



**TEXAS RE**

# **2023 ERO Implementation Plan**

**Rashida Caraway  
Manager, Risk Assessment  
Texas Reliability Entity**

**December 18, 2023**

# CMEP Implementation Plan (CMEP IP) Purpose

Public

- ❑ Reflects ERO and Regional Entity-specific risk elements that regions prioritize for oversight of registered entities
- ❑ Developed by NERC and the Regional Entities
- ❑ Four risk priorities the CMEP IP manages
  1. Changing Resource Mix
  2. Cybersecurity Vulnerabilities
  3. Resource Adequacy and Performance
  4. Critical Infrastructure Interdependencies



## Risk Elements Developed Using:

- Compliance findings
- Recent event analysis
- Data analysis
- Committees
- Publications

## Risk Elements are Considered When Regions:

- Complete an Inherent Risk Assessment
- Complete a Compliance Oversight Plan
- Scope an engagement
  - Engagement team may use to focus on sampling and internal controls



# What's New with Risk Elements?

2023	2024
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
N/A	<b>Physical Security</b>
Incident Response	Incident Response
Stability Studies	Stability Studies
Inverter-Based Resources	Inverter-Based Resources
Facility Ratings	Facility Ratings
Cold Weather Response	<b>Extreme Weather Response</b>



# Remote Connectivity

- Focuses on the human element of security
- How do entities manage the risk of remote connectivity and the complexity of the tasks the individuals perform?

Standard	Requirement
CIP-005-7	R2, R3
CIP-007-6	R3
CIP-012-1	R1





# Supply Chain

Public

- ❑ A growing risk and focal point
- ❑ Various publications that highlight vendors, services, and products widely used

Standard	Requirement
CIP-010-4	R1
CIP-013-2	R1, R2



- Incidents increasing
- Many of the attacks have been against substations or distribution infrastructure
- Potential use of drones for attacks



Standard	Requirement
CIP-014-3	R4, R5



## Slido Question

**Physical security is not related to cyber-security risks.**

**True or False?**





# Incident Response

- ❑ Efforts underway to develop cyber tools that should assist industry in enhancing preparation and reaction plans
- ❑ Having and implementing a Cyber Security Incident response plan is important



Standard	Requirement
CIP-008-6	R1, R2, R3



# Stability Studies

- ❑ Focuses on how the changing resource mix impacts operational and transmission planning
- ❑ Reports have highlighted insufficient model quality checks

Standard	Requirement
CIP-014-3	R1
TPL-001-4 TPL-001-5.1	R4, R6



## Recent events highlighted IBR risks

- Ride-through capability during normal fault events
- Need to accurately model IBR characteristics
- Recent related NERC Alert

Standard	Requirement
FAC-001-4	R1, R2
FAC-002-4	R1, R2
MOD-026-1	R2
PRC-024-3	R1, R2



# Facility Ratings

- ERO has released a guide on related best practices
- ERO is understanding more about controls entities have in place



Standard	Requirement
FAC-008-6	R6





# Extreme Weather Response

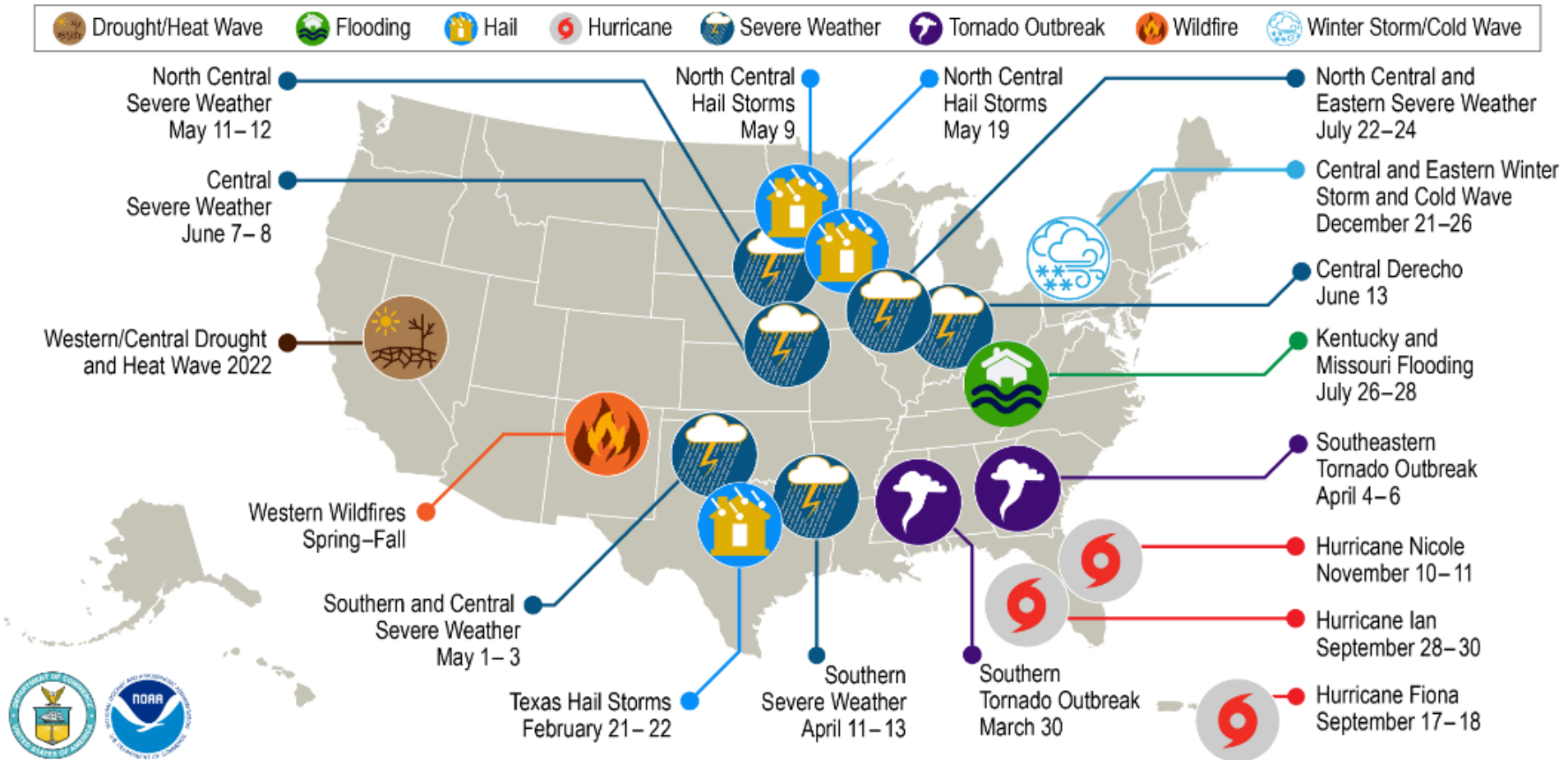
- Replaces Cold Weather Response Risk Element
- Extreme heat events have had impact on BPS

Standard	Requirement
EOP-011-2	R1, R2, R3, R6, R7, R8
EOP-012-1	R1, R2, R3, R4, R5, R6, R7
TPL-007-4	R1, R2, R4, R5, R7





# Extreme Weather Response: 2022 U.S. Weather and Climate Disasters



This map denotes the approximate location for each of the 18 separate billion-dollar weather and climate disasters that impacted the United States in 2022.

Source: NOAA National Centers for Environmental Information (NCEI) U.S. Billion-Dollar Weather and Climate Disasters (2023)  
<https://www.ncei.noaa.gov/access/billions/>

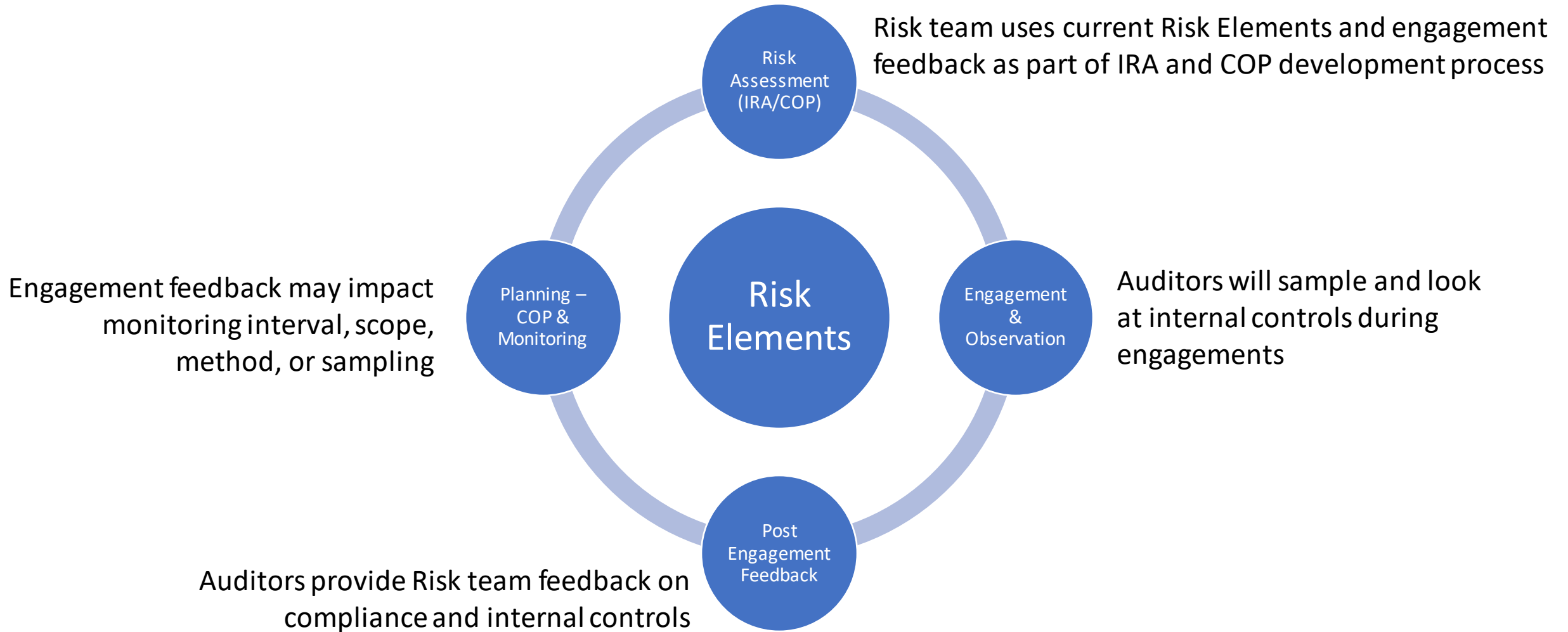


## Slido Question

Which Risk Element do you think poses the most risk to your registered entity(ies)?

- Remote Connectivity*
- Supply Chain*
- Physical Security*
- Incident Response*
- Stability Studies*
- Inverter-Based Resources*
- Facility Ratings*
- Extreme Weather Response*





# Questions?



**TEXAS RE**

Ensuring electric reliability for Texans