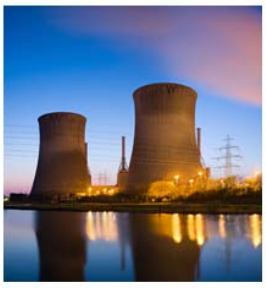
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Guide for Compliance Monitoring

October 2016

RELIABILITY | ACCOUNTABILITY

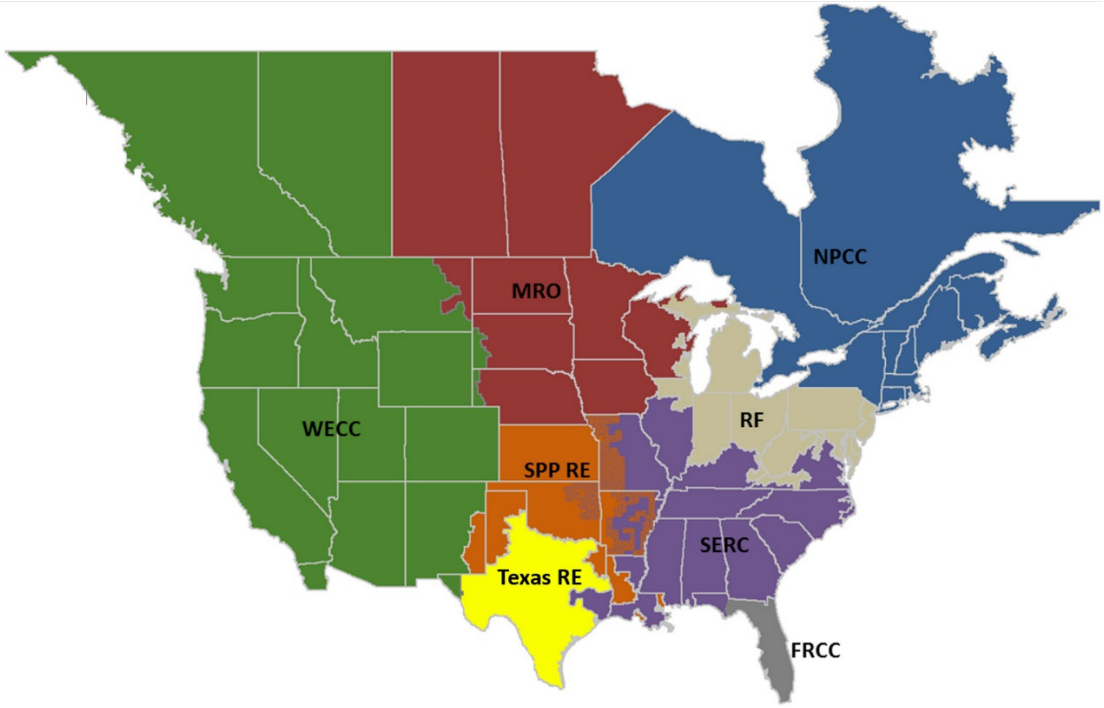
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure 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 eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight Regional Entity (RE) boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

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

Revision History

Date	Comments
July 16, 2014	Posted for Board of Trustees Policy Input
October 10, 2014	Posted for 2015 Implementation
October 2016	Revisions to address lessons learned from initial implementation. Significant Guide revisions are: • Guide enhancements to include details on overall Risk-based Compliance Monitoring Framework, including Compliance Oversight Plans (Section 3.0) and Risk Elements (Appendix C) • Revisions to the Inherent Risk Assessment process in Section 2.0. • Revisions to Appendices: ▪ Updated Appendix A, Definitions ▪ Removal of original Appendix B, Information Attributes ▪ Revisions to Risk Factors and Risk Factor criteria now found in Appendix B ▪ Inclusion of Risk Element development process in Appendix C

1.0 Introduction

This Electric Reliability Organization (ERO) Enterprise Guide for Risk-based Compliance Monitoring (Guide) describes the process Compliance Enforcement Authorities (CEAs) use to develop entity-specific Compliance Oversight Plans (COPs), and serves as a common approach for the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs) for implementing risk-based compliance monitoring under the NERC Rules of Procedure (ROP).

1.1 Processes within the Overall Risk-Based Compliance Oversight Framework

The ERO Enterprise Risk-based Compliance Monitoring Framework (Framework) focuses on identifying, prioritizing, and addressing risks to the bulk power system (BPS), which enables each CEA to focus resources where they are most needed and likely to be the most effective. CEAs are responsible for tailoring their approach to compliance monitoring (i.e., monitoring tools and the interval and depth of monitoring engagements) in accordance with the processes described herein.

Framework components described below, and in further detail within this Guide, are interdependent and interrelated. Each Framework component involves a series of ongoing activities that continuously consider NERC Reliability Standards; ERO global, regional, and entity-specific risks; and risk mitigation activities. The Framework allows for each component, like Inherent Risk Assessments (IRAs) and Internal Control Evaluation (ICE), to be dynamic and inform compliance monitoring. Having a dynamic framework allows a CEA to continuously assess and monitor a registered entity's risks to ensure reliability of the BPS, as well as compliance with the NERC Reliability Standards. The output of the Framework includes an entity-specific COP, with a refined CEA monitoring strategy of risks and associated NERC Reliability Standards. Figure 1 below illustrates the primary components within the Framework.

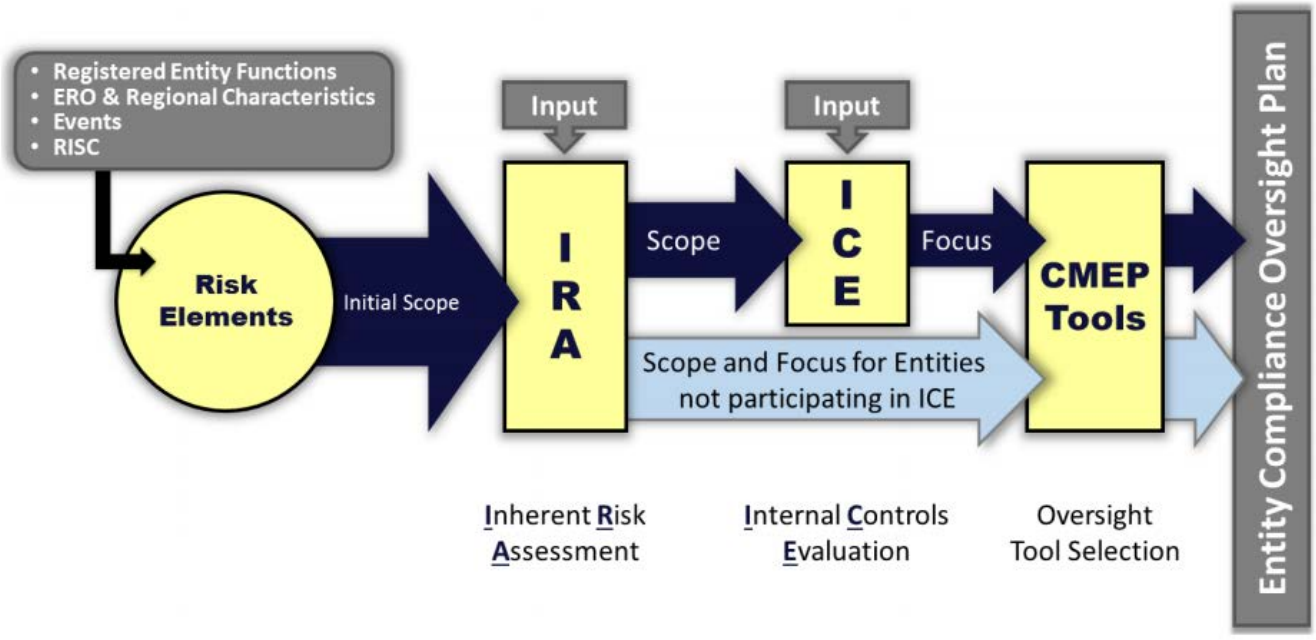


Figure 1. Risk-based Compliance Oversight Framework

1.2 Major Framework Components

As identified in figure 1, the Framework has four primary components that serve as input in developing an entity-specific COP. Risk Elements and the results of an IRA and ICE influence the COP, which is how the CEA plans to monitor a registered entity's compliance with the NERC Reliability Standards. Although the Framework seemingly depicts a linear progression and consideration of each of the major components, the Framework is a living, cyclical process, where risks and mitigating activities are considered throughout.

1.2.1 Risk Elements

Risk Elements identify and inform the ERO Enterprise of some of the more impactful risks to the BPS. While these Risk Elements highlight some of the emerging and impactful risks, other risk inputs are used by the CEA in evaluating risks, both ERO wide and region-specific.

The ERO Enterprise assesses risks to the reliability of the BPS, as well as mitigating factors that may reduce or eliminate a given reliability risk. Risk Elements represent major sources of risk that may impact the IRA, ICE, and COP. The ERO Enterprise uses different ERO industry groups, processes, and inputs to identify both ERO wide and region-specific Risk Elements. The IRA process uses these Risk Elements as a way to identify and address a registered entity's risk to the BPS. These Risk Elements can factor into how a CEA may monitor a registered entity whose inherent risk relates to a Risk Element.

Per the NERC ROP, Appendix 4C Section 3.0, NERC, with input from the REs, stakeholders and regulators, shall (at least annually) identify Risk Elements and related NERC Reliability Standards and requirements to be considered in the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP). NERC identifies these Risk Elements to categorize and prioritize continent-wide risks to the reliability of the BPS. These identified risks represent the focus for oversight activities in the upcoming year, and become inputs for developing COPs for individual registered entities.

In addition to ERO wide Risk Elements, CEAs perform regional risk assessments to identify region-specific Risk Elements. CEAs considers both lists of Risk Elements while developing registered entity COPs.

Refer to Appendix C of this Guide for the ERO Enterprise Risk Element Development Process.

1.2.2 IRA

The basis of an IRA is characteristics unique to a registered entity and its resulting inherent risks to the reliability of the BPS. The IRA process guides CEAs in identifying risks and determining areas of focus for a specific registered entity through compliance monitoring activities. Registered entities are responsible for compliance with all applicable NERC Reliability Standards, but the IRA process identifies specific NERC Reliability Standards that CEAs should consider for compliance monitoring.

The IRA process considers the NERC Reliability Standards applicable to the registered entity based on registered functions. CEAs also consider existing Coordinated Functional Registration (CFRs) or Joint Registration Organizations (JROs) and associated Standards for those CFRs and JROs.

1.2.3 ICE

An ICE enables a further refinement of a registered entity COP, and assists CEAs in identifying existing internal controls for compliance monitoring objectives - compliance with NERC Reliability Standards. An ICE refines the focus on those internal controls related to the entity-specific risks identified through the IRA allowing CEA staff to leverage the entire breadth of CMEP tools effectively, including in the determination of appropriate CMEP tools used in the COP.

1.2.4 CMEP Tools and COP

The COP is the output of the Framework and tailors compliance monitoring activities, such as Compliance Audits, Spot Checks, and Self-certifications, based on entity-specific risks and associated NERC Reliability Standards. The COP is dynamic (which will require updating from time to time) as it identifies and prioritizes risks considering risk mitigation activities, such as an entity's internal controls, and determines the interval of monitoring and depth of testing.

The COP considers Risk Elements, IRA results, and other risk inputs and regional considerations. Considerations may include, but are not limited to, the following:

- ERO Enterprise Risk Elements, identified in the Annual ERO Enterprise CMEP IP[1]
- Regional Risk Elements identified by the CEA
- Regional Risk Assessments conducted by the CEA
- NERC Reliability Issues Steering Committee (RISC)
- Event Analysis
- NERC Alerts
- Evaluations of internal controls and mitigating activities
- Additional qualitative and performance related factors (e.g. compliance history)

Appendix A contains definitions of terms used within the Guide, not defined in other ERO Enterprise documents (like the NERC ROP).

[1] Annual ERO Enterprise CMEP IPs are found here: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx

2.0 IRA Process

The IRA process includes the following steps to assess inherent risk posed by a registered entity:

1. Gather and maintain registered entity specific information and data;
2. Perform assessment to evaluate inherent risk using a registered entity's information, comparing it to the pre-determined Risk Factor criteria,[2] and
3. Identify and prioritize applicable NERC Reliability Standards for compliance monitoring activities based on the inherent risk.

The IRA process uses measureable aspects to identify a registered entity's risk characteristics related to requirements that are inherent to a registered entity's configuration and how it may affect the reliability of the BPS.

Figure 2 below provides an overview of how the IRA process supports overall development of registered entity COPs. The details of each process step are described below.

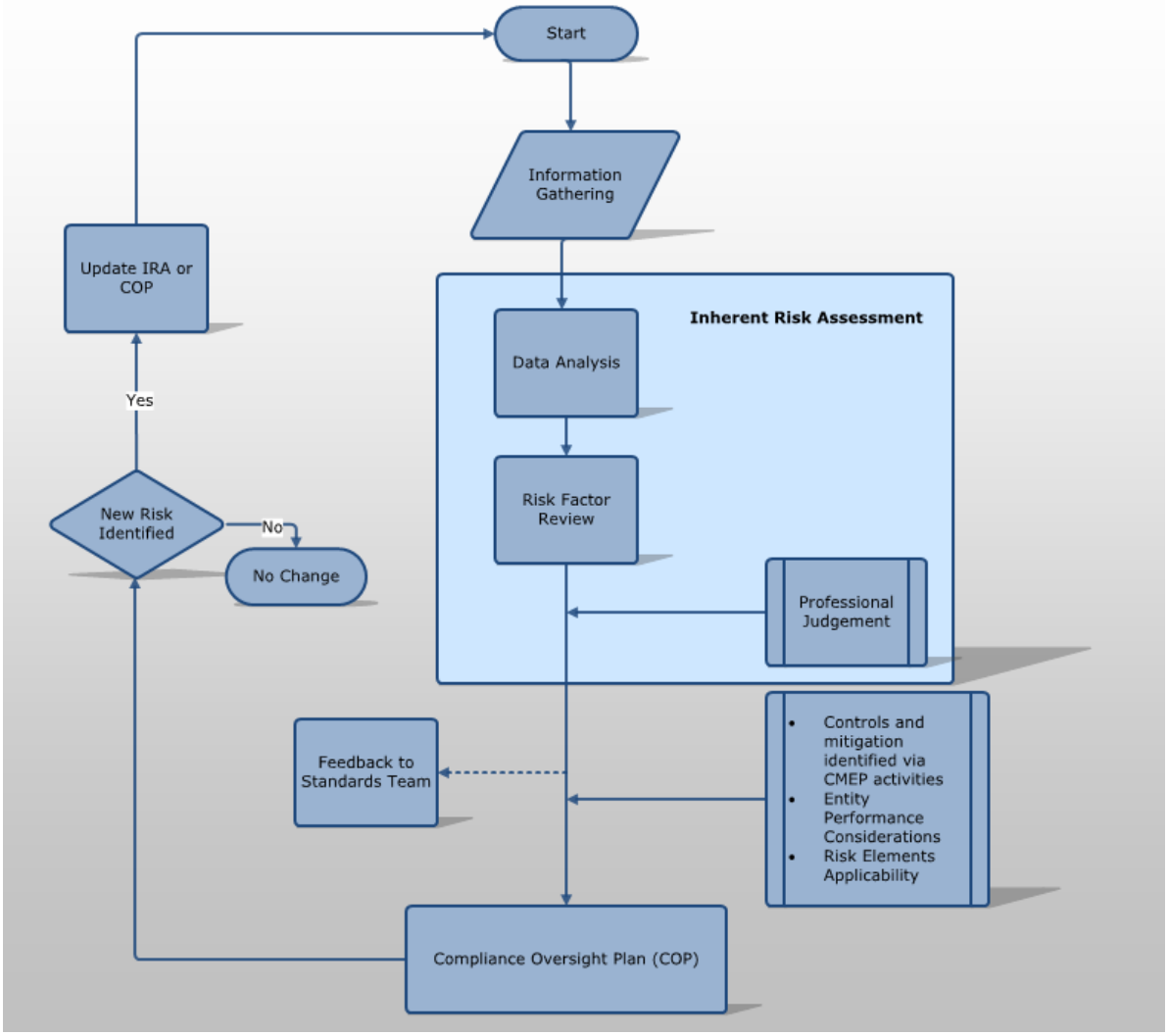


Figure 2. COP Development Process Overview

[2] The CEA has flexibility to use additional considerations and professional judgement in determining the registered entity's inherent risk.

The CEA gathers data, as it deems necessary, and assesses the information about a particular registered entity for appropriateness (relevance) and sufficiency (completeness and accuracy) to afford a reasonable basis for a conclusion. During this process, the CEA should leverage knowledgeable parties, both internal and external, to provide input as necessary and may verify accuracy of data with registered entities. CEAs will apply professional judgment, use peer reviews throughout the process, and document conclusions reached. The IRA output is also one of the key inputs when developing the COP for a registered entity.

2.1 Information Gathering

The information gathering process consists of identifying and collecting registered entity specific information required by the CEA to perform the IRA and COP. Determining entity specific information needed to perform IRA and COP, developing targeted information request list, and knowing the information gathering key outputs may assist CEAs in identifying the information already available, while highlighting additional information that may be required for IRA decision making. The following information may assist CEAs in identifying the information already available, while highlighting additional information that may be required for IRA and COP decision making.

2.1.1 Determine entity specific information needed to perform IRA and COP

To identify information already available, as well as information needed to conduct the IRA and COP, CEAs should:

- Review the Annual ERO Enterprise CMEP IP for applicability to the registered entity (i.e., determine if there are certain known risks to the reliability of the BPS, based on functional registration, apply to the registered entity and drive the need for further information).
- Leverage the CEA's existing understanding of the registered entity, which may include inventorying and aggregating information already held by the ERO (e.g., information from prior audits, compliance history information, etc.).
- Review the registered entity's registration, including applicable JROs and CFRs, to determine the registered entity's responsibilities.
- Reconcile the information on hand with the Risk Factor criteria list in Appendix B to identify potential information gaps and data verification needs. The CEA can use information specific to regional risk and professional judgement during the IRA process.
- Identify any other information needed for developing a COP.

2.1.2 Develop Targeted Information Request List

After completing an inventory of the information that is readily available and identifying the additional information needed, the CEA may develop targeted information requests.

The CEA should minimize its request for information from registered entities when the same information is available within the ERO or through other reliable sources, although the CEA may need to gather information from the registered entity if a new risk arises. The CEA should confirm that information collected is both appropriate and sufficient: appropriateness is a measure of the quality of information that encompasses its relevance, validity, and reliability, and sufficiency is a measure of the quantity of information that is necessary to draw conclusions.

Possible Guidance Questions

1. What Risk Factors are applicable?
2. What registered entity specific information needed to understand a registered entity's inherent risk and develop a COP?

For example, to verify information appropriateness, the CEA may confirm the accuracy and reliability of facility data with other independent sources such as maps, prior data requests, reliability assessments, event reports, and information from Periodic Data Submittals.

CEAs should exercise professional judgment when identifying the most reliable sources that will provide the required information to perform an IRA and COP. Professional judgment requires an appropriate skill set and experience to conduct the IRA and COP. When available, the CEA staff should use existing information, rather than creating new data requests for the registered entity. The CEA should take measures to ensure the information available is accurate and complete.

Possible Guidance Questions

3. Where is the source of information?
4. Is the information appropriate and sufficient?

2.1.3 Information Gathering Key Outputs

- Updated / verified registered entity data for assessment
- Targeted information request

2.2 Assessment of Information

Assessment of information consists of four main areas as identified below:

- Data analysis process
- Risk Factor review
- Assessment key outputs
- Additional regional considerations and use of professional judgement

During the assessment, the CEA will be able to identify the inherent risk associated with the registered entity based on the characteristics unique to the registered entity.

2.2.1 Data Analysis Process

CEAs perform data analysis to help develop understanding of a registered entity and support Risk Factor analysis and identification of risks. For data analysis, CEAs review information collected to assess and draw conclusions around registered entity data. The CEA should analyze any trends observed while reviewing registered entity data.

Possible Guidance Questions

5. Can the CEA verify the information received by the registered entity? For example, whether agreements exist between two registered entities, the existence of jointly owned facilities, and the Planning Authority Area in which the registered entity's facilities reside.
6. Which Risk Factors will apply to the registered entity and will be used to assess the level of significance of Reliability Standards and requirements from the IRA?

2.2.2. Risk Factor Review

In order to perform Risk Factor analysis, the CEA reviews the entity-specific information, including trends, as well as other known risks to the reliability of the BPS. The CEA uses this information to identify the risks associated with the registered entity based on the Risk Factor evaluation criteria identified in Appendix B and determines the level of risk to be high, medium, or low.

Appendix B contains the common set of ERO Enterprise Risk Factors and criteria used by CEAs. Some Risk Factor criteria, such as Underfrequency Load Shedding equipment, provides regional flexibility for determining risk levels to allow for technical variances across Interconnections, or in some cases, regional boundaries. Additionally, CEAs may need to deviate from an established Risk Factor criteria based on technical justification. Although deviations from defined Risk Factor criteria may occur, CEAs will justify any differences and may only significantly alter the core list of common risk factors in coordination with NERC and the other CEAs.

The criteria provided for each Risk Factor serves as a guideline and helps promote a consistent and repeatable process for assessing quantitative areas of risk. However, if certain facts or circumstances exist for a particular registered entity, the CEA should determine whether the criteria are appropriate and should identify the appropriate level of risk. CEAs should use professional judgement and justify the Risk Factors and criteria results.

Possible Guidance Questions

7. Is there other information that impacts Risk Factor and criteria decisions?
8. Does the justification provided support decisions on Risk Factor analysis and criteria decisions?

2.2.3 Assessment Key Outputs

After completing the Assessment, key outputs include:

- Trends that allow the CEA to focus on risks in specific areas.
- Details that identify associated Reliability Standards and requirements that potentially pose higher risk to reliability.
- Prioritized list of Risk Factors and criteria (including evaluation of impact) and associated Reliability Standards and requirements for COP consideration.
- Justification of decisions made during the assessment process and documentation supporting decisions.

2.3 IRA Results

The CEA should leverage subject matter experts throughout the IRA process as needed. Once preliminary Risk Factors and Reliability Standards and requirements conclusions have been reached, the CEA should consult additional subject matter experts (if applicable), or conduct an independent management review of the IRA output to verify the appropriateness based on the information known about the registered entity as a check on the IRA process.

2.3.1 IRA Results Key Outputs

At the completion of the IRA, assessment results will include:

- Risk assessment results, which include a list of Risk Factors and criteria and recommendation for specific Standards and requirements that should be considered for COP.
- Justification supporting conclusions on Risk Factor criteria.

2.4 IRA Triggers

The CEA may review and revise a registered entity's IRA at any time. A review or revision is more likely to occur if a registered entity experiences significant changes, new compliance responsibilities, or new reliability risks emerge. Significant changes may include, but are not limited to, registration changes, asset ownership changes, system events, severe risk violations, etc.

The CEA should rely on both internal and external sources to identify significant changes and triggers that may require an IRA review or revision.

Possible Guidance Questions

9. Are there any changes to the registered entity's characteristics since the last IRA?
10. Are there any significant reliability risks that indicates reviewing the registered entity's IRA is needed?

2.5 IRA Feedback into ERO Enterprise Processes

An ERO Enterprise feedback loop involving compliance monitoring activities will help determine future priorities, projects in the NERC standards development process, and other ERO Enterprise program areas. As CEAs conduct IRAs, CEAs may identify certain risk areas that do not map to current enforceable Reliability Standards. The CEAs may also determine other gaps, revisions, or retirement needs of Reliability Standards or other program activities. That feedback loop will mature with more experience implementing risk-based compliance monitoring methods.

3.0 Compliance Oversight Plan

The COP is the output of the Framework and tailors compliance monitoring activities for NERC Reliability Standards based on entity-specific risks. The COP includes the NERC Reliability Standards for monitoring, the interval of monitoring activities, and the type of CMEP tool (such as Compliance Audit, Spot Check, or Self-certification). The purpose of the COP is to capture how a CEA will monitor a registered entity's inherent risks and compliance with NERC Reliability Standards. The COP is subject to change and is not a static document. The COP process, outputs, and triggers described in this section provides CEAs guidance on how to use key considerations to develop entity-specific COPs.

3.1 COP Process

CEAs develop entity specific COPs by using IRAs, as well as additional considerations, such as Risk Elements, entity performance, and internal controls and mitigating activities. As described below, the CEA uses these additional considerations to prioritize monitoring of the risks and associated NERC Reliability Standards and to identify the appropriate CMEP Tool.

3.1.1 Risk Element Considerations

Although each registered entity has a unique inherent risk to the BPS, how the inherent risk may be monitored by the CEA can be impacted by broader regional or continent-wide risks. Therefore, the CEA may consider Risk Elements in determining the appropriate method and interval of monitoring. For instance, if a registered entity has a high inherent risk in one particular area that could impact a regional or continent-wide risk, the CEA may elect to monitor the registered entity accordingly to ensure broader risks are not actualized. As a result, both ERO Enterprise and region-specific Risk Elements developed by the CEAs serve as an input in determining the appropriate monitoring of risks and related Reliability Standards and requirements in the COP.

3.1.2 Entity Performance Considerations

Based on the output of the overall data analysis and Risk Factor review, the CEAs may use additional regional considerations[3] and professional judgement to further refine the risk associated with the registered entity. For example, compliance history, event analysis trends, or other performance data may impact a CEA's decision to monitor a specific risk area or NERC Reliability Standard assessed during the IRA. The CEA may also weigh the registered entity's compliance monitoring history and those areas that have been monitored frequently in the past. If there were no identified issues, the CEA may decide to modify future intervals of monitoring. Registered entity performance considerations also reflect the notion that inherent risk alone is not the only consideration in developing COPs.

Possible Entity Performance Consideration Examples

11. Has the entity had repeated, ongoing, or substantial issues with a particular function, such as protection system maintenance? This may impact the monitoring tools or interval used for PRC-005 evaluation.
12. Have any events occurred on the entity's system that may indicate a potential issue with a Reliability Standard? Are misoperations being reported and do they indicate a need for further review?
13. Have any recent issues been discovered for neighboring or similar entities that may also impact the registered entity under review?

[3] Additional regional considerations might be additional qualitative information identified by the CEA that can help refine the risk

3.1.3 Internal Controls and Mitigating Activities

Internal controls and other mitigating activities may impact compliance monitoring determinations. CEAs utilize available information to determine whether internal controls provide reasonable assurance of compliance with mandatory NERC Reliability Standards. CEAs obtain an understanding of internal controls through ICE, and through ongoing activities and interactions with the registered entity. The ERO Enterprise ICE Guide describes the common ERO Enterprise process for evaluating internal controls.

In general, CEA staff have to obtain an understanding of internal controls related to the scope of work performed during compliance monitoring activities. In addition to the ICE process, CEA staff can obtain an understanding of internal control through inquiries, observations, inspection of documents and records, review of other CEA staff reports, or direct tests. The nature and extent of procedures CEA staff perform to obtain an understanding of internal control may vary among compliance monitoring activities based on compliance monitoring objectives, inherent risk, known or potential internal control deficiencies, and the CEA staff's knowledge about internal controls gained in prior compliance monitoring activities.

A good sound business approach to incorporating effectively designed and implemented internal control improves operational and compliance performance. Through evaluations, the CEA may take into account good governance practices of registered entities that effectively manage risk to BPS. In addition, the lessons learned from evaluating internal controls may encourage the adoption of such practices throughout the ERO Enterprise and industry.

The ERO Enterprise recognizes that internal controls cannot provide absolute assurance of compliance with Reliability Standards, whereas CEAs may modify the nature, timing, or extent of compliance monitoring activities based on their understanding and evaluations of internal controls. When developing a registered entity COP, the CEA may work with the registered entity to identify and review existing internal controls, which may be used to focus and select appropriate tools used by the CEA under the CMEP.

3.2 COP Key Outputs

When complete, the COP will include, at a minimum, the following items: A list of the NERC Standards and requirements identified for monitoring, possible CMEP Tools used for monitoring the identified NERC Reliability Standards, and the interval of monitoring to be performed.

Note that a COP is dynamic and subject to change. CMEP Tools are used, as needed, by CEAs to evaluate compliance and are implemented considering numerous factors including, but not limited to, the required notification periods within the NERC ROP. Registered entities are required to be compliant with all applicable Standards and requirements at all times. The COP is subject to change and adjustments may be made as needed. CEA staff have the responsibility to change compliance engagement scopes, if there is a recognized need based on facts and circumstances.

3.3 COP Triggers

CEAs can review and revise the COP of a registered entity at any time and should be cognizant of the effect that a registered entity's risks may pose to maintaining a reliable BPS. This understanding is essential in developing a COP, as it establishes a frame of reference by which the COP is implemented. Importantly, a COP may need to be revised as new, emerging, or unique information is obtained either about the registered entity or about risks to the reliability of the BPS.

The COP will be performed on a periodic basis as determined by the CEA, including consideration for IRA refreshes that contain material changes. Additional triggers for conducting a COP may include (but are not limited to) changes to a registered entity, a change in registration, a change in the registered entity IRA, new Reliability Standards, changes in controls, emerging risks, changes in performance considerations, and

feedback from CEA staff or CMEP activities. Some changes may impact both the IRA and the COP, while others may only inform one process or the other (e.g. registered entity involvement in an event may trigger monitoring adjustment in the COP, but does not impact Inherent Risk).

4.0 Documentation

CEAs should document work performed during IRA, ICE or other control reviews, COP development. Documentation should contain sufficient detail to enable other experienced CEA or NERC staff to understand the steps performed and conclusions reached. The sections below highlight key activities for sharing results with registered entities, documenting results, maintaining documentation and confidentiality of information.

4.1 Sharing of Results

CEAs should facilitate a collaborative dialogue with the registered entity throughout the IRA process. As needed, CEAs should work with the registered entity to ensure the CEA has appropriate and sufficient information to conduct the IRA and ultimately develop a COP. At minimum, the CEA will communicate the CMEP tools planned to be utilized, the monitoring interval(s), and if appropriate, NERC Reliability Standards and requirements for compliance monitoring. The CEA will communicate this information by sharing the initial IRA results and COP. The CEA will continue to share IRA results and communicate COPs no later than the notification periods required by NERC ROP for selected CMEP tools, and CEAs will also provide additional information on compliance monitoring activities in the Annual ERO Enterprise CMEP IP.

4.2 Results Documentation

The CEAs should follow established documentation protocols, refer to the NERC ROP, and use professional judgment, where appropriate, when determining documentation needs throughout the IRA process. The CEA should maintain documentation that clearly supports conclusions made during any part of the IRA process and compliance oversight planning. At a minimum, documentation includes data and information obtained, reviewed, and used as inputs to the IRA, and should be linked to conclusions so that one can easily see why final determinations were made. The CEAs should maintain documentation, demonstrating the nature and extent of information reviewed and IRA conclusions reached.

The extent of the resulting documentation is directly linked to the (1) nature, size, and complexity of the issues, (2) procedures performed, and (3) methods and technologies used during the process. The more significant and complex these factors are, the greater and more detailed the documentation may be.

4.3 Documentation Retention

Upon completion of the IRA process, the CEA should retain relevant documentation that supports the procedures performed and conclusions reached. Examples of documentation that should be retained include (but are not limited to) the following: IRA programs, analyses, memoranda, summaries of significant findings or issues, checklists, abstracts, copies of important documents, and paper or electronic correspondence concerning significant findings or issues. Additionally, finalized narrative descriptions, questionnaires, checklists, and flowcharts created through the IRA process are also considered important documentation and should be retained.

When making the determination of the nature and extent of documentation that should be retained, the CEA should consider the information that would be required for experienced CEA staff understanding the work performed and the conclusions reached during the IRA. Incomplete or preliminary documentation does not need to be maintained.

CEAs follow NERC ROP, ERO Enterprise, where applicable, and Regional Entity processes for handling confidentiality of information and data retention periods.

5.0 References

Below are a list of reference materials that support the basic principles, concepts, and approaches within this Guide. CEAs use these reference materials to assist in implementing the Framework and processes detailed in this Guide. These reference materials can assist with determining: (1) where and to what extent professional judgment should be applied, (2) the sufficiency and appropriateness of evidence to be examined, and (3) the sufficiency and appropriateness of the documentation required. Additionally, NERC ROP and key Federal Energy Regulatory Commission (FERC) filings and Orders contain descriptions of the Framework discussed in this Guide.

- Generally Accepted Government Auditing Standards (GAGAS), located at: http://gao.gov/assets/590/587281.pdf
- ERO Enterprise CMEP Manual, located at: http://www.nerc.com/pa/comp/Pages/ERO-Enterprise-Compliance-Auditor-Manual.aspx
- Annual ERO CMEP IP, located at: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx
- NERC ROP, located at: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx
- Key FERC filings and Orders:
  - Informational Filing of NERC Regarding Implementation of the Reliability Assurance Initiative (November 3, 2014)
    - FERC Order on Risk-based Compliance Monitoring and Enforcement Program (February 19, 2015)
  - Compliance Filing of NERC and Petition for Approval of Rules of Procedure Revisions (July 6, 2015)
    - Order Conditionally Accepting CMEP Compliance Filings and ROP Revisions (November 4, 2015)[4]
  - Annual Compliance Monitoring and Enforcement Program Report (February 19, 2016)
    - Letter Order Accepting Annual CMEP Report (April 14, 2016)

[4] FERC's November 4 Order directed NERC to revise the applicable Rules of Procedure to reflect certain components of the risk-based CMEP, specifically related to enforcement activities of self-logging and compliance Exceptions. Therefore, related filings and Orders are note appropriate for this Guide.

Appendix A – Definitions

Appendix A includes terminology used within this Guide, where the term is not defined in other ERO Enterprise documents or the NERC ROP.

Areas of Focus: The outcomes of the IRA process and determines: Risks deemed applicable to the registered entity; NERC Reliability Standards deemed appropriate to apply to the registered entity; and associated Risk Factors to NERC Reliability Standards and requirements

Compliance Oversight Plan: A plan consisting of the oversight strategy for a registered entity, including the list of Standard requirements for monitoring, the CMEP tool to be used, and the interval of monitoring.

CMEP Tools: In context of the IRA, these are tools used during the compliance monitoring processes to develop the COP. CMEP tools are described in Section 3.0 of the NERC ROP, Appendix 4C, and includes but are not necessarily limited to Compliance Audits, Spot Checks, Self-Certifications, and Periodic Data Submittals.

Inherent Risk: Attributes specific to a registered entity that could impact the reliability of the BPS. For example, entity configuration and profile, registration, transmission and generation assets, etc.

Professional Judgment[5]: CEA staff use professional judgement in planning, performing, and reporting results of CMEP activities. Professional judgment represents the application of the collective, individual, knowledge, skills, and experiences of all the personnel involved with a CMEP activity. In addition to personnel directly involved in the audit, professional judgment may involve collaboration with other stakeholders, external specialists, and management in the audit organization.

Reasonable Assurance[6]: Conclusions based on evidence that is sufficient and appropriate to support the CEA's conclusions. (Note: Emphasis on reasonable, not "complete" or "absolute" assurance).

Risk[7]: Risk is the likelihood of an event occurring, coupled with a negative consequence of the event occurring. In other words, a risk is a potential problem — something to be avoided if possible, or its likelihood and/or consequences reduced if not avoided.

Risk Factors: Measureable aspects used during an IRA to identify a registered entity's risk characteristics related to requirements that are inherent to a registered entity's configuration and may impact the reliability of the BPS.

[5] Generally Accepted Government Auditing Standards Section 3.60-3.68.

[6] Generally Accepted Government Auditing Standards Section 6.03.

[7] ERO Enterprise Self Report User Guide, located here: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf

Appendix B – ERO Enterprise Risk Factors

Below is the ERO Enterprise list of common Risk Factors and assessment criteria CEAs use to complete the IRA for a registered entity.

Risk Factors	Criteria for Assessment			
Risk Factor	**N/A**	**Low Risk**	**Medium Risk**	**High Risk**
CIP - Impact Rating Criteria	Entity has no BES Cyber Systems (BCS)	Entity has one or more low impact BCS(s)	Entity has one or more medium impact BCS(s)	Entity has one or more high impact BCS(s)
ICCP Connectivity	Entity has no BES Cyber Systems (BCS)	Entity has low impact BCS(s) without ICCP connections or external routable connectivity	Entity has low impact BCS(s) with at least one ICCP connection - or - Entity has low impact BCS(s) with external routable connectivity (LERC) - or - Entity has medium impact BCSs	Entity has medium impact BCS(s) with at least one ICCP connection - or - Entity has high impact BCS(s)
Load	Entity does not have any system load	Entity's system load is less than 300 MW	Entity's system load is between 300 - 1,000 MW	Entity's system load is greater than 1,000 MW
Transmission Portfolio	Entity does not own, operate, coordinate, plan, design, or monitor the status of transmission facilities	Entity has transmission facilities less than 200kV	Entity has transmission facilities between 200 -300 kV - or - Entity has over 1,000 miles of transmission lines 100 kV or greater	Entity has transmission facilities greater than 300 kV - or - Entity has over 4,000 miles of transmission lines 200 kV or greater
Critical Transmission	Entity does not own, operate, coordinate, plan, design, or monitor the status of transmission facilities	Entity's system is not critical to adjacent entities as it is not being used as a flow through system for power flow	Entity's system is critical to adjacent entities as it is being used as a flow through system for power flow	Entity's system includes elements (owned or operated) of an IROL / Flowgate / Major Transmission Path (WECC) / Generic Transmission Limit (Texas RE) / Cranking Path

Risk Factors	Criteria for Assessment			
Risk Factor	**N/A**	**Low Risk**	**Medium Risk**	**High Risk**
Voltage Control	Entity does not own or operate any voltage control equipment	----------	Entity owns and/or operates reactive resources to provide voltage control	Entity owns and/or operates reactive resources other than generators to provide voltage control
Largest Generator Facility	Entity does not own any generation facilities	Entity's largest single generation facility is less than 500 MVA	Entity's largest single generation facility is between 500 - 1,000 MVA	Entity's largest single generation facility is greater than 1,000 MVA
Total Generation Capacity	Entity does not own or operate any generation facilities	Entity's total generation nameplate capacity is less than 1,000 MVA	Entity's total generation nameplate capacity is between 1,000 - 5,000 MVA	Entity's total generation nameplate capacity is greater than 5,000 MVA
Variable Generation	Entity does not meet any of the identified criteria	Less than 10% of the entity's BA Area total generation nameplate MVA is comprised of non-dispatchable generation	10% - 25% of the entity's BA Area total generation nameplate MVA is comprised of non-dispatchable generation	Over 25% of the entity's BA Area total generation nameplate MVA is comprised of non-dispatchable generation
Balancing Authority (BA) Coordination	Entity does not meet any of the identified criteria	Entity's BA Area has less than 5,000 MW of generation capacity	Entity's BA Area has between 5,000 - 10,000 MW of generation capacity	Entity's BA Area has greater than 10,000 MW of generation capacity - or - Entity's BA Area has greater than 5,000 MW of generation capacity and its Generation to Peak Load ratio is more than 1.2
Planned Facilities	Entity does not meet any of the identified criteria	Entity is planning on or currently building transmission facilities less than 200 kV in the next three years - or - Entity is planning on or currently building generation facilities that are less than 500 MVA in the next three years	Entity is planning on or currently building transmission facilities between 200 - 300 kV in the next three years - or -	Entity is planning on or currently building transmission facilities greater than 300 kV in the next three years - or - Entity is planning on or currently building generation facilities greater than 1,000 MVA in the next three years

Risk Factors	Criteria for Assessment			
Risk Factor	**N/A**	**Low Risk**	**Medium Risk**	**High Risk**
			Entity is planning on or currently building generation facilities that are between 500 and 1,000 MVA in the next three years	
RAS/SPS	Entity does not own, operate, coordinate, plan, design, or monitor the status of a RAS/SPS	----------	Entity owns or designed a RAS/SPS that is not needed to meet TPL requirements - or - Entity owns or operates equipment that is part of a RAS/SPS that is not needed to meet TPL requirements	Entity owns or designed a RAS/SPS that is needed to meet TPL requirements - or - Entity owns or operates equipment that is part of a RAS/SPS that is needed to meet TPL requirements
Workforce Capability	Entity does not meet any of the identified criteria	Less than 25% of the entity's System Operators have less than 5 years of System Operator experience	Between 25 - 50% of the entity's System Operators have less than 5 years of System Operator experience	Greater than 50% of the entity's System Operators have less than 5 years of System Operator experience
Monitoring and Situational Awareness Tools	Entity does not meet any of the identified criteria	Entity does not have monitoring and situational awareness tools and operates 10 or more lines over 100 kV	Entity does not have monitoring and situational awareness tools and operates 10 or more lines over 200 kV	Entity does not have monitoring and situational awareness tools and operates 20 or more lines over 200 kV
System Restoration	Entity has no responsibilities during system restoration	Entity has regional or company system restoration responsibilities limited to load restoration	Entity has Blackstart Resource(s) - or - Entity provides switching or other logistics based on the direction from a different entity responsible for the restoration plan	Entity is an RC - or - Entity is responsible for independent actions coordinated with an RC

Risk Factors	Criteria for Assessment			
Risk Factor	**N/A**	**Low Risk**	**Medium Risk**	**High Risk**
UFLS Equipment	Entity does not own or operate UFLS equipment	Entity is responsible for "X%"[8] of the entire regionally identified UFLS program	Entity is responsible for "X%" of the entire regionally identified UFLS program	Entity is responsible for "X%" of the entire regionally identified UFLS program
UFLS Development and Coordination	Entity is not responsible for developing or coordinating a UFLS program	Entity is responsible for developing and/or coordinating a UFLS program for "X" MWs of load	Entity is responsible for developing and/or coordinating a UFLS program for "X" MWs of load	Entity is responsible for developing and/or coordinating a UFLS program for "X" MWs of load
UVLS	Entity does not have any UVLS responsibilities	----------	Entity is responsible for 1 - "X" MWs of load shed by a UVLS program	Entity is responsible for greater than "X" MWs of load shed by a UVLS program

[8] Risk Factor criteria that contain an "X" indicates the existence of regional criteria based on technical justifications.

Appendix C – Risk Elements Development Process

The purpose of Appendix C is to outline the process by which NERC will identify continent-wide risks to the reliability of the BPS, as well the Reliability Standards and registration functional categories related to those risks. This information will be used to develop the annual ERO Enterprise CMEP IP[9] and the included ERO Enterprise Risk Elements. The annual IP provides guidance to CEAs on identifying and justifying regional Risk Elements for inclusion in in the RE IPs.[10] The IP provides input to individualized COPs for registered entities. The transformation to focus on identifying and prioritizing risks replaces a static, one-size-fits-all list of Reliability Standards and prioritizes functions and Reliability Standards based on risk to determine the appropriate oversight method.

NERC annually identifies and prioritizes risks to reliability of the BPS, taking into account compliance findings and event analysis experiences, data analysis provided in several NERC publications and reports, and expert judgment of ERO Enterprise staff, committees and subcommittees. Each year, NERC compliance assurance staff, with input from other departments at NERC and the Regional Entities, will execute the following process to identify Risk Elements and select specific requirements from the Reliability Standards for increased focus. The results of this process will be reflected in the IP and will also guide the development of the RE IPs.

The risks identified through the following process does not constitute the entirety of the risks that may affect the reliability of the BPS. REs are expected to consider local risks and specific circumstances associated with individual registered entities, within their footprint, in developing their compliance oversight plans:

1. During Q1 and Q2 of each year, NERC staff will collect the ERO Enterprise data, reports, and publications (available at the time) that identify reliability risks. Examples of such data and reports include the State of Reliability Report, the Long-Term Reliability Assessment, publications from the Reliability Issues Steering Committee (RISC), special assessments or reports, the ERO Enterprise Strategic Plan, ERO Event Analysis Process insights, significant occurrences noted by NERC and Regional Entity Situation Awareness staffs, and other relevant documents pertaining to risks to the reliability of the BPS.
2. Beginning in August, NERC staff will review those reports to develop a list of reliability risks. This risk prioritization will be informed by facts and circumstances, but will consider, among other factors, the sources of the risk, how many different sources identified the same risk, and the level of analysis that supports the assertion that the risk merits action.
3. NERC staff will then identify a preliminary list of effective body of Reliability Standards and requirements for the relevant year that are related to those reliability risks for additional focus. NERC staff will note those risks that are not addressed or mitigated by existing Reliability Standards as potentially requiring further analysis, consideration and potential action in other areas of ERO Enterprise operations.
4. From that set of requirements, NERC staff will consider the following additional factors and remove those requirements that are not appropriate for additional focus:
    a. Does the requirement contribute strongly to reliability? One way to evaluate this is to consider the FERC-approved Violation Risk Factor (VRF) of the requirement. Though VRFs are not the sole criterion to measure risks to reliability, in general, Low-VRF requirements are not good candidates for increased focus, while High-VRF requirements typically merit consideration.
    b. Have the requirements associated with the NERC reliability Standards been identifies through compliance data analysis as having moderate or significant risk impacts on BPS reliability when violated.

[9] CMEP (Appendix 4C to the Rules of Procedure) § 4.1. See also Rules of Procedure § 401.6.

[10] CMEP (Appendix 4C to the Rules of Procedure) § 4.2.

5. NERC staff will review the functional entities to which the remaining requirements apply, considering if some functions are more important to reliability with regard to a specific requirement than others. NERC staff will then remove functions from consideration for requirements as appropriate.
6. Finally, NERC staff, in coordination with REs, will review the preliminary lists of risks, associated Reliability Standards and requirements, and functions (if applicable) identified for areas of focus, to determine the final ERO Risk Elements to include in the Implementation Plan.

By September of each year, NERC staff will take the results of the steps described above and include such results in that year's IP. The IP will be posted on or about September 1 of each year.[11]

RE IP's should take into account the most important reliability risks within a given Regional Entity footprint and initiate plans for managing them through appropriate elements of the compliance monitoring and reliability assurance process. These may include, but are not limited to, the Risk Elements identified in the IP, regional risks identified by the RE, or a combination of both. The RE IP should explain how it identified the risks in a particular RE footprint, including reasons why Risk Elements identified in the ERO CMEP IP are not included. Note that not all risks identified in the IP need to be monitored with respect to each entity registered for a particular function.

RE IPs are provided to NERC staff on or about October 1. RE IPs are subject to review and approval by NERC.[12]

Using the IRA and considering ICE results and other considerations, the RE can further tailor the NERC Reliability Standards and requirements and determine monitoring approach. The RE may use any of the available compliance and monitoring tools in assuring compliance of a given entity. Registered Entities are, as always, required to comply with all applicable Reliability Standards, whether or not they are scheduled to be monitored on that particular Reliability Standard.

An ERO Enterprise feedback loop from compliance assurance activities will help inform future priorities and projects in the NERC standards development process, as well as other ERO Enterprise processes. This feedback loop will operate in areas where there may be gaps, as well as areas in which requirements should be retired. It is expected that the feedback loop will mature as more experience with the development and implementation of risk-based compliance monitoring methods is gained.

[11] CMEP (Appendix 4C to the Rules of Procedure) § 4.1.

[12] Rules of Procedure § 402 and CMEP (Appendix 4C to the Rules of Procedure) § 4.0.