NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program

September 5, 2014

RELIABILITY | ACCOUNTABILITY



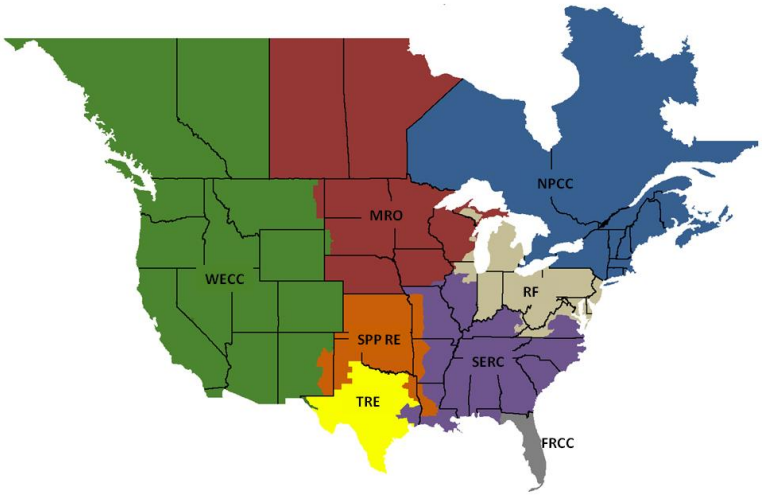

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

In November 2012, the ERO Enterprise launched a multi-year effort, known as the Reliability Assurance Initiative (RAI), to identify and implement changes to enhance the effectiveness of the Compliance Monitoring and Enforcement Program (CMEP). Based on the work conducted through RAI, NERC has implemented a more robust risk-based program for compliance monitoring and enforcement of Reliability Standards. Under this program, focused compliance monitoring, appropriate deterrence through enforcement, and a feedback loop to improve Reliability Standards result in reasonable assurance of reliability.

As explained in the ERO Enterprise white paper, *Incorporating Risk Concepts into the Implementation of Compliance and Enforcement*, it is not practical, effective, or sustainable for the ERO Enterprise to monitor all compliance issues to the same degree or to treat all noncompliance in the same manner. 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. It also encourages registered entities to enhance internal controls, including those focused on the self-identification of noncompliance.

The ERO Enterprise has tested a number of concepts, processes and programs over the course of 2013 and 2014 for implementation in 2015. By the end of September 2014, NERC will have published guides and program documents related to all of the new and expanded processes and programs to allow for implementation in 2015.

Full implementation of these processes and programs began with the publication of the 2015 ERO CMEP Implementation Plan, as discussed below. Implementation also is being accompanied by training and outreach efforts directed at ERO Enterprise staff and industry stakeholders. The expansion of these processes throughout 2015 and beyond is being closely monitored to ensure a successful implementation.

The processes and programs discussed herein are based on long-standing monitoring and enforcement concepts and principles that are widely used in most regulated industries and certified quality management programs. The program refinements build upon existing practices and bring the ERO Enterprise monitoring and enforcement activities in line with standard regulatory practice. Common program guides for the new and expanded processes and programs will increase transparency and help ensure consistency of application.

As a result of the work conducted as part of RAI, which will end as a separate initiative with the publication of the guides and program documents noted above, the ERO Enterprise is now transitioning to the implementation of risk-based reliability assurance methods with the goal of full implementation of a mature compliance monitoring and enforcement program.[1]

[1] The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) is Appendix 4C to the NERC Rules of Procedure. Sections 4.0 and 5.0, in particular, are relevant to and provide the bases for the risk-based reliability assurance methods described herein.

Compliance Monitoring and Oversight

The RAI's transformation for compliance monitoring involves the use of the oversight plan framework (Framework) depicted in Figure 1 below. The Framework focuses on identifying, prioritizing and addressing risks to the BPS, which enable each Compliance Enforcement Authority (CEA) to focus resources where they are most needed and likely to be the most effective. Regional Entities are responsible for tailoring their approach to compliance monitoring (i.e., monitoring tools and the frequency and depth of monitoring engagements) in accordance with the processes described herein.

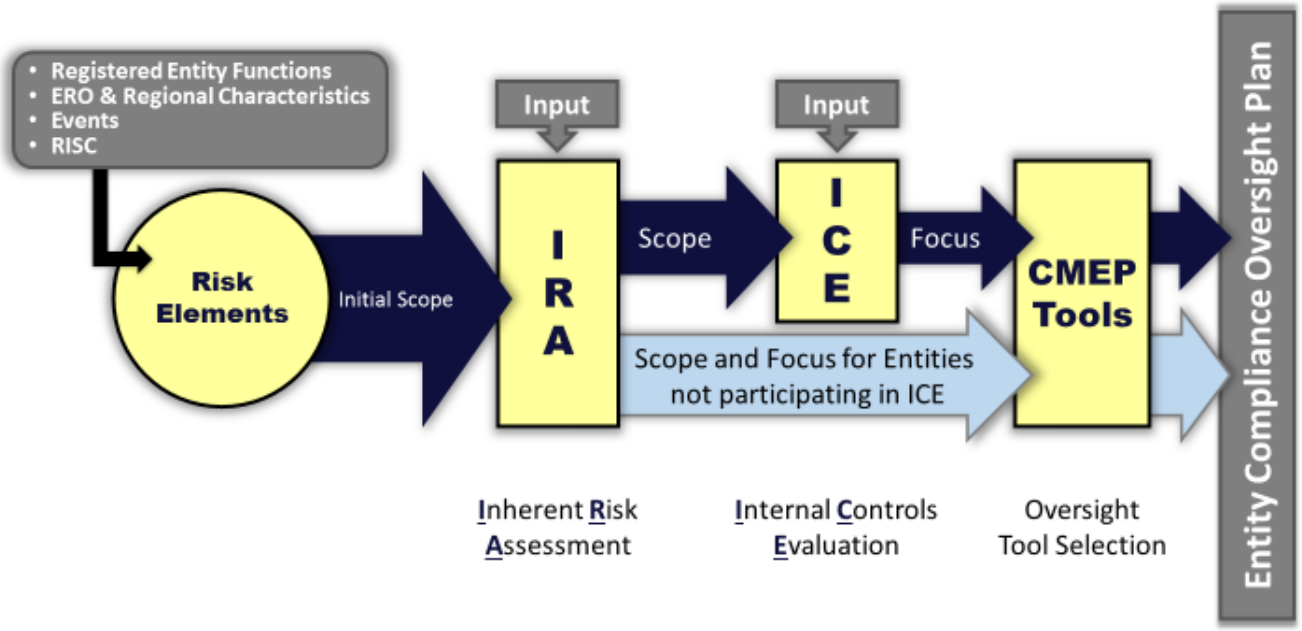


Figure 1 – Risk Based Compliance Oversight Framework

The first step of the Framework is the identification and prioritization of continent-wide risks. These are identified and prioritized based, among other things, on the work done by NERC staff and the Reliability Issues Steering Committee (RISC), initiatives such as the Standards Independent Experts Review Project, and the risks identified in the ERO Enterprise Strategic Plan, which incorporate the input of industry stakeholders, Regional Entities, and Applicable Governmental Authorities. Risks are identified and prioritized based on the potential impact to the reliability of the BPS and the likelihood that such an impact might be realized. Risks may be categorized as operational risks and planning risks, as well as threats to cyber systems or physical security. While risk identification occurs on an annual basis, risks are dynamic. Accordingly, periodic reviews and updates may be necessary and appropriate to address increased or emerging risks and to reflect mitigated risks.

Through the review of the ERO Enterprise-wide risks, the ERO develops an annual compilation of **Risk Elements**, which are reflected in the **ERO Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP)**. The ERO CMEP IP serves as guidance to Regional Entities in the preparation of their **Regional Entity Implementation Plans (Regional Entity IP)**. Any needed updates will be reflected in the ERO CMEP IP on a dynamic basis. The Regional Entity IP is subject to review and approval by NERC as noted in the Rules of Procedure.

Reliability Standards are in place to help ensure the reliable operation of the BPS. That is, the elements of the BPS should be operated so that instability, uncontrolled separation, and cascading failures of the system will not occur.

Through the identification of Risk Elements, the ERO Enterprise is able to map a preliminary list of applicable Reliability Standards and responsible registration functional categories to the top reliability risks identified. This preliminary list, which is reflected in the ERO CMEP IP, replaces the Actively Monitored List used in prior years. However, the risks and associated Reliability Standards identified through this process do not constitute the entirety of the risks that may affect the BPS. Regional Entities are expected to consider local risks and specific circumstances associated with individual registered entities within their footprint in developing their compliance oversight plans. As a result, the scope of monitoring of a particular registered entity may include more, fewer, or different Reliability Standards than those outlined in the ERO CMEP IP.

After risk elements are identified and prioritized, the **Inherent Risk Assessment (IRA)** enables the CEAs to determine areas of focus by scoping oversight of specific registered entities. As a result, the IRA identifies the Reliability Standards and Requirements that should be monitored.

The IRA Guide describes the process used to assess inherent risk of registered entities by CEAs. The IRA is a review of risks posed by an individual registered entity to the reliability of the BPS. An IRA considers factors such as assets, systems, geography, interconnectivity, functions performed, prior compliance history, and culture of compliance, among others. The IRA will be performed on a periodic basis. The frequency of conducting an IRA may vary based on occurrence of significant changes to reliability risks or emergence of new reliability risks.

For monitoring activities performed in 2015, Regional Entities are in various stages of conducting IRAs for registered entities within their footprint. During 2015 and beyond, Regional Entities will continue to expand the IRA process to entities in their footprints based on risk and compliance monitoring schedules.

In developing more specific monitoring plans for registered entities in their footprints, the Regional Entities also take into account any information obtained through the processes outlined in the **Internal Control Evaluation (ICE)** Guide. The ICE Guide is being developed by the ERO Enterprise in collaboration with a focus group of registered entities. The guide describes the process for identifying key controls, testing their effectiveness, and documenting the conclusions of the internal controls evaluation. Regional Entities will select registered entities for the ICE process based on the risk posed by particular entities and compliance monitoring schedules.

The ICE allows a further refinement of the compliance oversight plan. Registered entities have an opportunity to: (i) provide, on a voluntary basis, information to their respective Regional Entity about their internal controls that address the risks applicable to the entity and for identifying, assessing and correcting noncompliance with Reliability Standards; and (ii) demonstrate the effectiveness of such controls. As a result of the ICE, the Regional Entity may further focus the compliance assurance activities for a given entity. For example, the depth of any particular area of review may be modified.[2] Registered entities may elect not to participate in an ICE. In that case, the CEA would use the results of the IRA to determine the appropriate compliance oversight strategy, including focus and tools within the scope determined through the IRA.

Ultimately, the Regional Entity will determine the type and frequency of the **compliance monitoring tools** (i.e., off-site or on-site audits, spot checks or self-certifications)[3] that are warranted for a particular registered entity based on reliability risks. The determination of the appropriate CMEP tools will be adjusted, as needed, within a given implementation year.

[2] For example, if a Registered Entity demonstrates effective internal controls for a given Reliability Standard during the ICE, the Regional Entity may determine that it does not need to audit the Registered Entity's compliance with that Reliability Standard as frequently or may select a different monitoring tool.

[3] CMEP §3.0.

With the exception of those entities required to be audited at a three-year interval per the NERC Rules of Procedure, more resource-intensive compliance monitoring activities, particularly compliance audits, will generally be used for those functions or entities within a specific Regional Entity that can have the most significant impact on reliability of the BPS, as determined through the IRA. For functional roles or entities that have a lesser impact on reliability to the BPS, compliance monitoring approaches may be tailored accordingly. Use of spot checks and/or self-certifications may be appropriate tools in such instances. Audits and spot checks may include on-site and off-site reviews as warranted, in accordance with the NERC Rules of Procedure.

Enforcement

The ERO Enterprise recognizes that enhancement of internal controls, self-identification of noncompliance, and corrective action are the fundamental intended results of the CMEP for optimal reliability assurance.

Consequently, not all instances of noncompliance require the same type of processing and documentation and that there is a need to streamline processes for resolving minimal and moderate risk issues. This is necessary to allow the ERO Enterprise as well as industry to allocate resources to the issues posing a higher level of risk to reliability. This approach also encourages the enhancement of internal controls and self-identification of noncompliance by registered entities (as these practices are appropriately valued and rewarded).

As a result, over the past several years, the ERO Enterprise has been migrating to a risk-based strategy of assessing and processing noncompliance. The Find, Fix, Track and Report (FFT) process, introduced in 2011, has successfully been used to resolve over 2,000 instances of noncompliance with the Reliability Standards, most of which posed a minimal risk to the reliability of the BPS. Since June 2013, the FFT process has also been used to resolve noncompliance posing a moderate risk to the BPS.

Based on the experience with a streamlined process and a reduced record, since 2013, NERC and the Regional Entities have exercised discretion when deciding whether to initiate an enforcement action for certain noncompliance posing a minimal risk to the reliability of the BPS. Issues resolved outside of an enforcement action are referred to as **compliance exceptions**. The resolution of these issues outside of an enforcement action has not eliminated oversight or visibility over the issues. Rather, these issues are provided for review by NERC and FERC. The process, however, has allowed NERC and the Regional Entities to work with registered entities to identify and mitigate minimal risk issues promptly and more efficiently. Beginning in January 2015, all minimal risk noncompliance will be eligible for resolution as a compliance exception. While compliance exceptions will effectively supersede FFT as the process for resolving minimal risk noncompliance in the future, for the time being, the FFT process remains relevant, particularly as it relates to moderate risk issues.

In addition, beginning in October 2013, NERC and the Regional Entities began to allow select registered entities with demonstrated effective management practices to self-identify, assess, and mitigate instances of noncompliance to **self-log** minimal risk noncompliance that would otherwise be individually self-reported. Properly logged items are entitled to the presumption of being resolved as compliance exceptions unless there are additional risk factors involved. This is consistent with the notion that noncompliance that is self-identified through internal controls, corrected through a strong compliance culture, and documented by the entity, should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the BPS.

The self-logging program also encourages the development and communication of management practices and rewards registered entities for demonstrated, effective controls in place to detect and correct issues as they arise. Registered entities currently participating in the program report that they see a significant potential benefit, particularly associated with the presumption that logged items will be resolved as compliance exceptions absent additional risk factors or other issues.

Oversight

Oversight is key to the long-term success of the compliance monitoring and enforcement program. Oversight ensures consistency in identification of risks, and evaluation of processes, procedures, and internal controls, as well as the assessment of risks associated with noncompliance and mitigation.

NERC oversight focuses on the review of the Regional Entity's processes and implementation of program parameters and guidelines. An example is NERC's oversight of the FFT program, which is based on an annual review of the Regional Entity's procedures and a review of a sample set of FFTs from each Regional Entity. This review is prospective in nature, in that it is not intended to reopen closed matters, but rather to identify implementation issues and opportunities for improvement. Findings and recommendations are discussed with Regional Entities and FERC, and a summary of the results is presented to the public on an annual basis.

As part of its oversight, NERC also will conduct training on, and may observe, Regional Entity compliance assurance activities.

Feedback to Standards

An ERO Enterprise feedback loop from compliance assurance and enforcement activities will help inform future priorities and projects in the standards development process as well as other ERO Enterprise processes. This feedback loop can operate both with respect to areas where there may be gaps as well as areas in which specific Requirements may be suitable for retirement. It is expected that this feedback loop will continue to mature with more experience in the implementation of risk-based compliance monitoring and enforcement.