NPCC Entity Risk Assessment
Program Guide for Risk-based Compliance Monitoring and Enforcement Program

ERA-01
Rev. 1

Process Owner: NPCC Manager, Entity Risk Assessment

Effective Date: 03/02/2015
Table of Contents

1. Introduction ......................................................................................................................2
2. Purpose ...........................................................................................................................2
3. Roles and Responsibilities ...............................................................................................4
4. Procedure ........................................................................................................................5
   4.1 Risk Elements ............................................................................................................5
   4.2 Inherent Risk Assessment (IRA) ................................................................................5
   4.3 Internal Controls Evaluation (ICE) ..............................................................................8
   4.4 Entity Compliance Oversight Plan ............................................................................ 10
5. Glossary of Terms ......................................................................................................... 11
6. References .................................................................................................................... 12
7. Summary of Changes .................................................................................................... 13
8. Periodic Review Date .................................................................................................... 13

Review and Re-Approval Requirements

This document will be reviewed every two years from the effective date, or as appropriate, for possible revision. The existing or revised document will be posted to the NPCC ERA website for NPCC registered entity reference.
1. Introduction

The NERC Risk-based Compliance Monitoring and Enforcement Program (Risk-based CMEP) was developed through the Reliability Assurance Initiative (RAI).

Risk-based compliance monitoring is intended to establish the type and frequency of Regional Entity compliance oversight based on the specific reliability risks posed by a registered entity.

It is not practical, effective or sustainable to monitor all compliance issues to the same degree or treat all noncompliance in the same manner. A risk-based approach to compliance monitoring is 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 enables proper allocation of resources from both the Regional Entity and registered entity for compliance monitoring, and encourages registered entities to enhance internal controls, including those focused on the self-identification of noncompliance.

In January 2015, the Northeast Power Coordinating Council, Inc. (NPCC) Entity Risk Assessment (ERA) Group was formed within the NPCC Compliance Department to support the Risk-based Compliance Monitoring and Enforcement Program (Risk-based CMEP).

2. Purpose

The ERA Group is tasked with implementing the Risk-based Compliance Oversight Framework ("Framework"). This includes considering Risk Elements, conducting Inherent Risk Assessments (IRA) for all registered entities and Internal Controls Evaluation (ICE) for registered entities that volunteer for ICE.
The purpose of this ERA Program Document is to describe the NPCC roles and responsibilities, processes, and results, in order to ensure consistent, complete, and comprehensive implementation of the Risk-based CMEP Framework. ¹

The ERA Group will develop the procedures, forms, templates, and necessary tools to conduct and document the results of IRA and the ICE. The ERA group will revise and maintain them as necessary to incorporate efficiencies and changes in guidance from the North American Electric Reliability Corporation (NERC). The scope, monitoring method and periodicity of compliance monitoring for each registered entity will be determined based on these tools and documentation.

The ERA Group will develop outreach to industry, provide training support to the Electric Reliability Organization (ERO), and provide recommendations to related ERO or NPCC processes and documents to improve implementation and effectiveness of the Risk-based CMEP. These include, but are not limited to the annual NERC CMEP Implementation Plan, NPCC CMEP Implementation Plan, and NPCC Compliance Procedures.

¹ This document is written for the mature ERA program state. Refer to ERA Implementation Plan for schedule, scope or priorities of process implementation and deliverables.
3. Roles and Responsibilities

The ERA group is responsible for implementation, management and overall administration of the Entity Risk Assessment Program. The ERA group ensures that all NPCC ERA processes, tools, and evaluations adhere to Risk Management principles and practices and correlate to NERC guidance. These include the development of procedures, tools, and assignment of resources to conduct and document IRA and ICE, and Implementation Plan to prioritize and schedule ERA activities; scope, monitoring method and periodicity of compliance monitoring based on IRA and ICE results; creation and change management of registered entity Compliance Oversight Plans; interfacing with supporting NPCC groups and NERC; metrics demonstrating the impact of IRA and ICE in supporting Risk-based CMEP; outreach to industry; training support to the Electric Reliability Organization (ERO); review of Risk Elements/Focus Areas for inclusion in annual NERC/NPCC CMEP Implementation Plans; recommendations to improve ERO processes and tools for implementation and effectiveness of the Risk-based CMEP, including, but not limited to annual NERC CMEP Implementation Plan, NPCC CMEP Implementation Plan, and NPCC Compliance Procedures.

The ERA group shall be knowledgeable in NERC processes, procedures, and guidance related to Risk-based CMEP as well as other risk management and internal controls governance processes (e.g. Enterprise Risk Management (ERM), COSO/CoCo/CoBIT models, SAC, SAS 55/78, GAGAS/Yellow Book, CGAP).
4. Procedure

The Risk-based Framework focuses on identifying, prioritizing and addressing risks to the Bulk Electric System (BES), which enables NPCC to focus resources where they are most needed and effective. NPCC will tailor its approach to compliance monitoring (i.e., monitoring tools, frequency and depth of monitoring engagements) in accordance with guidance provided by NERC.

The Basic Steps of the Framework are:

- Identify Continent-Wide Risks
- Identify Region-Wide Risks
- Perform Inherent Risk Assessment (IRA)
- Develop Scope of Monitoring Engagement (SoME)
- Perform voluntary/complimentary Internal Controls Evaluation (ICE)
- Summarize results of IRA and ICE into registered entity’s Compliance Oversight Plan (COP)

4.1 Risk Elements

Prioritization of Continent-wide and Region-wide risks based on the potential impact to reliability is identified annually as Risk Elements. These Risk Elements are reflected in the ERO Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP), and the NPCC CMEP IP (Appendix A3 to CMEP IP).

4.1.1 The Focus Areas associated with each Risk Element are a list of NERC Reliability Standards and Requirements which require greatest attention for monitoring.

4.1.2 The ERA group considers these Focus Areas mandatory for audit engagements in the preliminary Scope of Monitoring Engagement (SoME). These Focus Areas will be coded into the preliminary SoME for each registered entity.

4.2 Inherent Risk Assessment (IRA)

The NPCC ERA group will use an IRA form to assess the registered entities’ risks in various areas. The IRA results enable NPCC to determine risk-based areas of focus based on specific information about each registered entity’s inherent risks to the BES.

4.2.1 The ERA group will document the in-house information they have available about the registered entity by filling out the information fields on the IRA form. In doing so, information gaps will be identified that challenge a complete and accurate completion of the IRA.
4.2.2 The ERA group will contact the registered entity and provide the IRA form listing the documentation that the ERA group possesses. The registered entity will be asked to provide missing and/or updated information to enable ERA group to perform the IRA as accurately as possible. The registered entity will be provided with secure method and file naming protocol to submit information to NPCC.

4.2.3 The ERA group will post the blank IRA form on the NPCC ERA webpage so that registered entities can see what information is used to perform their IRA. The registered entities may provide updated information which affects their risk profile should they choose to do so without waiting for NPCC to contact them (examples: acquisition of BES assets from another entity, or disposal of same; new owner of Special Protection System as of certain date; generator no longer a Blackstart unit, etc.).

4.2.3.1 This fosters transparency and establishes real-time communication between the registered entity and NPCC so that the information used to conduct the IRA is complete, accurate and up-to-date.

4.2.3.2 Instructions for completion of the form and secure submittal of data will be provided on the NPCC ERA webpage.

4.2.4 Results of the IRA will be summarized and inputted to the registered entity’s Compliance Oversight Plan.

4.2.5 Results of the IRA will be used by ERA group to develop the preliminary SoME.

4.2.5.1 NERC and NPCC Focus Areas are automatically included in preliminary audit scope.

4.2.5.2 These may be changed to alternate monitoring methods, or removed entirely based on results and basis of the registered entity’s IRA.

4.2.5.3 Other exclusions or inclusions of NERC requirements to monitoring are made to the preliminary SoME, with supporting rationale by ERA group.

4.2.6 If there is no Internal Controls Evaluation (ICE), then this preliminary SoME represents the FINAL SoME describing the scope and monitoring methods for Compliance engagements for the registered entity.

4.2.7 If the registered entity is scheduled for an audit engagement, the items designated for audit in the FINAL SoME will be listed as Attachment 1 in the Audit Notification Letter sent to the registered entity in accordance with NPCC Compliance Procedures CP-02 and CP-03.

4.2.8 In general, the overall IRA process follows the flow diagram shown below:
4.2.9 If a registered entity volunteers for ICE, then the ERA group will work with the entity to review its schedule, resources, and registered entity’s IRA (if any) and latest SoME, to determine when an ICE can be performed for further reduction or change in monitoring method and frequency. See Section 4.3, Internal Controls Evaluation.
4.3 Internal Controls Evaluation (ICE)

When developing specific monitoring plans for registered entities, NPCC will take into account information obtained through the processes outlined in the NERC Internal Control Evaluation (ICE) Guide. The ICE Guide describes the process for identifying key controls, testing their effectiveness and documenting the conclusions of the Internal Controls Evaluation. ICE is voluntary for registered entities and allows a further refinement of their Compliance Oversight Plans. NPCC will perform ICE based on the completed IRA and preliminary SoME for the registered entity.

4.3.1 If a registered entity volunteers for ICE, then an ICE worksheet will be developed for the registered entity based on the results of the registered entity’s IRA (if available) or all the applicable requirements for the registered entity’s registered function. NERC and NPCC Focus Areas will be flagged on the ICE worksheet. The registered entity may request a smaller subset of standards and requirements on which to provide their internal controls information for ICE.

4.3.2 The registered entity has the flexibility to choose the extent of ICE. As few, some, many or all of the registered entity’s internal controls may be offered for evaluation. The registered entity’s compliance monitoring schedule will be reviewed to determine the various “phases” of ICE.

4.3.3 An ICE Notification letter will be sent to the registered entity describing the ICE process and worksheet; composition of the NPCC ICE team; a proposed timeline for completion, review, and onsite evaluation/testing of the Internal Control Design; and how the results can benefit the registered entity.

4.3.4 If the registered entity has a scheduled audit:

4.3.4.1 The ICE package should be sent approximately 5 – 6 months prior to the engagement to give the registered entity adequate time to complete the ICE worksheet. This would also allow the NPCC ICE Team time to review and schedule an onsite ICE evaluation to determine possible reduction in audit scope, and alternate monitoring methods. The near term goal of ICE is to determine possible scope reduction so that the FINAL audit scope may be determined and documented in the Audit Notification Letter sent in accordance with NPCC CP-02 or CP-03 for Onsite and Offsite audits.

4.3.4.2 If the ICE package cannot be sent with adequate time for the registered entity to complete it in its entirety, then priority should be given to completing the worksheet for those items designated as in the preliminary audit scope. Concentration on these items may allow the ICE Team to evaluate and remove items from audit scope prior to NPCC sending the Audit Notification Letter. This would provide greatest benefit to the registered entity and is considered “phase 1” of the overall ICE.

4.3.4.3 Items on the ICE worksheet that were not part of audit scope can be completed later by the registered entity and/or evaluated later by the ICE Team for finalization of the SoME. This would be considered “phase 2” of the ICE.
4.3.5 The ICE results will be summarized, changes in scope reduction and/or monitoring methods documented, and input to the registered entity’s Compliance Oversight Plan.

4.3.6 In general, the overall ICE process follows the flow diagram shown below:

4.3.7 Registered entities may elect not to participate in an ICE. In that case, NPCC will use the results of the registered entity’s IRA and SoME to determine the appropriate compliance oversight strategy, including focus and tools within the determined scope. These results will be summarized and input to the registered entity’s Compliance Oversight Plan. See para. 4.2.6.
4.4 Entity Compliance Oversight Plan

Ultimately, NPCC will determine the type and frequency of the compliance monitoring tools (e.g., off-site or on-site audits, spot checks or guided self-certifications) that are warranted for a particular registered entity based on reliability risks.

4.4.1 The results of registered entity IRAs, and ICE will be summarized to determine the FINAL SoME, their monitoring method, and frequency or interval within a given implementation year. These summaries will be input to each registered entity’s Compliance Oversight Plan.

4.4.2 Results of the IRAs and ICEs will be made available to the individual registered entities. Registered entities may request a discussion with NPCC regarding the results of the IRAs.

4.4.3 Change management of the registered entity’s Compliance Oversight Plans is required periodically due to, but not limited to the following changes which could affect the Risk-based CMEP Framework.

4.4.3.1 Changes to a registered entity’s IRA which require refreshing of the IRA.

4.4.3.2 Changes or additions to a registered entity’s Internal Control Designs which require re-performance of ICE.

4.4.3.3 Changes to annual Risk Elements and Focus Areas by NERC and/or NPCC which require refreshing of IRA, SoME and ICE.

4.4.3.4 Retirement of standards, implementation of new standards, changes in Violation Risk Factors, new Information Attributes for IRA, new guidance for ICE. All require refreshing of applicable standards for registered functions, IRA, and ICE.

4.4.3.5 Other Risk Elements not identified by the above which may require ERA group to review for impact on existing and future IRA and ICE.
5. Glossary of Terms

5.1 Risk-based Compliance Oversight Framework

The ERO Enterprise’s Risk-based Compliance Oversight Framework (Framework) consists of processes that involve reviewing system-wide risk elements, an assessment of a registered entity’s inherent risk, and, on a voluntary basis, an evaluation of a registered entity’s internal controls prior to establishing a monitoring plan that is tailored to a particular entity or group of entities.

5.2 Risk Elements

A list of identified and prioritized continent-wide and regional risks to the reliability of the BPS resulting from the NERC Risk Elements Development Process described in the NERC Risk Elements Guide. These risks further identified the Reliability Standards and registration functional categories related to those risks and serve as Focus Areas in the annual NERC CMEP IP and Regional CMEP IP describing CMEP activities to be performed by the Regions.

5.3 Inherent Risk Assessment

Regional Entities perform an Inherent Risk Assessment (IRA) of registered entities to identify areas of focus and the level of effort needed to monitor compliance with NERC Reliability Standards for a particular registered entity. The IRA is a review of potential risks posed by an individual registered entity to the reliability of the BPS. An IRA considers risk factors such as assets, systems, geography, interconnectivity, prior compliance history, and overall unique entity composition when determining the Compliance Oversight Plan for a registered entity. The IRA will be performed on a periodic basis, with the frequency based on a variety of factors, including, but not limited to, changes to a registered entity and significant changes or emergence of new reliability risks.

5.4 Internal Controls Evaluation

An evaluation by the Regional Entity of a registered entity’s Internal Controls for addressing risks applicable to the registered entity and for identifying, assessing and correcting noncompliance with Reliability Standards. The ICE is volunteered for by the registered entity to refine the list of monitored standards for future engagements.

5.5 CMEP Tools

The CMEP Tools are the methods of monitoring (i.e., off-site or on-site audits, spot checks, or self-certifications) determined by the Regional Entities. Regional Entities will tailor compliance monitoring activities for registered entities in their footprint based on reliability risks. Reliability Coordinators, Balancing Authorities, and Transmission Operators are expected to remain on a three-year audit cycle. The determination of the appropriate CMEP tools will be adjusted, as needed, within a given implementation year.
6. References

6.2 ERO Enterprise Inherent Risk Assessment Guide, October 2014
6.3 ERO Enterprise Internal Control Evaluation Guide October 2014
6.4 2015 ERO Compliance Monitoring and Enforcement Implementation Plan, November 18, 2014
6.5 CMEP IP, Appendix A3 - Northeast Power Coordinating Council (NPCC) 2015 CMEP Implementation Plan for Entities within the U.S.
6.6 New Brunswick 2015 Annual Implementation Plan, Version 1, December 22, 2014
6.7 Memo of Understanding between the Independent Electricity System Operator (Ontario) and NERC and NPCC, November 29, 2006
6.8 Québec Reliability Standards Compliance Monitoring and Enforcement Program (QCMEP) 2015 Annual Implementation Plan, Version 1, April 1, 2015 (pending)
6.9 Memo of Understanding between Nova Scotia Power Incorporated and NPCC and NERC, May 9, 2010
7. Summary of Changes

<table>
<thead>
<tr>
<th>Revision</th>
<th>Reason for Change</th>
<th>Approved By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None – This is the original issue.</td>
<td>Ben Eng/ Manager, Entity Risk Assessment</td>
<td>03/02/15</td>
</tr>
<tr>
<td>1</td>
<td>Revised Roles and Responsibilities section and editorial changes throughout the document</td>
<td>Ben Eng/ Manager, Entity Risk Assessment</td>
<td>03/26/15</td>
</tr>
</tbody>
</table>

8. Periodic Review Date

<table>
<thead>
<tr>
<th>Changes Necessary? (If Yes, provide Revision No. and Date)</th>
<th>Performed By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(03/26/17)</td>
</tr>
</tbody>
</table>