TEXAS RE

Engagement Objectives

Sridhar Pushpavanam
Senior Risk Assessment Engineer

August 27, 2026

Agenda

- Compliance Engagement Objectives
- Engagement Scopes
- Engagement Timelines
- Closing the Loop

Compliance Engagement Objectives

PURPOSE OF COMPLIANCE ENGAGEMENTS

Reduce risks to the reliability and security of the North American BPS through risk-based oversight, promote continuous improvement and foster shared understanding of compliance goals

The new engagement objectives section in audit and spot-check handoffs provides insights on

Scope Rationale

Why each Requirement was selected for the engagement

Alignment with COP and ERO Priorities

How the scope ties to your Compliance Oversight Plan (COP) and the Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP)

Focus Areas and Future Risk Reduction

What auditors look for, and the internal controls that reduce future risk

Engagement Scopes

Performance Data

- Compliance History
- Misoperations
- Events
- GADS/TADS etc.

COP

- Inherent Risk Assessment (IRA)
- Risk categories
- Monitoring period

CMEP IP

- ERO Risk Priorities
- Annual Risk Elements

Risk-based scope (specific Standards and targeted Requirements)

Your scope comes from your COP, performance data, and ERO priorities – it is not selected at random

Engagement Timelines

Risk Assessment
- Refresh IRA/COP/performance data
- Review/finalization of scope

Entity Handoff Call (around T-135)
- Scope
- Engagement objectives
- Engagement timelines/processes

ANL (T-120)
Audit Notification Letter available in Align

Engagement start date
T-0: Audit or spot-check begins

You see the scope and the engagement objectives at the handoff call, typically about 135 days before the engagement starts

T-# = calendar days prior to the engagement start date. ANL = Audit Notification Letter.

Example – Entity Background

Sample scenario for illustrative purposes only

- **Entity is a GO, GOP, TO, TOP**
- **Key entity risks identified in IRA/performance data**
  - Owns and operates generation in areas prone to extreme cold weather; generation impacted during winter storm Fern
  - Medium impact TOP Control Center; updated its emergency management system (EMS) recently, including Electronic Security Perimeter (ESP)
  - CIP security risks identified at low-impact substations
  - Added multiple inverter based resource (IBR) generating units
  - Entity had repeated difficulties maintaining generator voltage within the specified band

Example – Entity Background

Key risks from the COP

- Asset/system management and Maintenance
- Identity management and access control
- Emergency operations planning
- Modeling data
- Normal system operations

Example – Entity Background

Key risks applicable to entity from 2026 CMEP IP

- Remote connectivity
- Supply chain
- Physical security
- Facility ratings
- Grid transformation
- Extreme weather response

On-site audit for the GO, GOP, TO, TOP functions

Scope

- CIP-003-9 R2 (TO)
- CIP-005-7 R2, R3 (TOP)
- CIP-013-2 R1, R2 (TOP)
- EOP-012-3 R4 (GO)
- EOP-012-3 R5 (GO, GOP)
- FAC-008-5 R6 (GO)
- VAR-002-4.1 R2 (GOP)

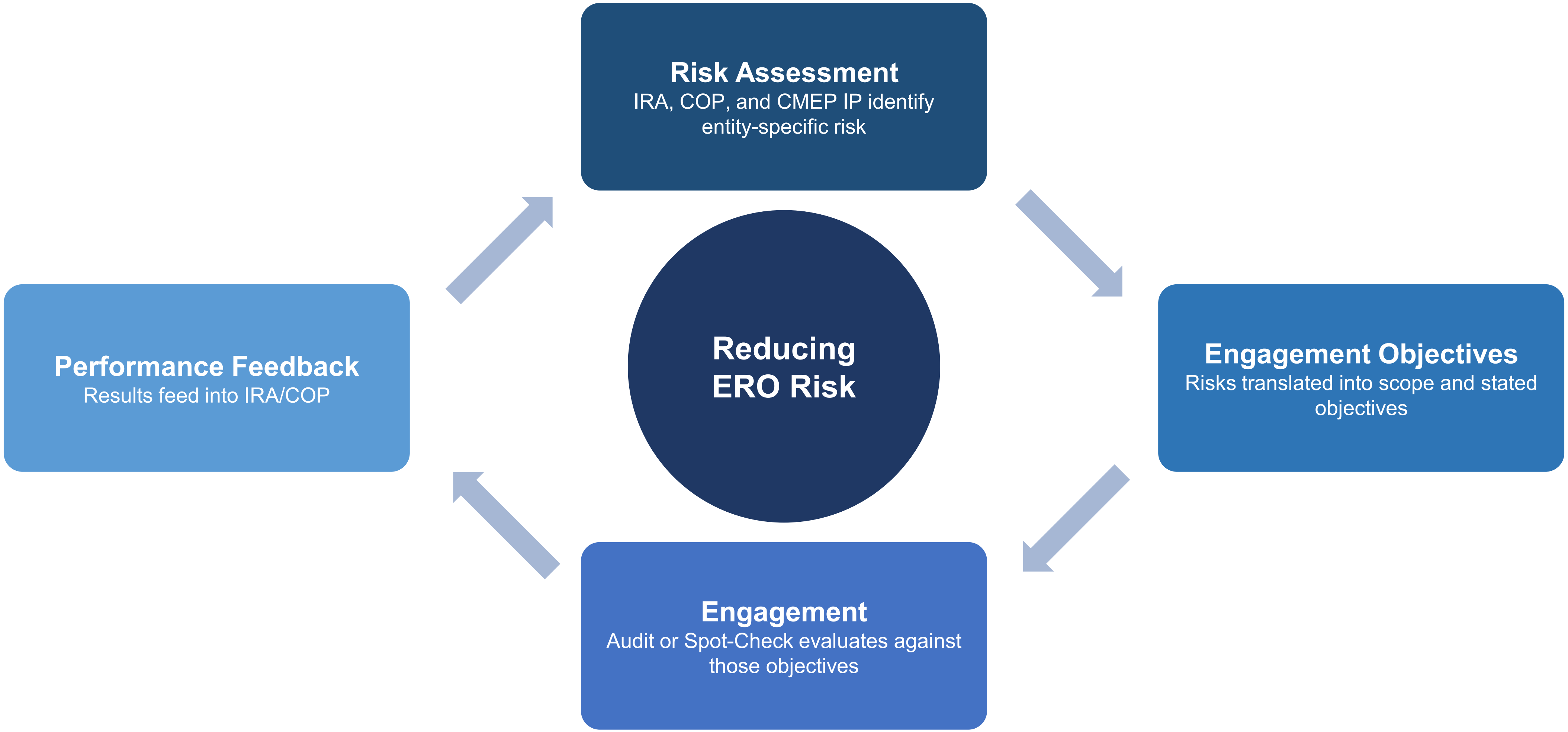
Example – Engagement Objectives: O&P

Risk Category	Source of Risk Area	Residual Risk Objective(s)	Audit Scope
Emergency Operations Planning	• 2026 CMEP IP • Large installed generation in ERCOT weather zones prone to very cold temperatures during winter	Confirm the cold weather plan covers freeze protection for every critical component on every unit, that generator performance is reviewed annually to update plans and operator training, and that internal controls manage generation risk at Extreme Cold Weather Temperature (ECWT).	EOP-012-3 R4, R5
Modeling Data	• 2026 CMEP IP • Added multiple IBR generating units during audit period	Confirm clear ownership to review, update, and communicate required operational data, and explicit responsibility to verify and maintain accurate Facility ratings	FAC-008-5 R6
Normal System Operations	• Observed generation voltage performance	Review internal controls for maintaining the voltage schedule established by the TOP, including processes to review voltage deviations and train personnel	VAR-002-4.1 R2

Example – Engagement Objectives: CIP ...continued

Risk Category	Source of Risk Area	Residual Risk Objective(s)	Audit Scope
Asset/System Management and Maintenance	• 2026 CMEP IP • Multiple event(s)	Confirm security management controls are consistent, sustainable, and actively protecting BES Cyber Systems at low-impact substations	CIP-003-9 R2
Identity Management and Access Control	• 2026 CMEP IP • EMS upgrade	Ensure entity implemented its supply chain cyber security risk management plan given the recent EMS upgrade. Validate that entity has appropriate internal controls in place to protect its BCS against compromise	CIP-005-7 R2, R3 CIP-013-2 R1, R2

Engagement Objectives: Closing the Loop



Wrap-up

Applies to Audits and Spot-Checks only

Scope is locked once Risk Lead communicates it

Auditors may expand scope as new risks emerge

Texas RE Contacts

Rashida Caraway
Manager, Risk Assessment
Rashida.Caraway@texasre.org

Sridhar Pushpavanam
Senior Risk Assessment Engineer
Sridhar.Pushpavanam@texasre.org

Questions?