NORTHEAST POWER COORDINATING COUNCIL, INC.

Introduction to Compliance Oversight Plans (COP)

December 9, 2020

Ben Eng
NPCC
Manager, Entity Risk Assessment

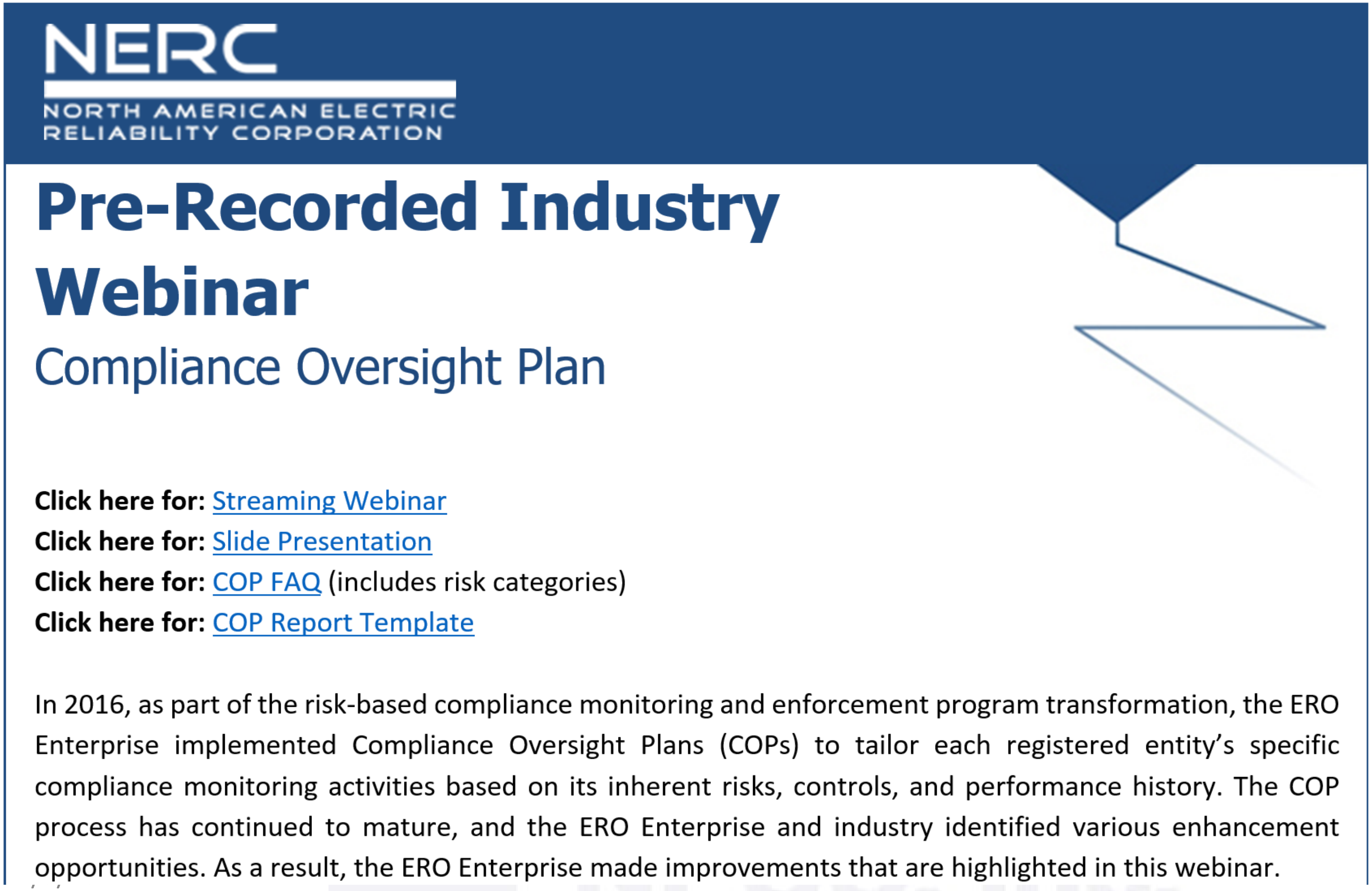
'Assuring BES Reliability through Risk and Controls Management '

Objectives

- Show where recent information regarding COPs may be found
- Describe the purpose, inputs, components and outputs of COPs
- Elaborate on the definitions and answers provided in the COP FAQs
- Describe the interactions between NPCC and Registered Entities to create and deliver the COP and ANL
- Demonstrate the above with a Process Flow Diagram showing the activities related to the creation and change management of entities’ COPs and its role in Compliance Monitoring and entity Continuous Improvement

Compliance Oversight Plan

Announced on Nov. 13, 2020 (email from Heather Miller/NERC)



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pre-Recorded Industry Webinar

Compliance Oversight Plan

Click here for: Streaming Webinar
Click here for: Slide Presentation
Click here for: COP FAQ (includes risk categories)
Click here for: COP Report Template

In 2016, as part of the risk-based compliance monitoring and enforcement program transformation, the ERO Enterprise implemented Compliance Oversight Plans (COPs) to tailor each registered entity's specific compliance monitoring activities based on its inherent risks, controls, and performance history. The COP process has continued to mature, and the ERO Enterprise and industry identified various enhancement opportunities. As a result, the ERO Enterprise made improvements that are highlighted in this webinar.

Highlights Enhanced COP Processes

Enhanced Analysis

Inherent & Performance Data

Analysis of inherent and performance data provides an understanding of an entity's overall inherent risk and performance profile

Targeted Oversight

Risk Categories

Selected risks provide a focus for an entity's continuous improvement & to Regional Entities for its compliance monitoring activities

Prioritized Monitoring

Oversight Strategies

Provide target interval frequency for oversight, primary monitoring tools, and informs annual planning

Standards to Risk

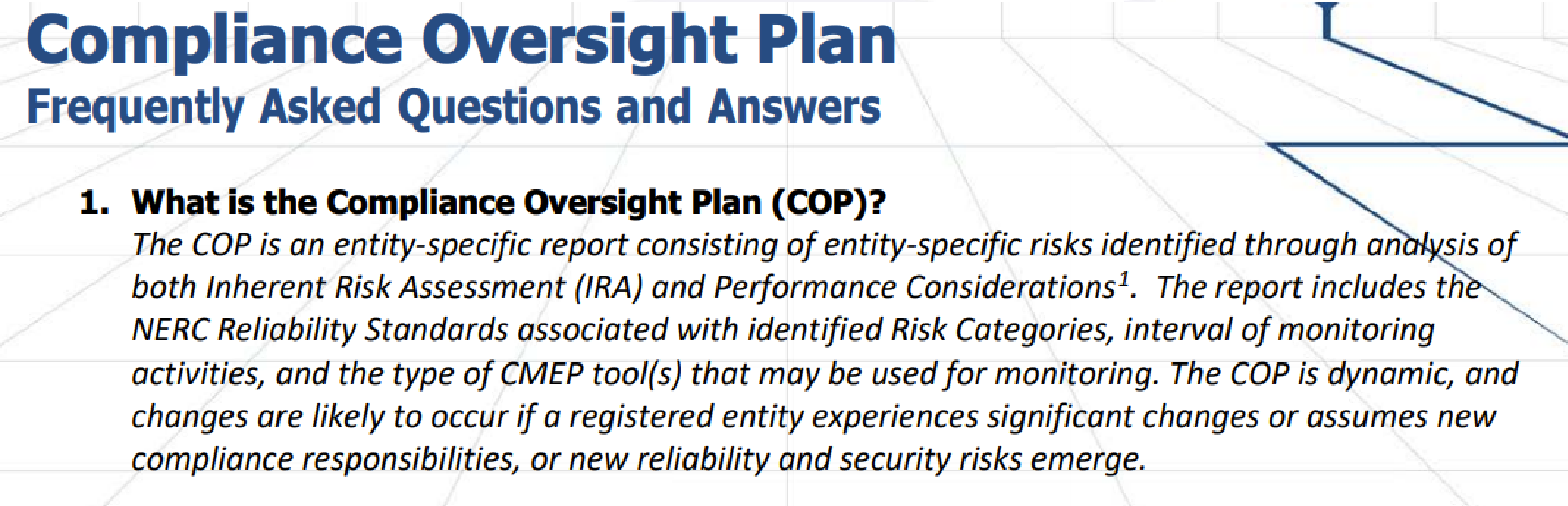
Appendix B

Provides Reliability Standards associated with the entity-specific risks. The scope of monitoring activities is derived from this list

COP Report

Common Template

One report to provide both inherent risk assessment results and the compliance oversight plan



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.

- Provides an oversight strategy with a target interval and frequency for oversight activities.
- Tailored to each entity's entity specific risks based on inherent and operational risks (the IRA, Performance Considerations), and associated Risk Categories.
- Is dynamic and requires change management to capture changes that may impact Reliability and Risks (See Question 5)

COP FAQs

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.

Implementation and release of COPs varies across the ERO Enterprise

COP Report

1. Purpose
2. Analysis and Results
3. Oversight Strategy

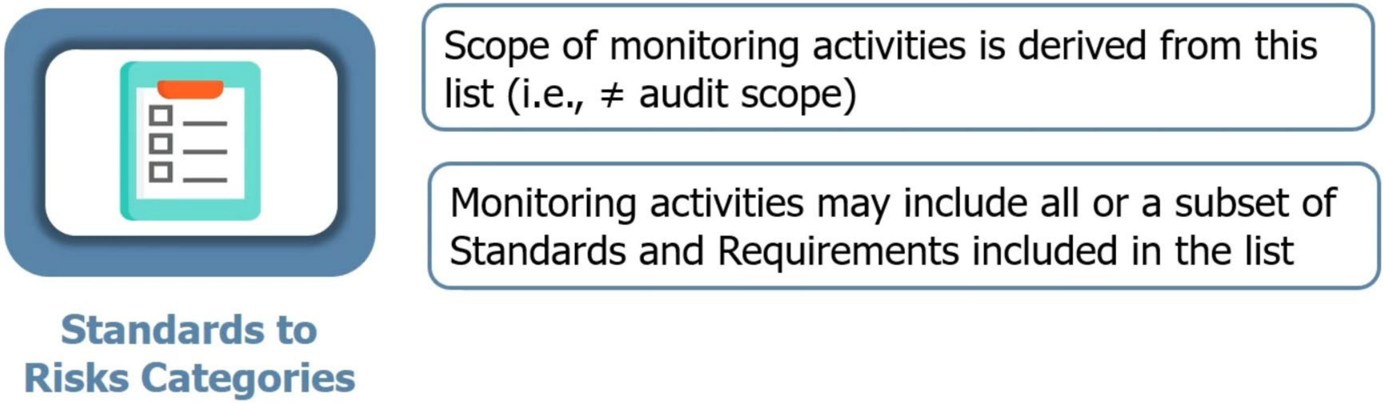
App. A: IRA Results Summary

App. B: Standards and Requirements for Monitoring

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.

COP FAQs

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.

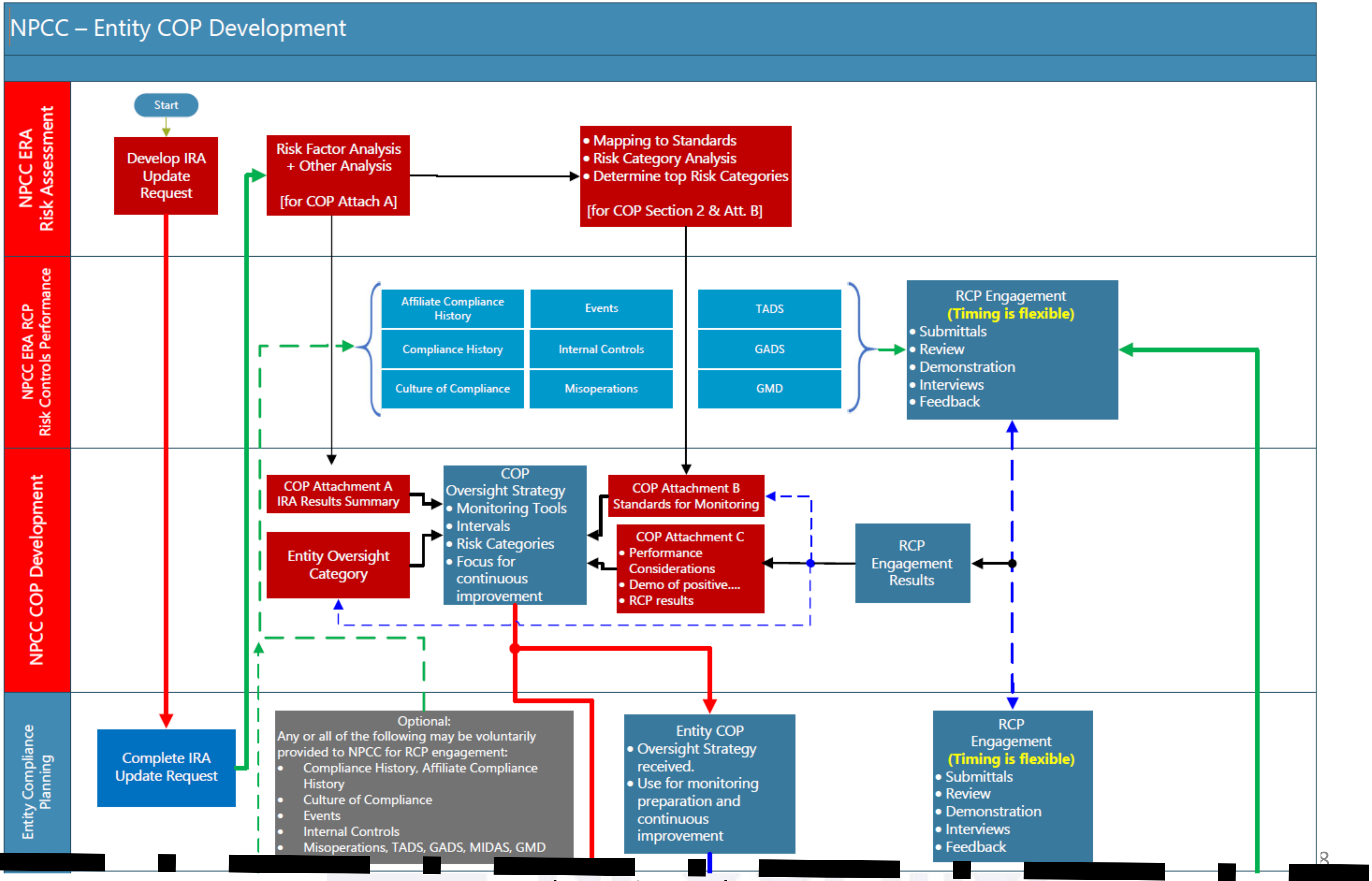


Standards to Risks Categories

Scope of monitoring activities is derived from this list (i.e., ≠ audit scope)

Monitoring activities may include all or a subset of Standards and Requirements included in the list

NPCC COP process flow diagram (upper)



NPCC – Entity COP Development

NPCC ERA Risk Assessment

Start

Develop IRA Update Request

Risk Factor Analysis + Other Analysis

[for COP Attach A]

- Mapping to Standards
- Risk Category Analysis
- Determine top Risk Categories

[for COP Section 2 & Att. B]

NPCC ERA RCP Risk Controls Performance

Affiliate Compliance History

Events

TADS

Compliance History

Internal Controls

GADS

Culture of Compliance

Misoperations

GMD

RCP Engagement

(Timing is flexible)

- Submittals
- Review
- Demonstration
- Interviews
- Feedback

NPCC COP Development

COP Attachment A IRA Results Summary

Entity Oversight Category

COP Oversight Strategy

- Monitoring Tools
- Intervals
- Risk Categories
- Focus for continuous improvement

COP Attachment B Standards for Monitoring

COP Attachment C

- Performance Considerations
- Demo of positive....
- RCP results

RCP Engagement Results

Entity Compliance Planning

Complete IRA Update Request

Optional:

Any or all of the following may be voluntarily provided to NPCC for RCP engagement:

- Compliance History, Affiliate Compliance History
- Culture of Compliance
- Events
- Internal Controls
- Misoperations, TADS, GADS, MIDAS, GMD

Entity COP

- Oversight Strategy received.
- Use for monitoring preparation and continuous improvement

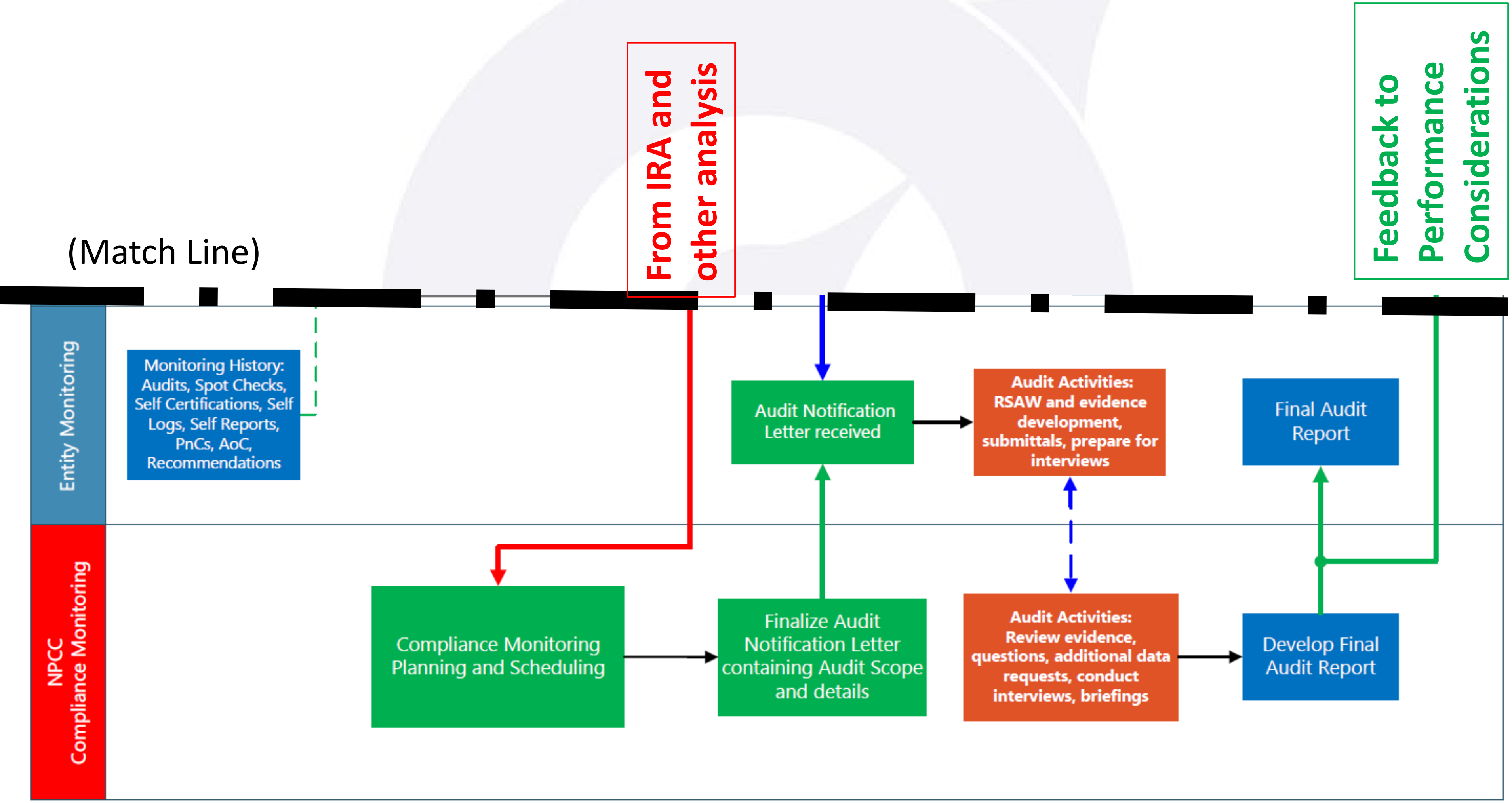
RCP Engagement

(Timing is flexible)

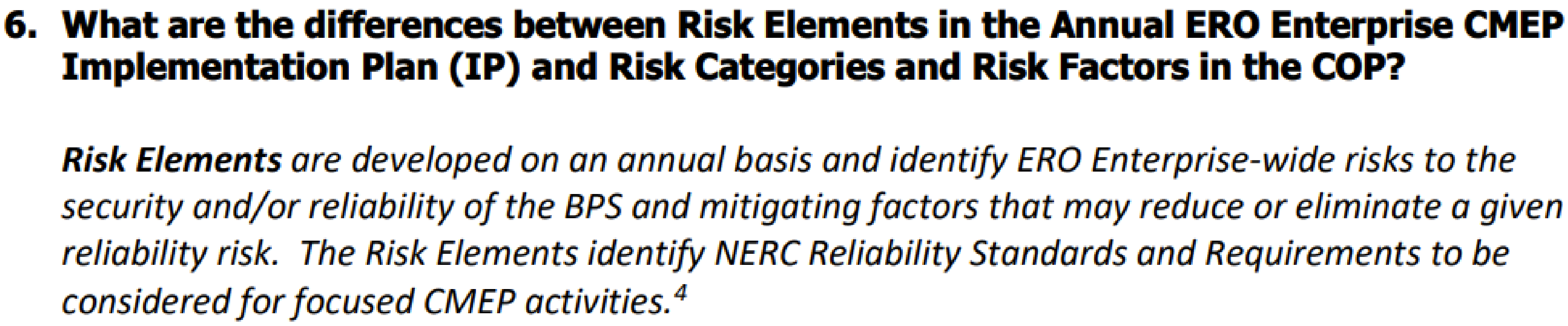
- Submittals
- Review
- Demonstration
- Interviews
- Feedback

(Match Line)

NPCC COP process flow diagram (lower)


(Match Line)
From IRA and other analysis
Feedback to Performance Considerations
Entity Monitoring
NPCC Compliance Monitoring
Monitoring History: Audits, Spot Checks, Self Certifications, Self Logs, Self Reports, PnCs, AoC, Recommendations
Audit Notification Letter received
Audit Activities: RSAW and evidence development, submittals, prepare for interviews
Final Audit Report
Compliance Monitoring Planning and Scheduling
Finalize Audit Notification Letter containing Audit Scope and details
Audit Activities: Review evidence, questions, additional data requests, conduct interviews, briefings
Develop Final Audit Report

Risk Elements, Risk Categories and Risk Factors (oh my!)

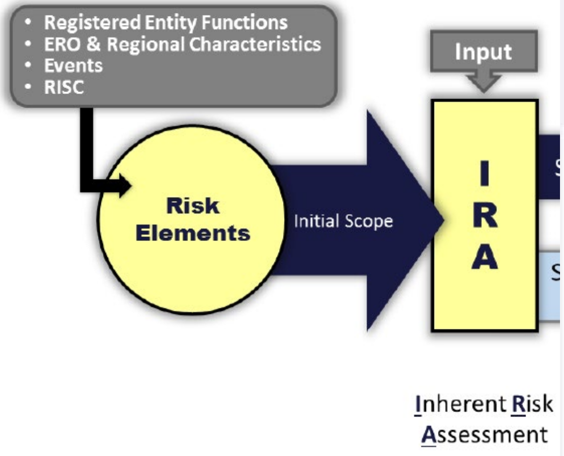


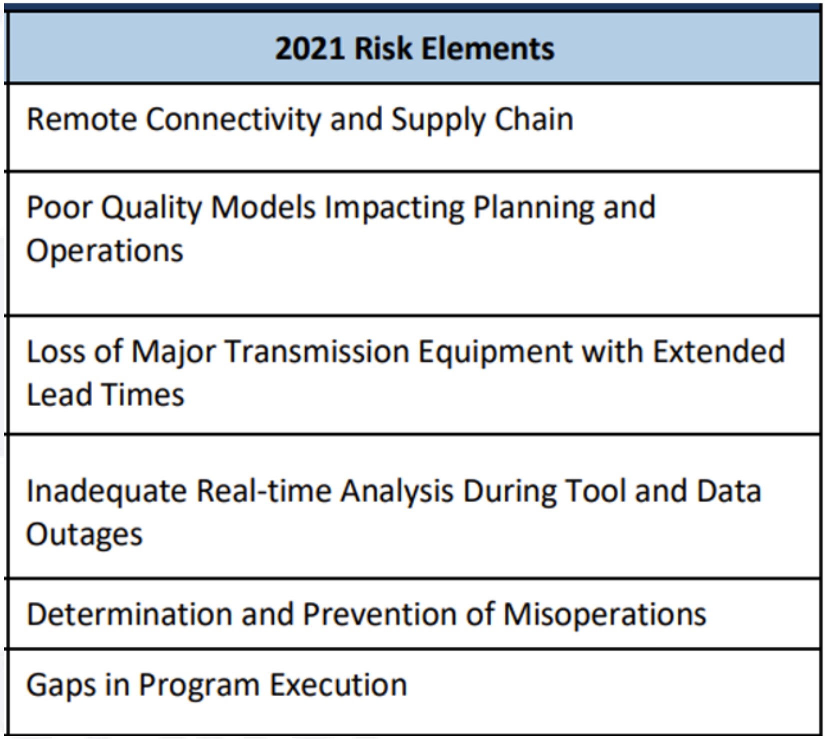
6. What are the differences between Risk Elements in the Annual ERO Enterprise CMEP Implementation Plan (IP) and Risk Categories and Risk Factors in the COP?

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 Elements are listed in the ERO Annual CMEP Implementation Plan (IP)

There are 6 Risk Elements for 2021

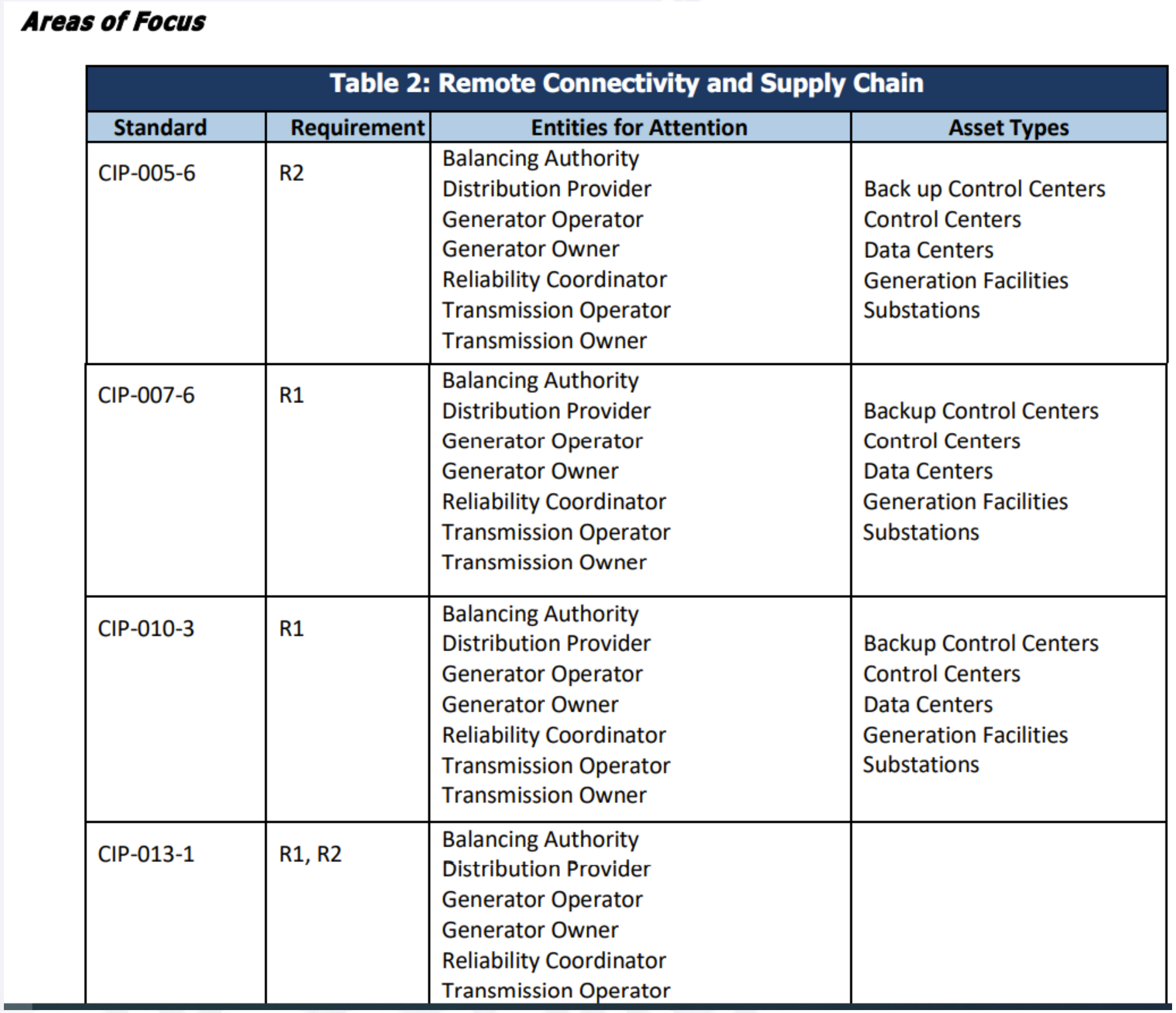




2021 Risk Elements
Remote Connectivity and Supply Chain
Poor Quality Models Impacting Planning and Operations
Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages
Determination and Prevention of Misoperations
Gaps in Program Execution

Risk Elements

- Each of the 6 Risk Elements is described in greater detail and lists the NERC Reliability Standards that are Areas of Focus
- Table 2 shown.
- See CMEP IP for Tables 3 thru 7 for Areas of Focus associated with the Risk Elements listed on previous page



Areas of Focus

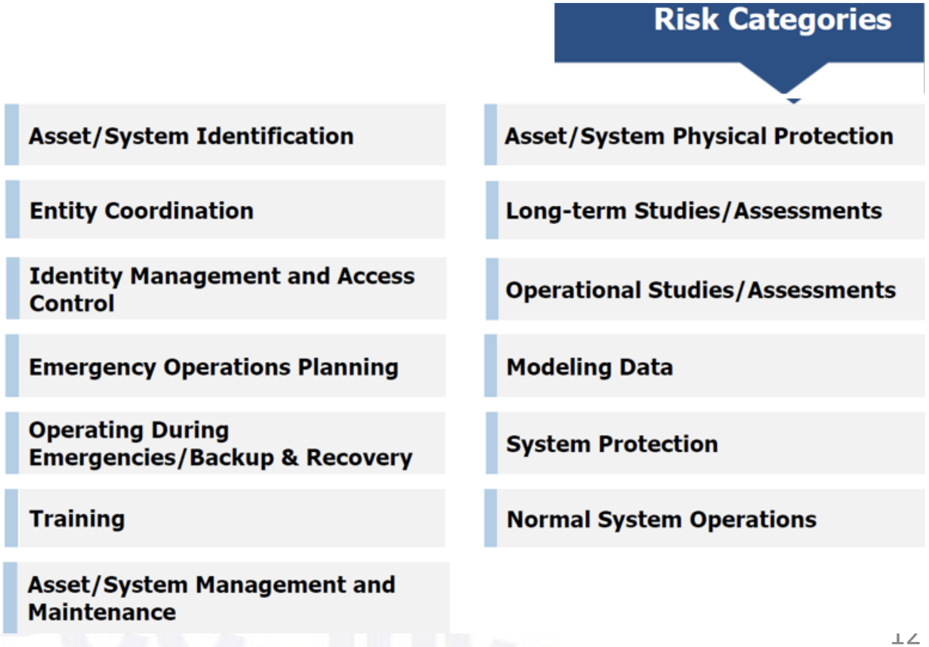
Table 2: Remote Connectivity and Supply Chain

Standard	Requirement	Entities for Attention	Asset Types
CIP-005-6	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Back up Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-007-6	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-010-3	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-013-1	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator	

Risk Categories

***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.*

- There are 13 Risk Categories to categorize the Standards/Requirements for monitoring listed in Appendix B of the COP

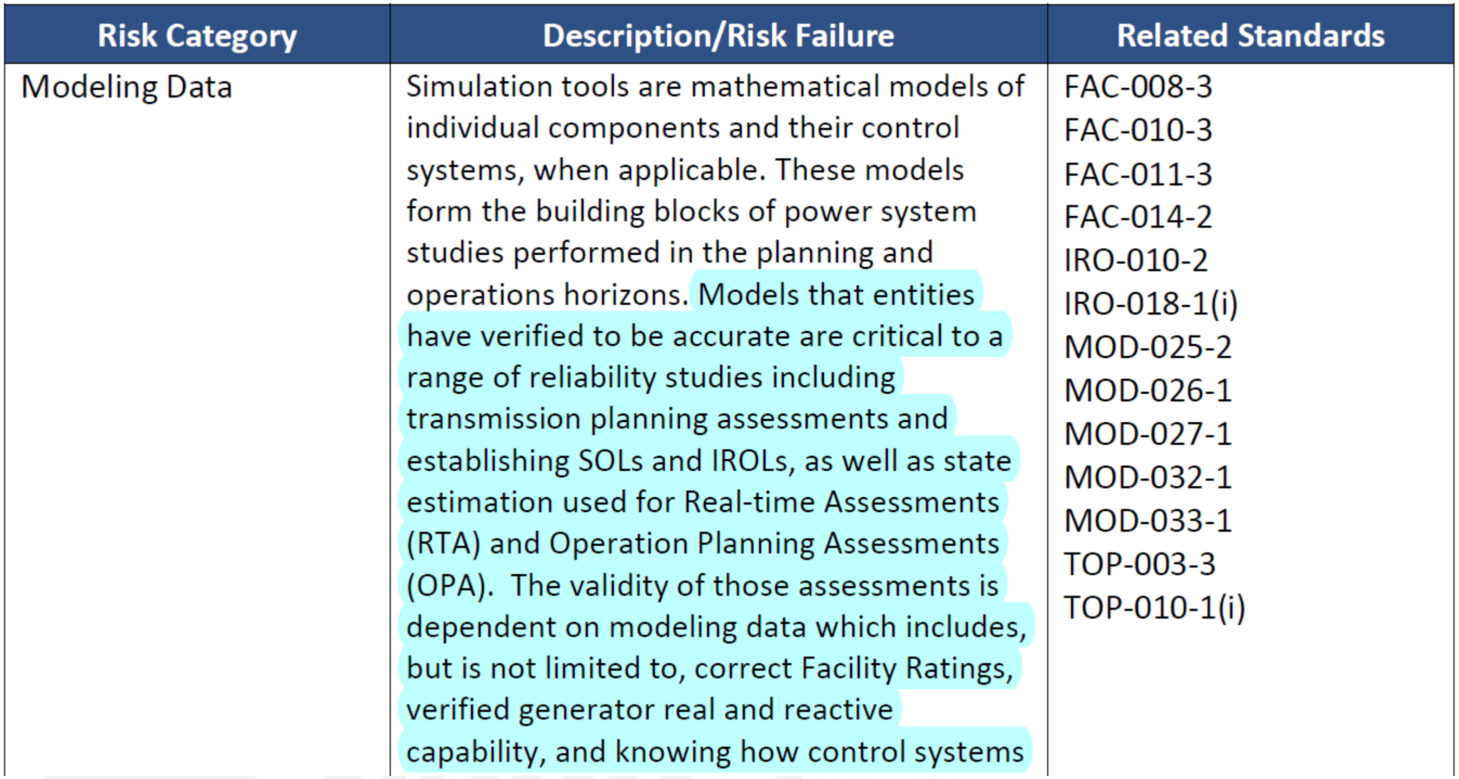


Risk Categories

- Asset/System Identification
- Entity Coordination
- Identity Management and Access Control
- Emergency Operations Planning
- Operating During Emergencies/Backup & Recovery
- Training
- Asset/System Management and Maintenance
- Asset/System Physical Protection
- Long-term Studies/Assessments
- Operational Studies/Assessments
- Modeling Data
- System Protection
- Normal System Operations

Risk Categories

- This is an example of the *Modeling Data* Risk Category and the list of related NERC standards that would be candidates for monitoring. This could appear in COP Appendix B if the *Modeling Data* Risk Category is one of your higher Risk Categories.



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	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 Factors

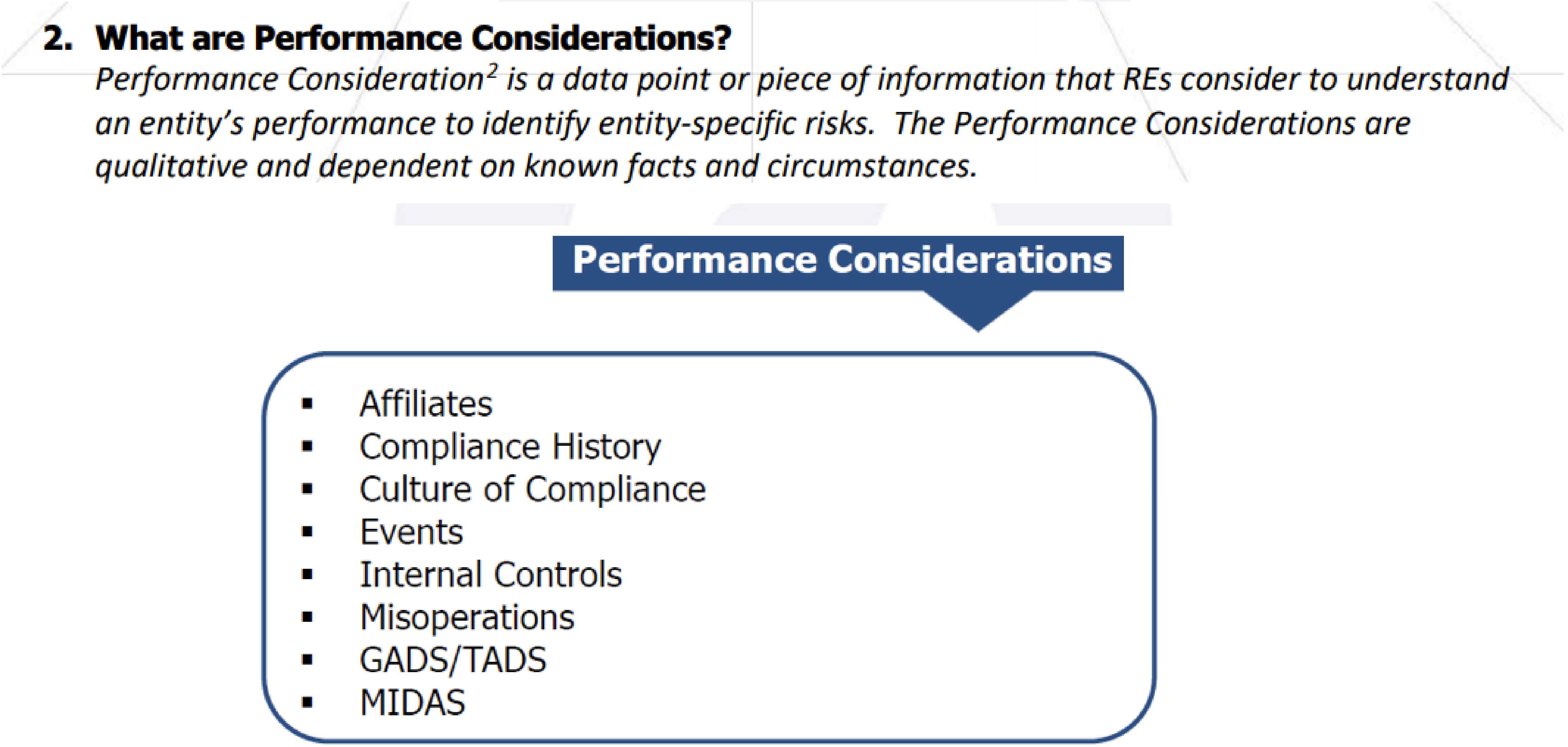
***Risk Factors** are measureable aspects used during an IRA to identify a registered entity's risk characteristics related to Standards/Requirements that are inherent to a registered entity's configuration and may impact the reliability of the BPS.*

- There are 18 ERO Risk Factors.
- These may look familiar to you because they are listed in the NPCC IRA Update request template.
- Your answers to the Risk Factor questions help create Appendix A, *Inherent Risk Assessment (IRA)* to the COP.

ERO Enterprise Risk Factors

- CIP-Impact Rating Criteria
- ICCP Connectivity
- Load
- Transmission Portfolio
- Critical Transmission
- Voltage Control
- Largest Generator Facility
- Total Generation Capacity
- Variable Generation
- BA Coordination
- Planned Facilities
- RAS/SPS
- Workforce Capability
- Monitoring & Situational Awareness Tools
- System Restoration
- UFLS Equipment
- UFLS Development and Coordination
- UVLS

COP FAQs



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.

Performance Considerations

- Affiliates
- Compliance History
- Culture of Compliance
- Events
- Internal Controls
- Misoperations
- GADS/TADS
- MIDAS

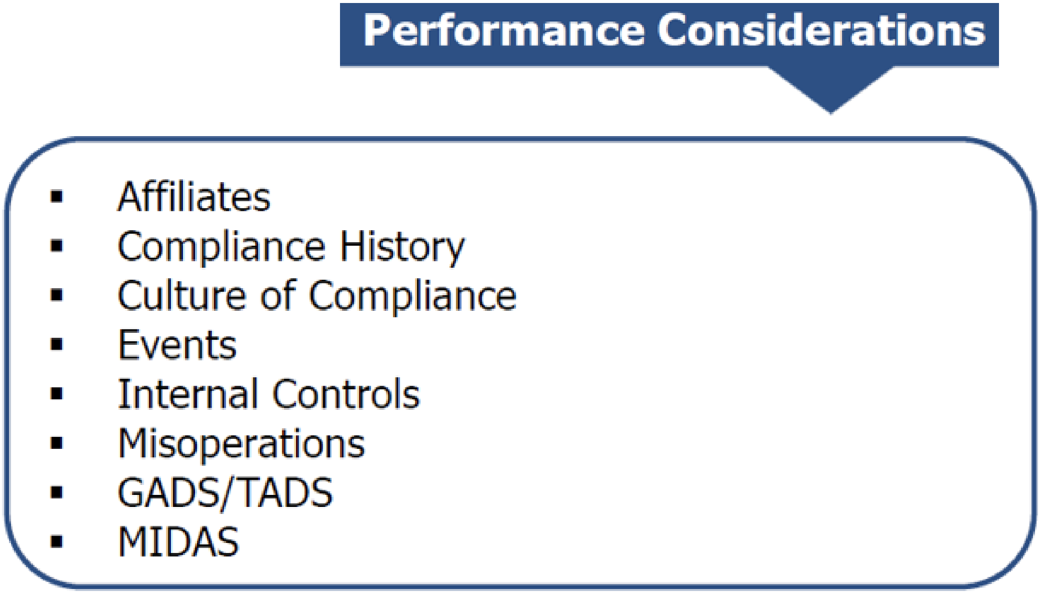
Demonstration of Positive Performance

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.

- There are 8 Performance Considerations listed.
- Unlike Risk Factors, these are not quantitative.
- Performance Considerations are ***qualitative*** and require a thorough understanding and analysis of how they help the entity mitigate risks to Reliability.



Performance Considerations

- Affiliates
- Compliance History
- Culture of Compliance
- Events
- Internal Controls
- Misoperations
- GADS/TADS
- MIDAS

Positive Performance and Oversight Stategy

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.

- Entity demonstrating Positive Performance in vast majority of Performance Considerations may:
- be moved to an Oversight Category with longer interval between monitoring
- allow standards to use different monitoring tool (Spot Check or Self Certification instead of audit)
- change one or more Risk Categories shown in Appendix B

Performance Considerations

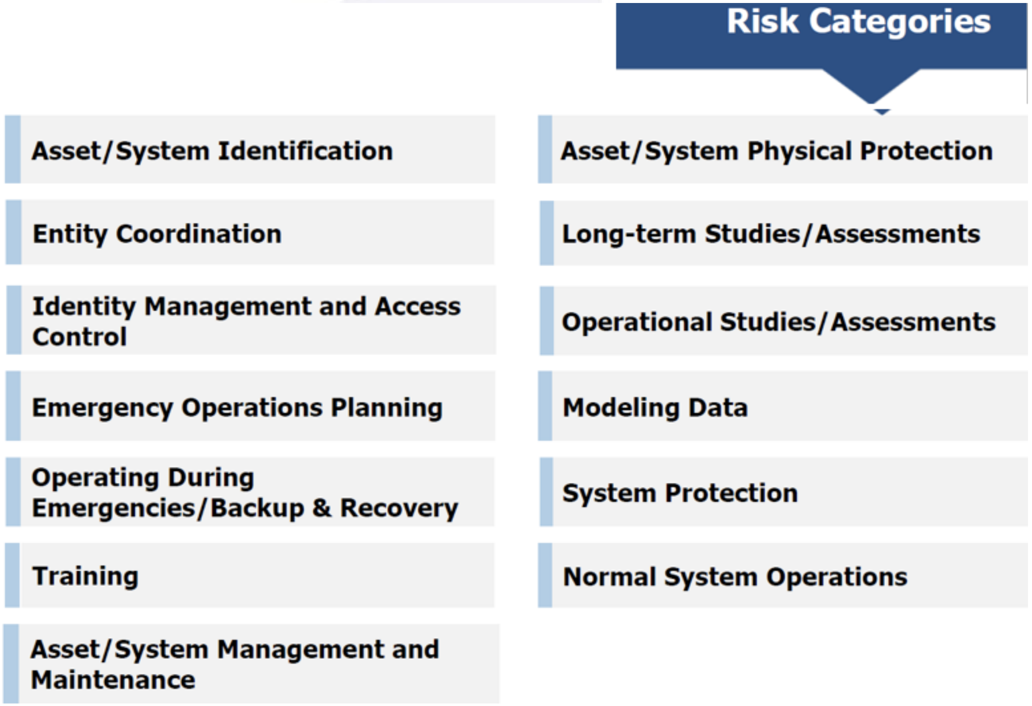
- Affiliates
- Compliance History
- Culture of Compliance
- Events
- Internal Controls
- Misoperations
- GADS/TADS
- MIDAS

Risk Categories

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.

- There are 13 Risk Categories shown at the right.
- See the COP FAQ document, pages 3 – 10 for a detailed list of NERC standards within each Risk Category
- Some (not all) of the Risk Categories would appear in Appendix B of the COP to provide focus to the entity to address entity specific risks to Reliability and Resilience.

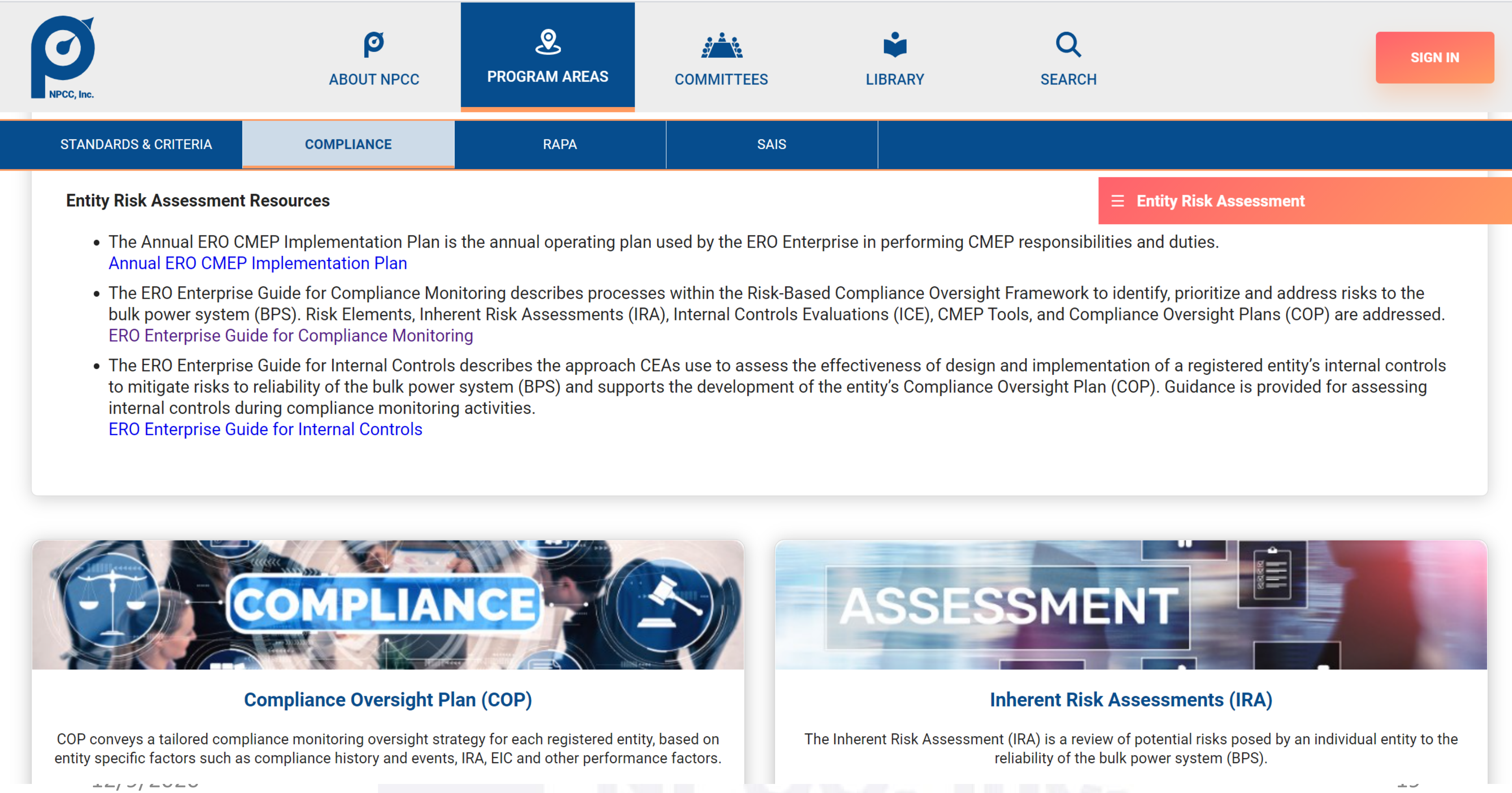


Risk Categories

- Asset/System Identification
- Entity Coordination
- Identity Management and Access Control
- Emergency Operations Planning
- Operating During Emergencies/Backup & Recovery
- Training
- Asset/System Management and Maintenance
- Asset/System Physical Protection
- Long-term Studies/Assessments
- Operational Studies/Assessments
- Modeling Data
- System Protection
- Normal System Operations

NPCC ERA Website

https://www.npcc.org/program-areas/compliance/entity-risk-assessment



Entity Risk Assessment Resources

- The Annual ERO CMEP Implementation Plan is the annual operating plan used by the ERO Enterprise in performing CMEP responsibilities and duties.
  Annual ERO CMEP Implementation Plan
- The ERO Enterprise Guide for Compliance Monitoring describes processes within the Risk-Based Compliance Oversight Framework to identify, prioritize and address risks to the bulk power system (BPS). Risk Elements, Inherent Risk Assessments (IRA), Internal Controls Evaluations (ICE), CMEP Tools, and Compliance Oversight Plans (COP) are addressed.
  ERO Enterprise Guide for Compliance Monitoring
- The ERO Enterprise Guide for Internal Controls describes the approach CEAs use to assess the effectiveness of design and implementation of a registered entity's internal controls to mitigate risks to reliability of the bulk power system (BPS) and supports the development of the entity's Compliance Oversight Plan (COP). Guidance is provided for assessing internal controls during compliance monitoring activities.
  ERO Enterprise Guide for Internal Controls

Compliance Oversight Plan (COP)

COP conveys a tailored compliance monitoring oversight strategy for each registered entity, based on entity specific factors such as compliance history and events, IRA, EIC and other performance factors.

Inherent Risk Assessments (IRA)

The Inherent Risk Assessment (IRA) is a review of potential risks posed by an individual entity to the reliability of the bulk power system (BPS).

Recommended Next Steps

- Review the ERO information on COPs
- Review the NPCC Process Flow Diagram to understand the COP development and change management process.
- Look at your COP Attachment B when you receive it.
- Use it to plan for your next audit and other monitoring.
- Review Performance Considerations applicable to your organization.
- Assess your processes relative to the Performance Considerations as a self-assessment exercise.
- Capture and assess your controls for high risk activities as a means of continuous self-improvement.
- Consider contacting NPCC to participate in a Risk Controls & Performance engagement well in advance of an audit.

Thank you

My name is Ben Eng

- I can be reached at beng@npcc.org
- Or text me at 917-828-4980

- Thank you for your attention!