to ensure the sender that SERC has received the inquiry and someone will respond as soon as possible.	Monitored throughout the year

Appendix A5: Texas Reliability Entity (Texas RE) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the Texas RE as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

In 2018, Texas RE continued to evaluate the risk-based compliance monitoring implementation efforts and continued to facilitate improvements in effectiveness and efficiency. Every registered entity selected for an engagement in 2019 will undergo an Inherent Risk Assessment (IRA) representing the current risks to reliability posed by the registered entity to focus efforts on reliability risks for the registered entity and provide focus for Texas RE staff.

Texas RE will follow the ROP requirements for notifying candidates once a CMEP Tool, as developed within the approved Framework, is determined. The ROP requires that a Reliability Coordinator (RC), Balancing Authority (BA), or a Transmission Operator (TOP) will have an audit performed "at least once every three years." Those RCs, BAs, or TOPs meeting the "at least once every three years" designation will be listed in the Annual Audit Plan.

During the implementation year, Texas RE may update the Implementation Plan. Updates can include, but are not limited to: changes to the compliance monitoring processes, changes to regional processes, updates resulting from a major event, FERC Order(s), or other matters deemed appropriate by Texas RE or NERC. When updates occur, Texas RE will submit updates to NERC, which will review and act on any proposed changes. NERC is responsible for updating the ERO Enterprise CMEP Implementation Plan (CMEP IP) to reflect any Texas RE changes. NERC will post the updated plan to the NERC website and issue compliance communications. Texas RE will evaluate Operations and Planning (O&P) Requirements and Critical Infrastructure Protection (CIP) Requirements concurrently during engagements rather than approaching Requirements relative to the risks separately.

As part of risk-based CMEP implementation, Texas RE further enhanced the in-house IRA tool. The IRA tool will continue to undergo improvements based on the ERO Enterprise Guide for Compliance Monitoring, NERC oversight feedback, lessons learned, registered entity feedback, and the straightforward common sense approach of the Texas RE Risk group. During 2019, every registered entity engagement will start with an IRA, the results of which will be used to develop appropriate oversight and will be provided to the registered entity as an IRA Summary Report. Additionally, as the ERO Enterprise matures the process to develop more comprehensive Compliance Oversight Plans (COP) for registered entities, Texas RE will enhance its internal process for COP and provide outreach for registered entities.

Other Regional Key Initiatives & Activities

Texas RE will support NERC management in preparations for the implementation of the Supply Chain Standards[37] (CIP-005-6, CIP-010-3, and CIP-013-1). Texas RE will continue its collaborative effort between NERC, the Regional Entities, and registered entities to identify and implement changes that enhance the effectiveness of the CMEP. Texas RE will focus on ensuring the risks to the Interconnection are evaluated effectively and efficiently to support reliable operations.

Regional Risk Assessment Process and Results

The regional risk assessment process is a facet of Texas RE's efforts to adequately plan effective compliance monitoring in the ERCOT Interconnection. The risk assessment process is used to determine compliance monitoring objectives, compliance monitoring scope, and an initial entity oversight plan. Sub-processes of the risk assessment process include: determining risk elements (Interconnection risks), conducting an IRA (entity-level Bulk Electric

[37] NERC Board of Trustees Resolution - Supply Chain Standard as reviewed during the August 10, 2017 Board of Trustees meeting

System (BES) risks), completing a voluntary Internal Controls Evaluation (ICE) (entity-level risk mitigation), and developing a COP (monitoring scope for an entity or class of entities). The work product of the BES risk assessment process is the determination of individual engagement type, individual engagement scope, and development of a COP for an entity or class of entities.

The process of evaluating BES risk fully satisfies the concerns of significance and compliance monitoring risk. The process work product is a BES risk-targeted scope. The risk assessment process may be used to perform both comprehensive and highly targeted compliance monitoring activities. There is no requirement to address all BES risks in a single, comprehensive checklist-style compliance monitoring activity. Monitoring of individual risks via multiple engagements may be used as an alternate and more effective approach. The premise of the reliability assessment process is that the amount of scrutiny a registered entity receives in terms of compliance monitoring will be directly commensurate with the risk it poses to the reliability of the BES. For entities that pose a limited reliability risk, minimum compliance monitoring activities may suffice. For entities that pose a significant risk to reliability, it will be necessary for those entities to undergo effective compliance monitoring such as additional focused spot checks, a greater number of self-certifications, or broader and deeper audits of greater frequency.

To assist Texas RE in determining how much risk an entity poses to reliability, Texas RE uses dedicated staff to review risk within the Interconnection. The staff relies heavily on feedback from other groups within Texas RE such as Registration, Enforcement, Reliability Services, and Compliance to achieve an understanding of the risks encountered or emerging within the Interconnection. Additionally, Texas RE reviews externally created reports, both locally and nationally, and discussions focusing on reliability risks. The ERO Enterprise Guide for Compliance Monitoring (Guide)[38] provides basic guidance for determining risks that may require some level of compliance monitoring. Texas RE has utilized the risk element development process outlined in the Guide to develop an internal process that enhances focus on risks within the Interconnection by involving local subject matter experts.

For example, the Texas RE Reliability Services department creates an annual Assessment of Reliability Performance Report[39]. Some aspects within the report correlate to the risk elements determined using the Guide but others are corollaries, such as inertia and resource adequacy both localized issues due to changes in the resource mix requiring localized focus. This localized focus could equate to a deeper review of previous ERO IP risk elements such as, in this case, “Monitoring and Situational Awareness” and “Extreme Physical Events.” Effects of the declining system inertia may be evident in system event responses both in terms of human responses and physical characteristics such as Primary Frequency Response. Primary Frequency Response has been identified as a risk to the Interconnection. There is a local working group, the “Performance, Disturbance, Compliance Working Group (PDCWG)” that is responsible for reviewing, analyzing, and evaluating the frequency control performance of the Interconnection. The PDCWG analyzes generation loss events of 450 MW or greater and system event frequency deviations of +/- 0.1 Hz or greater. As such, Standards related to frequency response, and critical operational aspects of a reliable grid could be utilized in compliance monitoring efforts for 2019.

Establishing knowledge of a new entity is important in determining risk associated with that entity. Texas RE carefully tracks new entities and will use registration input(s) as a way to help delineate the need to engage in compliance monitoring. The ERO IP states that monitoring of a particular registered entity may include more, fewer, or different Reliability Standards than those outlined in the ERO and Regional Entity CMEP IPs. Although the ERO IP and Regional IP identify NERC Standards and Requirements for consideration for focused compliance monitoring, the ERO recognizes that the Framework and risk-based processes will develop a more comprehensive, but still focused list of NERC Reliability Standards and Requirements specific to the risk a registered entity poses to the BES. Therefore, a particular area of focus under a risk element does not imply that: (1) the identified NERC Standard(s) fully addresses

[38] ERO Enterprise Guide for Compliance Monitoring, October 2016
[39] 2017 Assessment of Reliability Performance of the Texas RE Region, April 2018

the particular risk associated with the risk element; (2) the NERC Standard(s) is only related to that specific risk element; or (3) all Requirements of a NERC Standard apply to that risk element equally.

Texas RE will utilize determined risks to facilitate engagements with registered entities in such a way that prioritizes the evaluation of compliance for the determined risks. Texas RE will apply the appropriate risk element or risk elements and other clearly articulated factors to the appropriate registered entity to maintain a focus on reliability. Each registered entity is subject to an evaluation of compliance for all Standards, regardless of inclusion within the Areas of Focus described within the ERO IP. That fact allows, as indicated by the ERO IP, for a more in-depth review of additional requirements associated with risks beyond those shown within the ERO IP. As each entity represents a unique set of inherent risks to the Interconnection, Texas RE is committed to having each registered entity understand how the risks were developed for compliance monitoring engagements. Additional risk elements may be added as needed throughout the year.

Regional Risk Elements and Areas of Focus

For the purpose of the Texas RE Implementation Plan, areas of focus highlight ERO Enterprise and region-specific risks that merit increased focus for compliance monitoring that may become a part of an individual registered entity's COP. The areas of focus do not represent the exclusive list of important or relevant Reliability Standards or Requirements, nor the entirety of the risks that may affect the reliability of the BPS. Rather, Texas RE considers the risk elements and areas of focus to help prioritize compliance monitoring efforts.

When developing entity-specific COPs, Texas RE will consider local risks and specific circumstances associated with individual registered entities. The COP also takes into account the unique compliance history of each registered entity, along with both the timing of and the results of any prior compliance monitoring, when determining which compliance monitoring tools will be used for future monitoring. The COP focuses on a complete picture of reliability risks associated with a registered entity along with various mitigating factors, such as past performance or the presence of effective internal controls, to determine the appropriate compliance monitoring tool for registered entities.

As a result, a particular registered entity's scope of monitoring may include more, fewer, or different Reliability Standards than those outlined in the CMEP IP. The determination of the appropriate CMEP tools may be adjusted as needed within a given implementation year. Additionally, NERC and the REs have the authority to monitor compliance with all applicable Reliability Standards whether they are identified as areas of focus to be considered for compliance oversight in the annual IP or are included in a COP for a registered entity.

Table A6.1 contains the regional risk elements for focus during 2019. The table also contains areas of focus to identified risks that may be considered in the development of a registered entity's COP. The three risk elements, determined through the Regional Risk Element process for 2019, are Resource Adequacy, Facility Ratings, and Data Integrity. Effective management of these risks are particularly important largely due to the nature of the Interconnection.

Table A5.1 Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Resource Adequacy	This risk element is focused on ensuring the available resources are appropriately managing frequency control and voltage control aspects of this Interconnection. The need to actively monitor reactive resources within the system to ensure that voltage variations are minimized, preventing outages and damage to BES equipment, has been recognized as a risk. While voltage is generally a localized concern, there have been changes in the ERCOT Interconnection that have facilitated the use of more dynamic and static reactive devices in more areas. Additionally, there are several load pockets where the management of reactive sources plays a significant role in ensuring reliability. While frequency control metrics are being maintained at a high level, the shift in resource mix warrants appropriate compliance monitoring. The impact on system inertia is a risk as the resource mix continues to evolve. The load growth coupled with record breaking wind penetration puts an emphasis on managing the frequency before, during, and after events. Resources should have appropriate controls in place to support reliable operations as the resource mix within this Interconnection continues to change. All entities should have proper plans in place to act, and react, to operational risks.	BAL-001-TRE-1 R9, R10; VAR-002-4.1 R2; PRC-024-2 R2

Table A5.1 Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Facility Ratings	This risk element is focused on identifying potential gaps in the development and application of Facility Rating Methodologies for registered entities. Through the use of CMEP activities, Texas RE continues to identify multiple instances in the Interconnection in which registered entities have potential gaps and discrepancies in the development, application, consistency, implementation, and review of Facility Ratings. Failure of a registered entity to properly develop and apply Facility Ratings in a timely manner can result in potential high risk to the BES. Those risks include improper identification and mitigation of SOLs and IROLs and damage to BES equipment and facilities. Vegetation management has a direct relationship to Facility Ratings and will remain as an area of focus based on recent Interconnection observations. The standards selected are directly tied to developing and implementing Facility Ratings for a registered entity's BES Facilities.	FAC-003-4 R1, R2, R6, R7; FAC-008-3 R1, R2, R3, R6, R7, R8; MOD-025-2 R1, R2, R3; PRC-023-4 R1, R6
Data Integrity	This risk element focuses on availability of data, the quality of the data, and processes used in specifying, assessing, communicating, and addressing data needs by those entities responsible for operating the Interconnection. From 2013-2017, there were a total of 24 loss of EMS/SCADA events reported in the Interconnection. Loss of EMS or SCADA events will continue to be of concern due to their impact on visibility and situational awareness for System Operators. Data quality and data integrity represent a significant potential risk if not managed well. Accuracy and availability of telemetry is a key issue for situational awareness for System Operators as well as the proper functioning and application of tools used to reliably operate the Interconnection. Monitoring how data is specified, developed, utilized, and then analyzed by those entities reliably operating the Interconnection.	IRO-010-2 R3; TOP-003-3 R1, R3, R5; IRO-018-1(i) R1, R2, R3; TOP-010-1(i) R1, R3, R4

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2019 Compliance Audit Plan that lists all scheduled audits for registered entities during the 2019 implementation year. The 2019 Compliance Audit Plan, located on the Texas RE website here, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

Throughout the implementation year, Texas RE may make updates to the 2019 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

Texas RE conducts spot checks based on a registered entity's COP, or at Texas RE's discretion at any time. Texas RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. Texas RE will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

Texas RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. Texas RE will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the NERC ROP.

Texas RE does not have any planned Interconnection-wide Self-Certifications in 2019. Texas RE will utilize Self-Certifications on individual entities as a result of the individual registered entity's IRA and COP.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. Texas RE follows the ERO Enterprise 2019 Periodic Data Submittal posted here.

Compliance Outreach

Table A5.2 Compliance Outreach Activities

Outreach Activity	Anticipated Date
Spring Compliance Workshop	Spring 2019
Compliance 101	Summer 2019
Fall Compliance Workshop	Fall 2019
Talk with Texas RE	Projected Monthly (subject to change)
Texas *RE*view Newsletter	Projected Monthly

Appendix A6: Western Electricity Coordinating Council (WECC) 2019 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the WECC as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

In 2019, WECC will continue to conduct its monitoring and enforcement activities in accordance with the Board-endorsed Regulatory Philosophy, the key tenets of which are: be an informed regulator, find top risks to reliability, exercise discretion responsibly, and enforce fairly. WECC monitors FERC-approved NERC Reliability Standards for registered owners, operators, and users of the Bulk Power System (BPS), through a variety of risk-based activities, including Self-Certifications, Audits, Spot-Checks, and internal control evaluations, as directed in the NERC ROP, and the 2019 ERO Enterprise and WECC CMEP IPs. WECC compliance and monitoring staff will continue to assess, dedicate, and deploy required resources in support of the ERO Enterprise-level initiatives and activities. Based on these activities, WECC will use its discretion to modify its CMEP IP throughout the year to address reliability and security issues as they arise. The 2019 ERO Enterprise CMEP IP names several risk elements and areas of focus that provide a starting point for WECC's Inherent Risk Assessment (IRA), Compliance Oversight Plan (COP) development, and monitoring activities. Since reliability and security risks are not the same for each registered entity, WECC will add, subtract, or modify the Standards and Requirements identified in a registered entity's COP as necessary, based on considerations of the registered entity's IRAs and historical performance.

Other Regional Key Initiatives & Activities

In its effort to continually improve the content of our outreach initiatives and activities, WECC has made changes to its outreach program to align with its mission: To effectively and efficiently reduce risks to the reliability and security of the Western Interconnection's Bulk Power System. WECC is committed to providing targeted, in-depth, risk-based outreach; along with training activities that focus on addressing and mitigating risks. Participants will get timely and engaging content, take part in interactive presentations to ease knowledge transfer, and network with peers to share effective methods for compliance with FERC-approved NERC Reliability Standards.

Regional Risk Assessment Process and Results

WECC's Regional Risk Assessment considers previously identified and emerging risks that pose the greatest potential impact to the reliability of the Western Interconnection. The assessment includes a review of data including the following:

- ERO Enterprise CMEP IP risks
- Data and results of IRAs and COPs
- Data and results of residual risk following controls evaluations
- Regional noncompliance and corresponding cause trends
- Situational awareness, event, and misoperations reports
- The State of the Interconnection Report for the Western Interconnection
- NERC Alerts
- FERC Orders
- Electricity Information Sharing and Analysis Center (E-ISAC) Data
- Professional judgment of WECC Entity Oversight personnel

To address these risks, WECC identifies FERC-approved NERC Reliability Standards and Requirements which are used to supplement the ERO risk elements as necessary for the Western Interconnection. Throughout the year, WECC will continue to monitor FERC and NERC activities, system events, emerging threats, and WECC-identified risks; and will update its assessment when and where necessary.

Regional Risk Elements and Areas of Focus

The table below contains the regional risk elements, and expended ERO risk elements, for focus during the 2019 based on the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of a registered entity's compliance oversight plan (COP).

Table A6.1: Regional Risk Elements

Regional Risk Element	Justification	Associated Standard and Requirement(s)
Gaps in Program Execution	Categorization of BES Cyber Systems (BCS) informs an entity of the applicability of all other Critical Infrastructure Protection (CIP) standards. WECC has noticed that there have been instances of missing categorization of the BCS, or BES Cyber Assets (BCA) within the BCS. This categorization is critical to the success of a cyber security program and remains a major area of focus. WECC will be monitoring the Standard and Requirements associated with BCS categorization.	CIP-002-5.1a R1
	WECC has found another gap in program execution related to operating personnel training under COM-002-4, which adds increased risk in the Western Interconnection.	COM-002-4 R1, R2
Changing Reliability Coordinator	The Western Interconnection has one Reliability Coordinator (RC). In 2019, three entities are expected to register as RCs and the existing RC will be winding down its operations. WECC will consider more monitoring for Standards associated with RCs' collaboration and situational awareness, especially during transition periods. WECC will also monitor Standards about Balancing Authority (BA)/Transmission Operator (TOP) coordination with new RC(s).	FAC-011-3 R1, R3 FAC-014-2 R1 IRO-006-WECC-2 R1 IRO-008-2 R5 IRO-009-2 R1 IRO-014-3 R1, R3

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2019 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the Annual Audit Plan that lists all planned audits for registered entities during the 2019 implementation year. The Annual Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The Annual Audit Plan for this RE is found here, on the regional website. Throughout the implementation year, the RE may make updates to the Annual Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts spot checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the NERC ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the NERC ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the NERC ROP. The self-certification schedule is located on WECC's website.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the ERO Enterprise 2019 Periodic Data Submittal schedule, posted on WECC's website.

Compliance Outreach

Table A6.2 Compliance Outreach Activities

Outreach Activity	Anticipated Date
WECC Open Webinar	Third Thursday of most months
Reliability and Security Workshop	April 9–11, 2019 Anaheim, CA October 22–24, 2019 Las Vegas, NV

Appendix B: Compliance Assessment Report

Compliance Assessment Process for Events and Disturbances

The ERO Enterprise encourages registered entities to perform an initial compliance assessment (CA) concurrent with the registered entity's event review and analysis. When completing a CA, the registered entity should follow these steps:

1. Refer to the causes and contributing factors of the event as determined by the registered entity's events analysis process.
2. Identify all applicable NERC Reliability Standards and Requirements potentially implicated by the causes and contributing factors of the event.
3. After reviewing the facts and circumstances of the event, develop conclusions applicable to relevant NERC Reliability Standards and Requirements (see Step 2 above).
4. Self-report any findings of noncompliance to the RE per the CMEP procedures.
5. Provide a copy of the CA report to the RE compliance organization. The CA should be accompanied by the separate Event Analysis Report, Brief Report, or similar document that provides sufficient information for the RE to understand the event.

Sample Compliance Assessment Report Template

Event Cause or Contributing Factor	Applicable Reliability Standards and Requirements	Details of CA Efforts	Findings
Cause–Example 1	AAA-000-0 R 1	1. Identify the process used to assess compliance with this Requirement 2. Identify any evidence that demonstrates compliance 3. Identify any evidence that suggests noncompliance	Finding conclusion
Equipment failure of a high-side transformer—cleared along with two transmission lines	TOP-002-2a R6. Each BA and TOP shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 contingency planning) in accordance with NERC, Regional Reliability Organization, sub-regional and local reliability Requirements	Established transfer limits were followed such that the event did not result in instability. The limit for operating across this internal interface is established in the RC. "XYZ Interface All Lines In Stability Guide" (document provided)	No findings of noncompliance