[Regional Entity Logo]

Compliance Oversight Plan (COP) Report Template

[insert date here]

Registered Entity Name	
Registered Entity Acronym	
NCR ID # (NERC Compliance Registry – NCR)	
Registered Entity Functional Registration	[Enter all functions applicable to the registered entity.]

[Insert version #]

TABLE OF CONTENTS

[Regional Entity Logo]

1.0 Purpose

Regional Entities (RE) develop a Compliance Oversight Plan (COP) to capture how an RE will monitor a registered entity's compliance with selected NERC Reliability Standards based on entity-specific risks. COPs are developed by using results of the Inherent Risk Assessment and performance considerations. The Electric Reliability Organization (ERO) Enterprise Guide for Risk-based Compliance Monitoring[1] (Guide) describes the process used by [Regional Acronym] to develop entity-specific COPs and serves as a common approach for the North American Electric Reliability Corporation (NERC) and [Regional Acronym] for implementing risk-based compliance monitoring. As directed by the Guide, REs share a COP with the registered entity, which also includes a summary of the Inherent Risk Assessment results (IRA). The COP includes the NERC Reliability Standards associated with identified risks, the interval of monitoring activities, and the type of Compliance Monitoring and Enforcement Program (CMEP) tool(s) (such as Compliance Audit, Spot Check, or Self-certification). The COP is dynamic, and changes are likely to occur if a registered entity experiences significant changes, new compliance responsibilities, or new reliability risks emerge.

The COP does not change any obligation for a registered entity to be compliant with all NERC Reliability Standards. While the overall process identifies a planned compliance monitoring strategy for a registered entity, the COP should not be interpreted as a limitation to ERO Enterprise authority, under the NERC Rules of Procedure, to conduct any compliance monitoring activities as the ERO Enterprise may determine appropriate.

In addition to this COP, the annual ERO Enterprise CMEP Implementation Plan[2] detail the actual compliance monitoring that will occur in a given implementation year. REs will also follow the existing requirements in the NERC Rules of Procedures for notifying and conducting compliance monitoring activities.

2.0 Analysis and Results

[Regional Acronym] has carefully reviewed numerous inputs, including IRA results and performance considerations such as internal controls, mitigation plans, compliance history, event analysis trends, or other regional factors to identify key risks. The risk outlined below indicates the unmitigated, operational, or inherent risks identified by [Regional Acronym]. While all risks require monitoring and action to mitigate or reduce the likelihood of events that adversely impact the reliability of the Bulk Power System, [Regional Acronym] will focus its monitoring on these risks. Accordingly, monitoring of the risk may include one or more CMEP monitoring tools, as specified in Section 3.

Appendix A contains a table with the IRA summary results that include risk factors and assessments made by [Regional Acronym].

3.0 Oversight Strategy

Table 1.1, Oversight Strategy Categories, generally describes how the ERO Enterprise divides its oversight strategy into six categories to determine the appropriate interval and CMEP Tool(s) for a registered entity. Using this as a guide allows [Regional Acronym] to prioritize monitoring by focusing on higher risk areas and determining interval and intensity for monitoring. The intervals and primary CMEP

[1] ERO Enterprise Guide for Compliance Monitoring

[2] ERO Enterprise CMEP Implementation Plan

Tools should not be read to preclude different intervals or CMEP Tools depending on individual registered entity facts and circumstances.

Additionally, Appendix B contains NERC Reliability Standards associated with the identified risk(s) and considered as part of the oversight strategy.

Table 1.1 Oversight Strategy

Category[3]	Category Description	Target Monitoring Interval	Primary CMEP Tools
1	Represents an entity that has higher inherent risk without demonstrated positive performance considerations.	Every 1-3 years	Compliance Audit (on/off-site) Spot Check Self-Certification
2	Represents an entity that has higher inherent risk with demonstrated positive performance considerations.	Every 2-4 years	Compliance Audit (on/off-site) Spot Check Self-Certification
3	Represents an entity that has moderate inherent risk without demonstrated positive performance considerations.	Every 3-5 years	Compliance Audit (on/off-site) Spot Check Self-Certification
4	Represents an entity that has moderate inherent risk with demonstrated positive performance considerations.	Every 4–6 years	Compliance Audit (off-site) Spot Check Self-Certification
5	Represents an entity that has lower inherent risk without demonstrated positive performance considerations.	Every 5-7 years	Compliance Audit (off-site) Spot Check Self-Certification
6	Represents an entity that has lower inherent risk with demonstrated positive performance considerations.	Every 6+ years	Compliance Audit (off-site) Spot Check Self-Certification

[3]For entities registered as a Balancing Authority, Reliability Coordinator, or Transmission Operator, the Compliance Audit will be performed at least once every three years in accordance with the NERC Rules of Procedure.

Appendix A: IRA Results Summary

Appendix A identifies inherent risk by risk factors and assessment criteria of high, medium, or low based on predetermined criteria in the *ERO Enterprise Guide for Compliance Monitoring*. Included are RE justifications or explanations to support risk determinations.

Risk Factor Assessment		
Risk Factor	**(High, Medium, Low, NA)**	**Explanation**
		[Insert professional and technical justifications for risk levels]

Appendix B: Standards and Requirements for Monitoring

Appendix B identifies the NERC Reliability Standards that may be associated with the risk outlined in Section 2 and considered as part of the oversight strategy. Note that a COP is dynamic and subject to change. CMEP Tools are used, as needed, by REs to evaluate compliance. They are implemented considering numerous factors including, but not limited to, the required notification periods within the NERC Rules of Procedure. Registered entities are required to be compliant with all applicable Standards and Requirements at all times.

Associated NERC Reliability Standards and Requirements for Monitoring	
Standard	**Requirement**