NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Oversight Plan

Frequently Asked Questions and Answers

1. **What is the Compliance Oversight Plan (COP)?**
   The COP is an entity-specific report consisting of entity-specific risks identified through analysis of both Inherent Risk Assessment (IRA) and Performance Considerations[1]. The report includes the NERC Reliability Standards associated with identified Risk Categories, interval of monitoring activities, and the type of CMEP tool(s) that may be used for monitoring. The COP is dynamic, and changes are likely to occur if a registered entity experiences significant changes or assumes new compliance responsibilities, or new reliability and security risks emerge.

2. **What are Performance Considerations?**
   Performance Consideration[2] is a data point or piece of information that REs consider to understand an entity's performance to identify entity-specific risks. The Performance Considerations are qualitative and dependent on known facts and circumstances.

3. **Is it Mandatory for a Registered Entity to have a COP?**
   The ROP[3] and ERO Enterprise Guide for Compliance Monitoring require the development of an IRA and COP for each registered entity.

4. **Will the COP contain the audit scope?**
   No, the COP will not include the audit scope. Appendix B of the COP Report will list the Standards/Requirements associated with the identified Risk Categories, and these Standards/Requirements inform the audit scope and/or other compliance monitoring activities. In the case of Compliance Audits, the audit scope will be included in the Audit Notification Letter (ANL). For selected CMEP Tools, the Regional Entities will provide notifications no later than the periods required by NERC ROP.

5. **When does my COP get updated?**
   Regional Entities may 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 secure and reliable BPS. This understanding is essential, 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 security and/or reliability of the BPS.

[1] ERO Enterprise Guide for Compliance Monitoring
[2] Performance Considerations used by the ERO Enterprise include, but not limited to Affiliates, Compliance History, Culture of Compliance, Events, Misoperations, Internal Controls
[3] Rules of Procedure Appendix 4C, Section 3.1.4.1

6. What are the differences between Risk Elements in the Annual ERO Enterprise CMEP Implementation Plan (IP) and Risk Categories and Risk Factors in the COP?

Risk Elements *are developed on an annual basis and identify ERO Enterprise-wide risks to the security and/or reliability of the BPS and mitigating factors that may reduce or eliminate a given reliability risk. The Risk Elements identify NERC Reliability Standards and Requirements to be considered for focused CMEP activities.*[4]

Risk Categories *outlined in the entity-specific COP indicate the unmitigated and operational risks identified by the Regional Entity based on the entity's inherent risks (i.e., Risk Factors) and performance related to the operational risks. The RE focuses its monitoring on the risks identified in the Risk Categories to inform compliance monitoring as to the entity-specific risks. REs use Risk Categories to understand, monitor, and mitigate known and future unmitigated, operational, or inherent risks as determined by the RE. The Standards/Requirements associated with identified Risk Categories are located in Appendix B of the entity's COP Report.*

Risk Factors *are measureable aspects used during an IRA to identify a registered entity's risk characteristics related to Standards/Requirements that are inherent to a registered entity's configuration and may impact the reliability of the BPS.*

7. What is Demonstrated Positive Performance?

Demonstrated Positive Performance is the term used for determining entity-specific Oversight Strategy (Section 3.0 of COP report). An entity would need to have strong performance amongst the vast majority of the Performance Considerations.

The "without demonstrated positive performance" designation is not necessarily an indication that an entity has poor performance. It may indicate that an entity has a mix of strong, average, or weak performance amongst the Performance Considerations or the RE is not informed of a certain Performance Consideration by the registered entity.

8. How does Demonstrated Positive Performance help change the Oversight Strategy?

An Entity with designated "Demonstrated Positive Performance" will move from either an Oversight Category 1, 3 or 5 down to an Oversight Category 2, 4 or 6 respectively. For example, an Entity initially within Category 3 but "Demonstrated Positive Performance" will move to Category 4, with lengthier targeted monitoring intervals. Also, for such an entity, the primary CMEP tool for Compliance Audit may move from onsite audit to an offsite audit.

9. Where are the Risk Categories posted?

The Risk Categories and associated Reliability Standards are provided in the table below. The ERO Enterprise will update this table as needed.

[4] Defined in ROP Section 401: Scope of the NERC Compliance Monitoring and Enforcement Program

Risk Category	Description/Risk Failure	Related Standards
Asset/System Identification	The identification and tracking of assets and BES Facilities is required and critical to BPS reliability. Failure to correctly identify, document, and track items may result in gaps and compromise the integrity and reliability of the BPS.	CIP-002-5.1a CIP-014-2 PRC-002-2 PRC-005-6 PRC-018-1 TPL-001-4
Entity Coordination	Coordination among entities, both internally and externally, as well as 3rd party suppliers and contractors, is necessary before making changes to the system or taking any actions that have the potential to impact another entity and, in turn, may impact the reliability and security of the BPS. Coordination should address the risk associated with operating horizon, planning horizons, and during emergencies. Failure to coordinate may result in an impact on the reliability and security of the BPS.	CIP-013-1 (Eff. 10/1/2020) EOP-005-3 EOP-006-3 IRO-014-3 NUC-001-3 PRC-001-1.1(ii) (inactive 9/30/2020) PER-006-1 (Eff. 10/1/2020)
Identity Management and Access Control	Entities must develop controls to prevent or mitigate malicious or unintentional access to BES Cyber Assets. Failure to develop controls may compromise the integrity and operability of the BPS.	CIP-004-6 CIP-005-5 (inactive 9/30/2020) CIP-005-6 (Eff. 10/1/2020) CIP-006-6 CIP-007-6 CIP-010-2 (inactive 9/30/2020) CIP-010-3 (Eff. 10/1/2020) CIP-011-2 CIP-014-2

Risk Category	Description/Risk Failure	Related Standards
Emergency Operations Planning	Entities must have the necessary facilities, tools, processes, and procedures in place to prevent or respond to system events, emergencies, or unexpected conditions. Failure to develop adequate plans may result in gaps in processes, procedures, and tools, which may lead to a compromise of the integrity and reliability of the BPS.	CIP-008-5 (inactive 12/31/2020) CIP-008-6 (Eff. 1/1/2021) CIP-009-6 EOP-005-3 EOP-006-3 EOP-008-2 EOP-010-1 EOP-011-1 IRO-014-3
Operating During Emergencies/Backup & Recovery	Entities must take appropriate actions during an emergency, system event, or unexpected conditions that could result in instability, uncontrolled separation, or cascading outages within an Interconnection. This can include the following: • Ensure personnel are sufficiently prepared and have adequate access to the procedures, processes, tools, and facilities necessary to respond appropriately and effectively during a system event, emergency, or unexpected condition. • Ensure adherence to processes and procedures during a system event, emergency, or unexpected condition. • Ensure proper operation, availability, and utilization of facilities and tools during a system event, emergency, or unexpected condition.	BAL-002-3 CIP-008-5 (inactive 12/31/2020) CIP-008-6 (Eff. 1/1/2021) CIP-009-6 EOP-005-3 EOP-006-3 EOP-008-2 EOP-011-1 IRO-014-3

Risk Category	Description/Risk Failure	Related Standards
Training	It is necessary for individuals/personnel/operators to have adequate knowledge and skills to ensure the reliability and security of the BPS. Failure to adequately train operating personnel may compromise the integrity and reliability of the BPS.	CIP-003-8 CIP-004-6 COM-002-4 EOP-005-3 EOP-006-3 PER-003-2 PER-005-2 PRC-001-1.1(ii) (inactive 9/30/2020) PER-006-1 (Eff. 10/1/2020)
Asset/System Management and Maintenance	BPS reliability depends on an entity's success in tracking, managing, and maintaining significant amounts of data, components, assets, and systems. The scope and complexity of this effort require programs to ensure that the entity effectively performs these activities. Failure to execute these programs can result in various types of lapses and may compromise the integrity and reliability of the BPS.	CIP-003-8 CIP-007-6 CIP-010-2 (inactive 9/30/2020) CIP-010-3 (Eff. 10/1/2020) CIP-011-2 FAC-003-4 FAC-008-3 PRC-005-6 (PRC-005-1 & associated Standards) PRC-006-3 PRC-023-4 VAR-002-4.1
Asset/System Physical Protection	Failure to ensure the physical protection of BES assets could lead to access by unauthorized personnel. Such access might lead to actions that result in instability, uncontrolled separation, or cascading within an Interconnection.	CIP-003-8 CIP-006-6 CIP-014-2

Risk Category	Description/Risk Failure	Related Standards
Long-term Studies/Assessments	Long-term studies and assessments in the planning horizon are used to evaluate whether the system can reliably operate in real-time. This includes the correct identification and protection of transmission and generation assets, properly designed plans for System Restoration from Blackstart Resources, impact studies for new and revised facilities, correct methodologies to determine and communicate SOLs and transfer capabilities, analysis of disturbances and misoperations, proper design of UFLS and UVLS programs, and response to GMD events. Failure to do so will likely result in gaps and may compromise the integrity and reliability of the BPS.	CIP-014-2 EOP-005-3 FAC-001-3 FAC-002-2 FAC-010-3 FAC-011-3 FAC-014-2 FAC-013-2 PRC-002-2 PRC-006-3 PRC-010-2 TPL-001-4 TPL-007-3 (inactive 9/30/2020) TPL-007-4 (effective 10/1/2020)

Risk Category	Description/Risk Failure	Related Standards
Operational Studies/Assessments	Operational studies and assessments in the operations horizon are used to evaluate whether the system can reliably operate in real-time. This includes correct calculation of Area Control Error (ACE) to ensure proper deployment of Regulating Reserve, correct methodologies for determining and communicating SOLs, ensuring that complete and comprehensive data is captured for Real-time Monitoring and Analysis capabilities, proper design, operating plans and response to GMD events, and Interpersonal Communication capabilities and protocols are established between entities to support reliable system operations and prevent instability, uncontrolled separation, or cascading outages. Failure to produce operational studies and assessments used in the operations horizon to understand gaps may result in a compromise of the integrity and reliability of the BPS.	BAL-005-1 COM-001-3 EOP-010-1 FAC-011-3 FAC-014-2 IRO-002-6 IRO-008-2 IRO-010-2 IRO-018-1(i) TOP-002-4 TOP-003-3 TOP-010-1(i)

Risk Category	Description/Risk Failure	Related Standards
Modeling Data	Simulation tools are mathematical models of individual components and their control systems, when applicable. These models form the building blocks of power system studies performed in the planning and operations horizons. Models that entities have verified to be accurate are critical to a range of reliability studies including transmission planning assessments and establishing SOLs and IROLs, as well as state estimation used for Real-time Assessments (RTA) and Operation Planning Assessments (OPA). The validity of those assessments is dependent on modeling data which includes, but is not limited to, correct Facility Ratings, verified generator real and reactive capability, and knowing how control systems respond to dynamic system conditions. Failure by appropriate entities to provide that data in a timely manner and at intervals that will assure model accuracy during retirements and new construction, may compromise the integrity and reliability of the BPS.	FAC-008-3 FAC-010-3 FAC-011-3 FAC-014-2 IRO-010-2 IRO-018-1(i) MOD-025-2 MOD-026-1 MOD-027-1 MOD-032-1 MOD-033-1 TOP-003-3 TOP-010-1(i)

Risk Category	Description/Risk Failure	Related Standards
System Protection	The reliability of the BPS requires that adequate generation supplies meet the existing load during steady-state and expected dynamic conditions. When faults or failures occur, the system must respond in a manner that isolates the problem but maintains the integrity of the BPS as is possible. The protection systems must be capable of identifying the location of the problem, the type of problem, and isolating the appropriate part of the BPS while minimizing the disturbance to the remainder of the system. This requires the Protection Systems associated with the generation, transmission, and load to accurately detect system properties and respond appropriately to unsafe conditions. Protection System settings must allow control systems to provide a full range of control and allow the system to "ride-through" expected transients. Owners of interconnecting BPS devices and systems must coordinate the settings of their systems with the neighboring systems to ensure they interact in a manner to achieve the desired outcome and prevent unnecessary disconnection of equipment. The Protection System must also be prepared in a manner that will respond to Misoperations of the primary protection. Entities must identify and correct the source of those operational failures.	PRC-001-1.1(ii) (inactive 9/30/2020) PER-006-1 (Eff. 10/1/2020) PRC-002-2 PRC-004-5(i) PRC-005-6 (PRC-005-1 & associated Standards) PRC-006-3 PRC-010-2 PRC-015-1 PRC-016-1 PRC-018-1 PRC-019-2 PRC-023-4 PRC-024-2 PRC-025-2 PRC-026-1

Risk Category	Description/Risk Failure	Related Standards
Normal System Operations	Actions performed by operations personnel during real-time operations are necessary to maintain the security and reliability of the BPS. Failure to consider the balancing resources within defined values, appropriately capturing and reporting of defined events to required organizations, inability or inadequate capabilities to monitor and analyze data needed to perform reliability functions, as well as ensuring proper communications with a predefined protocol may compromise the integrity and reliability of the BPS.	BAL-001-2 BAL-002-3 BAL-003-1.1 BAL-005-1 COM-002-4 EOP-004-4 IRO-001-4 IRO-002-6 IRO-006-5 IRO-008-2 IRO-009-2 IRO-014-3 IRO-017-1 IRO-018-1(i) TOP-001-4 VAR-001-5 VAR-002-4.1

Contact Information

Please submit questions to COPFAQ@nerc.net or to the Regional Entity Contact listed below.

North American Electric Reliability Corporation
Yvette Landin, Senior Advisor
Email: Yvette.Landin@nerc.net; Phone: 404-446-9638

Midwest Reliability Organization
Jeff Norman, Director of Compliance Monitoring
Email: Jeff.Norman@mro.net; Phone: 651-855-1703

Northeast Power Coordinating Council, Inc.
Jenifer Farrell, Director, Compliance Monitoring and IT
Email: jvallace@npcc.org; Phone: 917-934-7970

ReliabilityFirst
Anthony Jablonski, Manager of Risk Analysis and Mitigation
Email: anthony.jablonski@rfirst.org; Phone: 216-503-0693

SERC Reliability Corporation
Janice Carney, Senior Compliance Engineer
Email: jcarney@serc1.org; Phone: 704-770-8457

Texas Reliability Entity, Inc.
Jeff Hargis, Manager, Risk Assessment
Email: Jeff.Hargis@texasre.org; Phone: 512-583-4933

Western Electricity Coordinating Council
Ruchi Shah, Director, Entity Risk Assessment, & Registration
Email: rshah@wecc.org; Phone: 801-883-6881