

# Reliability & Security Oversight Update

**Mailee Cook**

*Training and Outreach Specialist*

**Electric Reliability  
& Security for the West**

July 16, 2026



# **Future of Path Ratings in the Western Interconnection**

**In-Person | 10 a.m.–5 p.m. MDT  
July 23, 2026**





# **Reliability in the West**

**WECC**

**Reliability in the West Discussion Series:  
Cyber- and Physical Security**  
Wednesday, August 5, 2026  
11 a.m.—noon MDT



**Salt Lake City, Utah | August 11–13, 2026**



# **Grid Fundamentals**

**WECC**

**August 18–19, 2026**  
**Salt Lake City, Utah**



**Reliability & Security  
Workshop**

**WECC**

**October 27–28, 2026  
Scottsdale, Arizona**

**WICF  
October 29**

# Meeting Disclosures

---

- Participants are reminded of their obligations under the WECC Antitrust Policy and the NERC Antitrust Compliance Guidelines. The full Antitrust Statement is attached to this meeting's agenda.
- This meeting is public – confidential or proprietary information should not be discussed in open session.
- This meeting is being recorded and may be posted publicly. By participating, you give your consent for your name, voice, image, and likeness to be included in the recording.
- WECC strives to ensure the information presented today is accurate and reflects the views of WECC; however, all interpretations and positions are subject to change.
- If you have any questions, please contact WECC's legal counsel.

# Agenda

---

- NERC and WECC Happenings — Fahad Ansari, WECC
- New Align and SEL Reference Guide — Jessica King, WECC
- Standards Update — Donovan Crane, WECC
- Computational Load Entity Standard Drafting Team Update — Mark Rogers, WECC
- Internal Controls Maturity Self-assessment — Molly Elliott, WECC

# NERC and WECC Happenings

**Fahad Ansari**

*Senior Technical Advisor, Oversight Planning*

**Electric Reliability  
& Security for the West**

July 16, 2026

# NERC Happenings

---

- Reliability Standard Updated Version
  - [CIP-012-2](#) – Cyber Security–Communications between Control Centers
    - Effective July 1, 2026
- Reliability Standard Audit Worksheets
  - New CIP Virtualization [RSAWs](#) posted
- Reliability Insights
  - [Supply Chain Security](#)
- GADS Conventional and Wind/Solar Training
  - July 7–9 in-person training course for GADS reporting
- Computational Loads Level 3 Alert Webinar
  - [July 8 webinar recording posted](#)



# WECC Happenings

---

- Risk Management Program Virtual Town Hall
- [New Entity Resource Center](#)

# New Align and SEL Reference Guide

**Jessica King**  
*Business Analyst*

**Electric Reliability  
& Security for the West**

July 16, 2026

# New Align and SEL Reference Guide

## WECC ALIGN AUDIT & SPOT CHECK



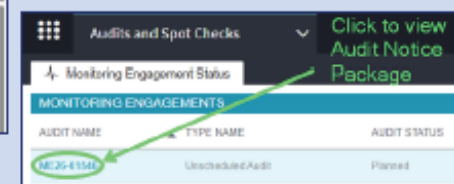
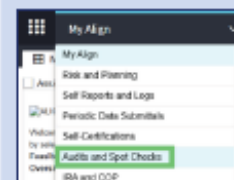
## REFERENCE GUIDE

### Purpose

This guide will help entities who are selected for a monitoring activity to find their Audit Notice Package (ANP) in Align, and it will outline WECC's Align audit and spot check process.

### Finding your Monitoring Engagement in Align

- Log in to [Align](#).
- Go to the **My Align** dropdown and select **Audits and Spot Checks**.
- **"ME"** is your monitoring engagement with the year.



#### Need Access to Align?

Align users must have an ERO Portal account.

Follow the [Align User Guide](#) to

- Set up account, p. 3-27
- Request access, p. 28-34
- Approve access, p. 35-37

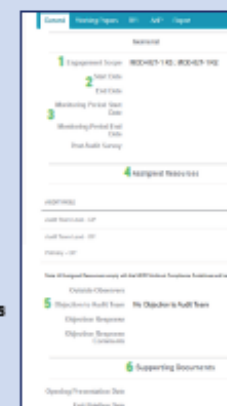
Note: Align permission are automatically given to the Primary Compliance Contact (PCC) of a registered entity.

### Reviewing the General Tab

The ANP opens to the General tab. Any changes to the audit team or scope will be shown on this tab.

The General tab contains:

1. Scope
2. Start and end dates
3. Monitoring period
4. Assigned resources (audit team)
5. Objections
6. Supporting documents (audit report upload here)



#### Objections to Audit Team

- Click **Edit** at the bottom of the window.
- Select **Objection to Audit Team** in the dropdown.
- Write your objections in the **Justification of Objection** box.



# Standards Update

**Donovan Crane**  
*Manager, Standards*

**Electric Reliability  
& Security for the West**

July 16, 2026



## Standards Update – NERC Projects

2023-09 Risk Management  
for Third-party Cloud Services

- Informal comment period to start week of July 6

2025-04 Order No. 901  
Planning Studies

- Final Ballot open through July 21

2022-05 Modifications to  
CIP-008 Reporting Threshold

- Formal comment period and initial ballot starting week of July 20

2025-01 Cold Weather  
Canadian Variance

- Formal comment period and initial ballot starting the week of July 13

ROP and SPM revisions

- Tentative to go out for comment and Ballot first week of September

# Standards Update – WECC Projects



[WECC-0142: Request to Retire BAL-002-WECC-3, Contingency Reserve](#)

FERC accepted the request to retire. Officially retired as of July 1, 2026



[WECC-0157: PRC-006-5 Automatic Underfrequency Load Shedding, Update to the WECC Regional Variance](#)

WSC accepted and voted to send to WECC's board for disposition. Anticipated to presented at the September Board meeting.



[WECC-0160: WECC IBR Modeling and EMT Screening Criteria](#)

Meeting Weekly on Mondays

# Computational Load Entity Standard Drafting Team Update

**Mark Rogers**

*Manager, Registration and Certification*

# Project 2026-02 Outreach

---

July 2026

# Project 2026-02 Goals

Project Goals include developing:

1

Changes to **NERC Glossary** to align with Rules of Procedure modifications

2

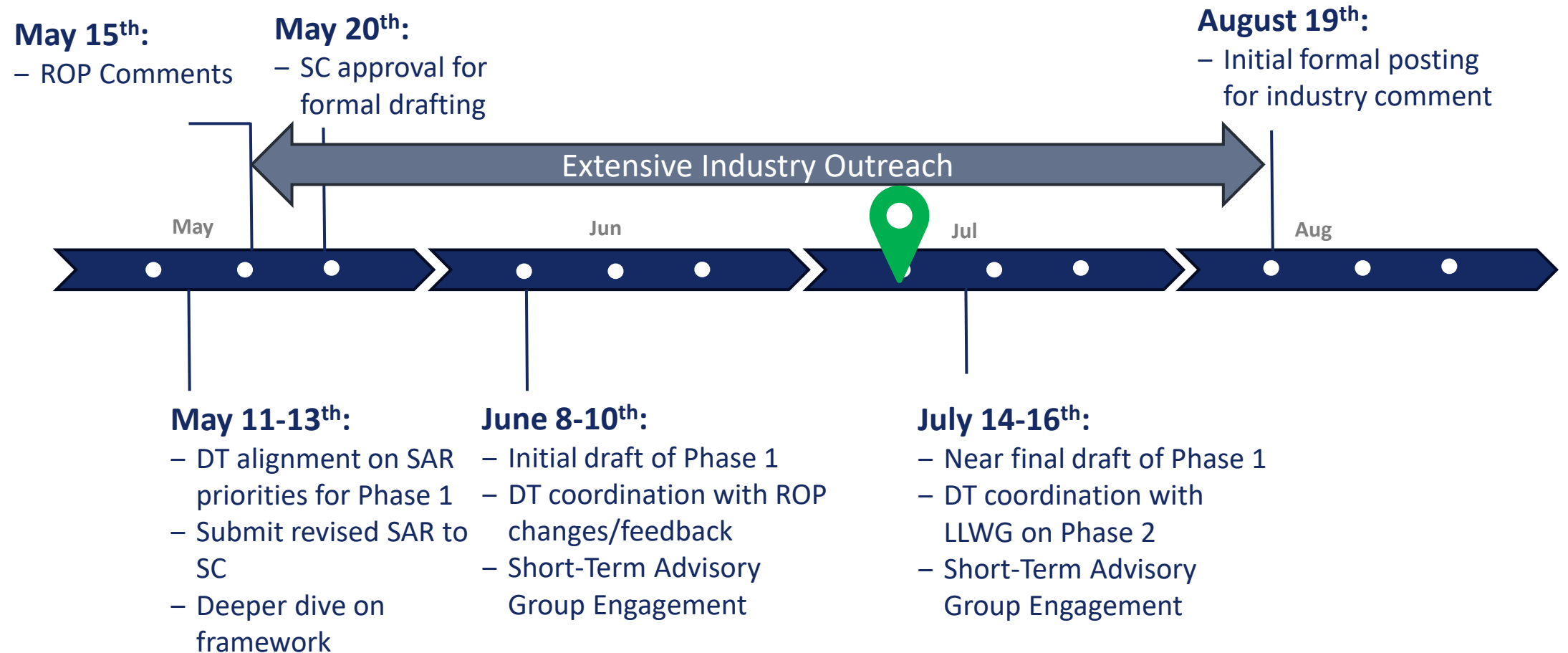
Requirements to address integration of Computational Loads onto the BPS

“This drafting team will develop one or more Reliability Standard(s) to address in the near-term **essential actions** entities must take to assure the reliable integration of large loads into the BPS.”

# 2026-02 Computational Loads Project Timeline

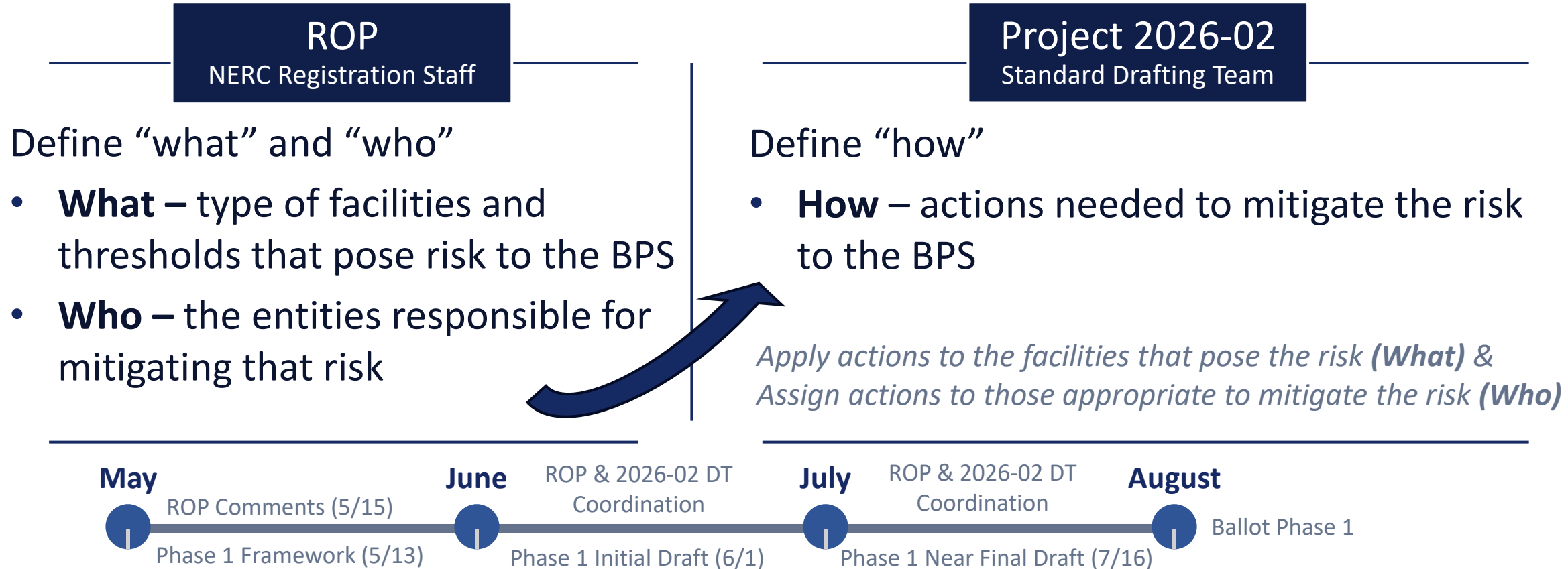


# Zoom-In



# Standard & ROP Development Coordination

Project 2026-02 and the ROP modifications are actively being developed in parallel



**Recent Feedback:** NERC preliminarily is expecting to have two new Functional Entities – Computational Load Owner and Computational Load Operator

# Latest ROP Coordination

**Computational Load Site** - One or more buildings, structures, or installations that:

1. **primarily** contains information technology infrastructure used for:
  - creating, executing, and delivering **software** applications and services;
  - artificial intelligences training, deployment, and delivery;
  - cryptocurrency mining; or
  - other computational activities at a data center; and
2. is supplied through electrical equipment that is connected to the BPS.

**Computational Load Owner (CLO)\*** - The entity that owns and maintains a Computational Load Site.

**Computational Load Operator (CLOP)\*** - The entity that operates a Computational Load Site.

\*Registration only applicable for Computational Load Sites greater than or equal to **50 MW** that is connected at a voltage greater than or equal to **100 kV** from one or more points of connection.

# Phase 1 Strategy: “Foundational” Standard(s)

---

Goal: Deliver Reliability Standard Requirements that...

1. Are essential actions that ‘move the needle the most’
2. Can be most effectively delivered on the targeted Phase 1 timeline (2026)

Strategy:

## **1. Set the Foundation:**

Focus on the core, process-related items in Phase 1 (set the foundation)

## **2. Don’t Start from Scratch**

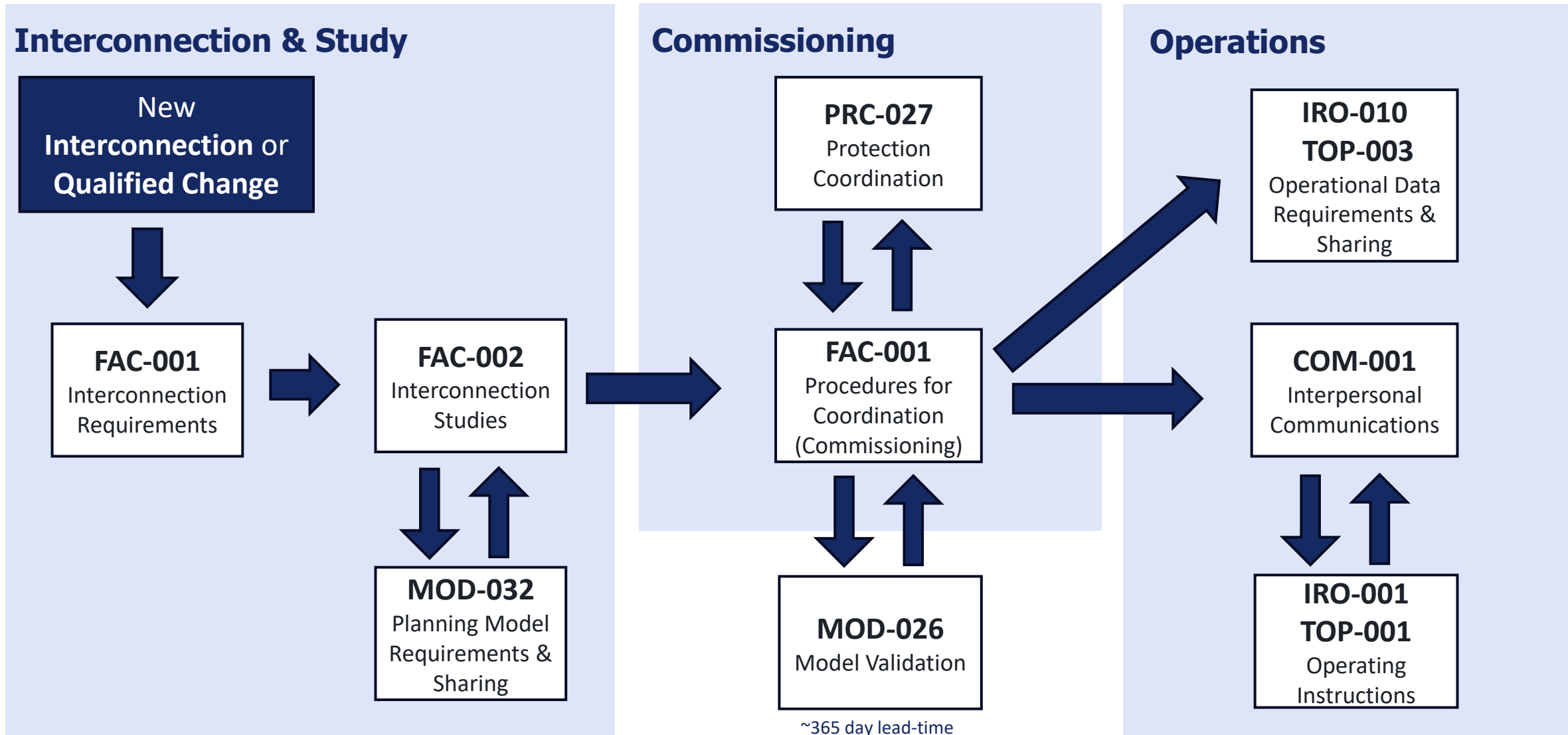
Leverage existing process-related frameworks & concepts for integrating elements onto the BPS

## **3. Enable Industry Flexibility in an Evolving Time**

Allow flexibility on process specifics, do not include technical specifics that are still evolving and/or may have regional variances

# Notable Integration Requirements: Other Facilities

Generation & transmission Facilities have foundational “essential actions” as part of integration



# Project 2026-02: “Six Core Buckets”

|                                                                                     |                                        |                                                             |
|-------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------------------------------|
|    | Data Sharing                           | – CL Data → Owners, Planners, Operators                     |
|    | Interconnection Requirements           | – Developed in coordination with Planners & Operators       |
|    | Interconnection Study & Modeling       | – Interconnection study process with accurate modeling data |
|    | Commissioning                          | – Establish commissioning procedures                        |
|   | Communications & Response              | – CLs have communication protocols with Operators           |
|  | High Resolution Disturbance Monitoring | – Require high-resolution monitoring for CLs                |

Phase 2 & Beyond to address gaps that require additional technical work (e.g., minimum Voltage & Frequency Ride-Through performance requirements)

# Voltage & Frequency Ride-Through (VRT/FRT)

Project 2026-02 is addressing **foundational** essential actions associated with VRT/FRT risk

Phase 1  
Foundational  
Requirements

Dynamic Modeling

Interconnection  
Studies

Interconnection  
Requirements

While Phase 1 is not planning to address **industry-wide**, minimum VRT/FRT performance thresholds due to further technical work required, work is **actively progressing in parallel**

LLWG Work  
Plan  
(Dec 2026 or  
sooner)

Whitepaper: Large  
Load Disturbance  
Performance

Assess appropriateness and reliability need for industry-wide vs. regional or local VRT/FRT thresholds

Provide insight on how to construct VRT/FRT, and post fault active power recovery requirements

# What We Must Deliver

Reliability Standards

v4 Draft Complete

Implementation Plan

v2 Draft Complete

Technical Rationale

v1 Draft Complete

Packaging & Redlines

Not Started

Robust Outreach Plan &  
Messaging

In Progress Complete

FAQ

v1 Draft Complete

# Frequently Asked Questions (FAQ)

## Project 2026-02 Computational Loads

Subscribe to Project Mailing List >

Table of Contents

Important Dates

Project Details

Development History

View Related Files >

### Status

The formal comment period for the Project 2026-02 Computational Loads Standard Authorization Request (SAR) concluded at 8 p.m. Eastern, Thursday, April 30, 2026.

### Important Dates

|                                                         |            |
|---------------------------------------------------------|------------|
| The Standards Committee authorized standard(s) drafting | 05/20/2026 |
| The Standards Committee accepted the SAR                | 03/18/2026 |
| Drafting Team appointed                                 | 03/18/2026 |
| Initial posting authorized                              |            |

### Frequently Asked Questions



Frequently Asked Questions

Modified: 06/26/2026

- Project Scope & Purpose
- Industry Engagement
- ROP Modifications
- Standard Applicability
- New vs. Existing Standards
- Implementation Plan
- Technical Topics

## Project 2026-02 FAQ

### Frequently Asked Questions

#### Project 2026-02 Computational Loads

An increasing number of large commercial and industrial loads are rapidly connecting to the bulk power system. Computational loads, such as data centers (including cryptocurrency and artificial intelligence), present unique challenges in forecasting and planning for increased demand. Through extensive analysis, report development, and ongoing engagement, NERC determined that it must act now to mitigate the risks associated with large computational loads, and a Large Loads Action Plan was developed. Through a three-pronged approach of technical justification, registration criteria for computational loads, and new Reliability Standards, NERC and our stakeholders can ensure new computational loads connect to the grid reliably and securely.

This Frequently Asked Questions document is intended to help stakeholders understand Project 2026-02 Computational Loads and the proposed CLE-001, CLE-002, and CLE-003 draft Reliability Standards. It summarizes the purpose of the project, the current standards framework, key process questions, and topics that may be addressed through future standards development work.

#### Project Scope and Purpose

##### What are Computational Loads?

Computational Loads generally refer to loads, such as data centers, that contain information technology infrastructure supporting computational activities like cryptocurrency mining, artificial intelligence training or inference, and cloud-based compute and storage.

##### What is the purpose of Project 2026-02 on Computational Loads?

Project 2026-02 is developing Reliability Standard requirements to address the *near-term essential actions* needed to support the reliable integration of large computational load sites onto the Bulk Power System. This project will serve as a foundation to support computational load integration in a manner that supports a resilient and reliable Bulk Power System.

##### Why are these new Reliability Standards needed?

Computational loads can be large and have unique operating characteristics, growth patterns, controls, and disturbance response behaviors. These characteristics can pose unique risks to the Bulk Power System as detailed in the NERC ["Characteristics and Risks of Emerging Large Loads"](#) whitepaper in July of 2025.

# Potential Structure of Phase 1 Standards

---

CLE-001: Interconnection, Studies, & Modeling Data

CLE-002: Operational Data & Communications

CLE-003: Protection & Disturbance Monitoring

# Standard Development Strategy

## “Compliance Words Matter”

We are using **time-tested**, **compliance-vetted**, and **industry-supported** language and making incremental changes where appropriate due to the uniqueness of Computational Loads

The drafting team is clearly denoting comparable integration requirements in existing standards and incremental changes to that language (based on industry feedback and support)

Black = Existing language in comparable requirements  
Blue = New language needed for Computational Loads

The latest version (6/11) is our 4<sup>th</sup> revision, reflective of extensive industry feedback and comprehensive DT discussions

### CLE-001-1 – Computational Load Interconnection, Studies, & Modeling Data

#### B. Requirements and Measures

Gray = Provides the reference to existing, comparable standard requirements,

Black = Existing language already in comparable standard requirements that can be leveraged,

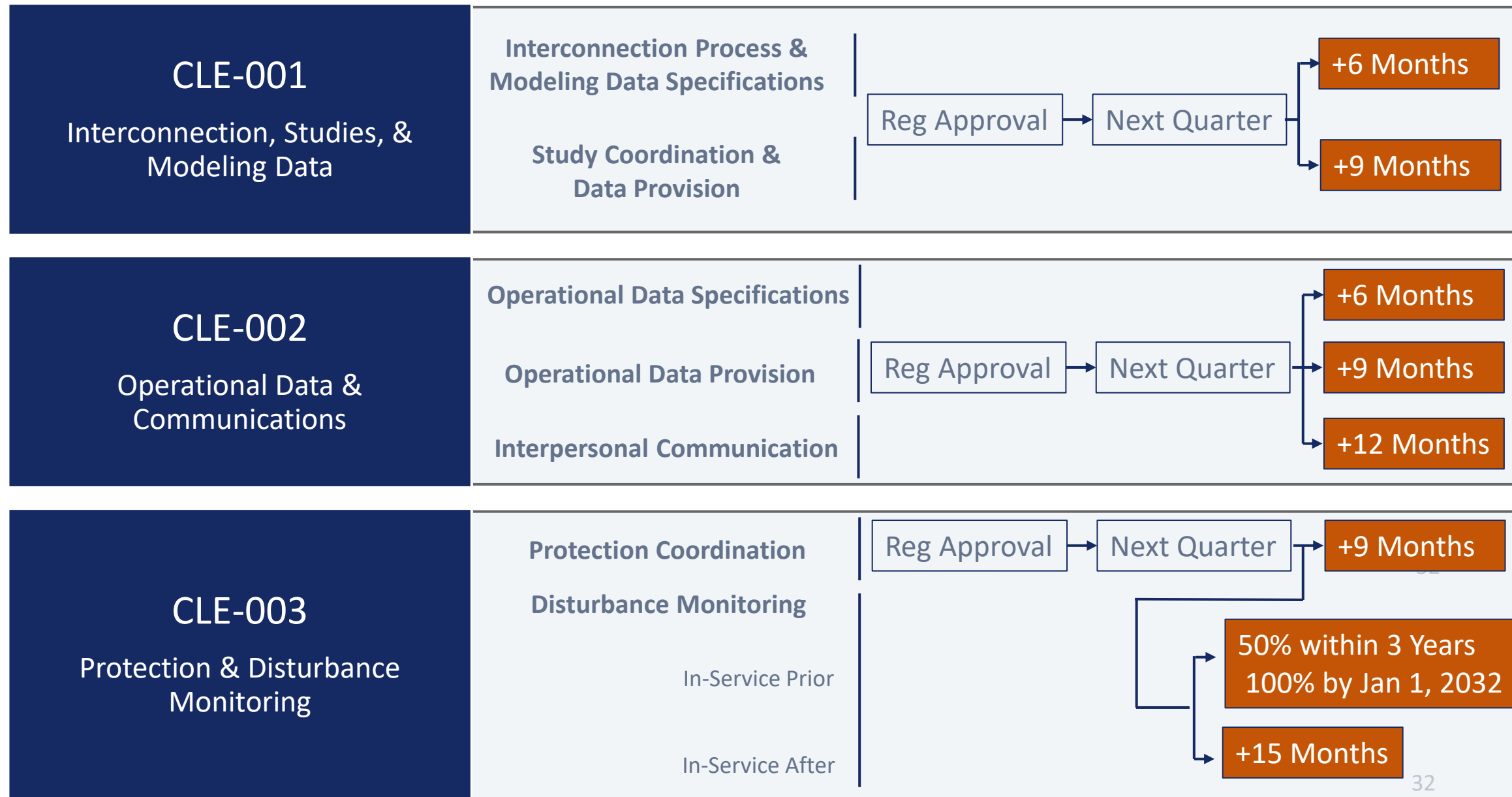
Blue = New, unique language to specifically address Computational Loads and Phase 1 essential actions,

Red = Specific Requirement references where numbering may change during future development.

#### Interconnection Requirements & Process

- R1. [FAC-001 R1] Each Transmission Owner and Distribution Provider shall document **Computational Load Site** interconnection requirements, update them as needed, and make them available upon request. [Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]
- M1. Each Transmission Owner and Distribution Provider shall have evidence (such as dated, documented **Computational Load Site** interconnection requirements) that it met all requirements in Requirement R1.
- R2. [FAC-001 R3] Each Transmission Owner and Distribution Provider shall address the following items in its **Computational Load Site** interconnection requirements: [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]
  - 2.1. Procedures for coordinated studies for new interconnections or existing interconnections seeking to make a qualified change as defined by the Planning Coordinator and their impacts on affected systems.
  - 2.2. Procedures for notifying those responsible for the reliability of affected system(s) of new interconnections or existing interconnections seeking to make a qualified change.
  - 2.3. Procedures for coordinating any interconnection requirements specific to **Computational Load Sites** with the applicable Transmission Planner, Planning Coordinator, Transmission Operator, Balancing Authority, and Reliability Coordinator responsible for the reliability of affected system(s) of new interconnections of **Computational Load Sites**.

# Draft Implementation Plan Development



# Notable Recent Draft Standard Modifications

---

- **ROP**
  - Computational Load Site
  - Computational Load Owner vs. Computational Load Operator
- **CLE-001**
  - TO, DP, GO applicability only for those with existing or future Computational Load Site Interconnection
  - Minimum modeling data specifications
  - Model Verification
- **CLE-002**
  - Modify Operating Instruction definition (add Computational Load Site)
- **CLE-003**
  - Sequence of Event Recording (SER) data

# Next Steps

---

- July
  - Updated ROP Functional Entity Definition Coordination (July 1<sup>st</sup>)
  - In-person drafting team meetings (July 14-16<sup>th</sup>) to create near final drafts
    - Standards, FAQ, Implementation Plans, Technical Rationale, Redlines & Packaging
  - NERC LLWG Coordination
  - Final ROP alignment pre-ballot
  - Continued extensive industry outreach, including Short-Term Advisory Group Engagement
- August
  - Target initial posting for industry comment on August 19<sup>th</sup>

# Internal Controls Maturity Self-Assessment Tool

**Molly Elliott**

*Senior Technical Analyst Internal Controls, Oversight Planning*

**Electric Reliability  
& Security for the West**

July 16, 2026

# Internal Controls Maturity Self-Assessment Tool



New resource for evaluating strengths and weaknesses in your system of risk mitigation and internal control and identifying areas for continuous improvement

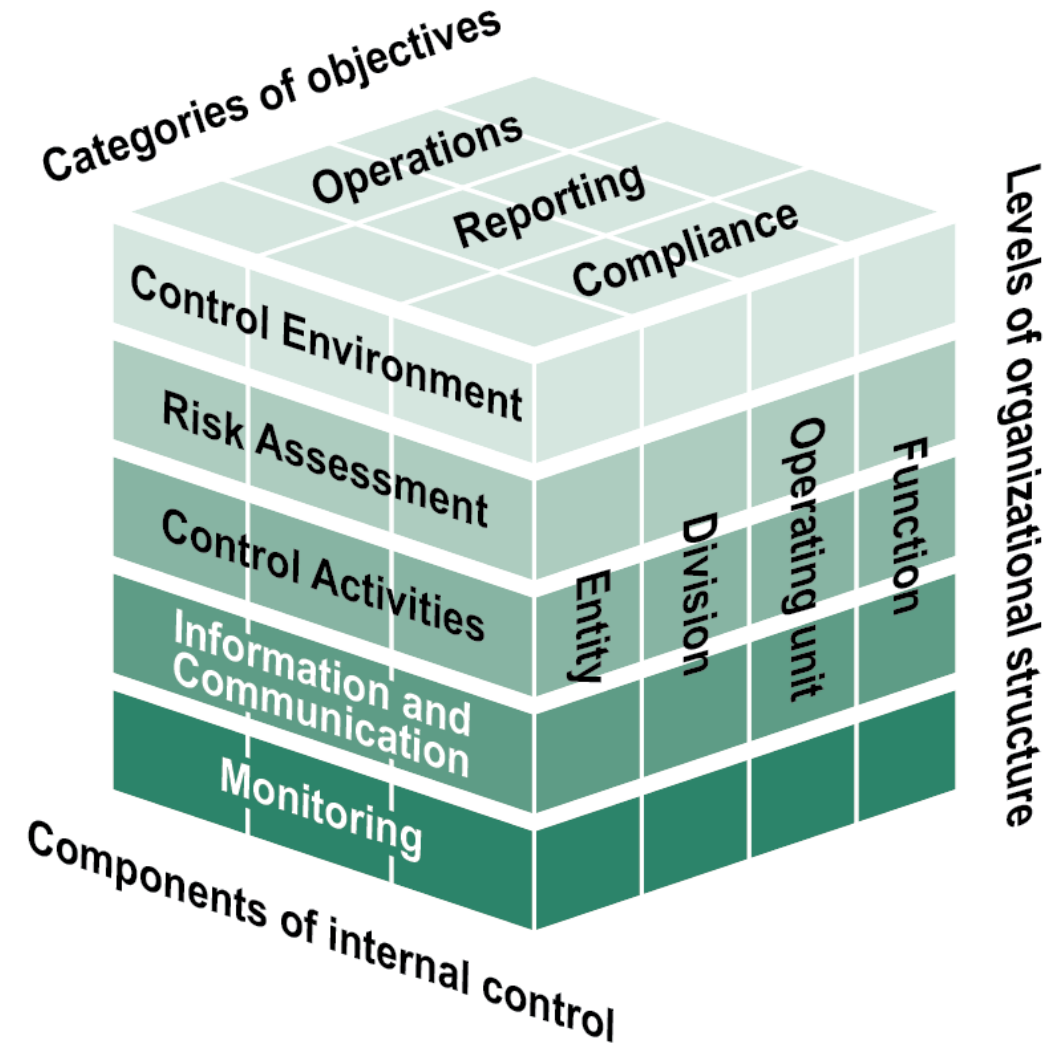


Complements WECC Controls Guidance documents which focus on control activities to meet process-level risks

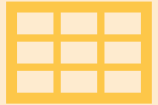


Complements Internal Compliance Program Self-Assessment which focuses on organizational structures to prevent and detect noncompliance and promote a culture of reliability

# What makes a good Internal Controls Program?



# What is a Maturity Model?



A maturity model is a structured framework that helps organizations assess their current capabilities in a specific discipline and provides a clear, step-by-step roadmap for continuous improvement and growth.



It is **not** a “grade.”



It **is** a measure of progress.

# What is a Maturity Model?

| #  | Name                   | Description                                                       |
|----|------------------------|-------------------------------------------------------------------|
| L1 | Initial                | Application limited or non-existent                               |
| L2 | Managed                | Applied in some business units or functions                       |
| L3 | Defined                | Applied organization-wide with documented, repeatable processes   |
| L4 | Quantitatively Managed | Measured and aligned with internal and external stakeholder needs |
| L5 | Optimizing             | Focused on continuous improvement and innovation                  |

# Internal Control Maturity

| Component                   | L1: Initial | L2: Managed | L3: Defined | L4:<br>Quantitatively<br>Managed | L5: Optimizing |
|-----------------------------|-------------|-------------|-------------|----------------------------------|----------------|
| Control Environment         |             |             |             |                                  |                |
| Risk Assessment             |             |             |             |                                  |                |
| Control Activities          |             |             |             |                                  |                |
| Information & Communication |             |             |             |                                  |                |
| Monitoring                  |             |             |             |                                  |                |



# Internal Control Maturity Self-Assessment

## Component 1: Control Environment

| L2 (Managed)                                                                                                                                                                        | L3 (Defined)                                                                                                                                                                                                    | L4 (Quantitatively Managed)                                                                                                                                              | L5 (Optimizing)                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Principle 1: Demonstrate commitment to integrity and ethical values</b>                                                                                                          |                                                                                                                                                                                                                 |                                                                                                                                                                          |                                                                                                                                                                                             |
| Management may attempt to establish organizational integrity and ethical values through staff meetings or individual influence but has not instituted a documented code of conduct. | Established processes evaluate performance against a documented code of conduct and address any deviations in a timely manner. Individuals can report issues through reporting lines such as an ethics hotline. | Key risk and performance indicators may target ethical behavior, structural issues, or competence issues. Measurement may increase the completeness of other principles. | Management's directives, attitudes, and behaviors are innovative and continually reinforce integrity and ethical values. These priorities are understood and practiced by all stakeholders. |
| <b>Principle 2: Exercise oversight responsibility</b>                                                                                                                               |                                                                                                                                                                                                                 |                                                                                                                                                                          |                                                                                                                                                                                             |
| An independent oversight body (e.g., board of directors) exists but may not have the information or authority necessary to effectively manage entity risk.                          | Independent oversight body oversees operations, provides constructive feedback to management, and makes decisions in alignment with strategic objectives and ethical values.                                    | Key risk and performance indicators are tracked and evaluated to provide the independent oversight body with greater visibility into organizational performance.         | Independent oversight body members understand current and emerging risks to entity objectives. The body works with key stakeholders to help fulfill their expectations.                     |

# Next Steps



Program Areas ▾

Committees ▾

## Compliance Monitoring and Enforcement

- Baja California, Mexico
- British Columbia
- United States
- New Entity Resource Center



**Recommended Action:** WECC strongly recommends entities regularly assess the maturity of their controls programs.

Internal Controls Guidance And Compliance Failure Points ▾

Internal Controls Failure Points ▾

Internal Controls Information And Tools ▾



Oversight Trends ▾



# Outreach Tools

---

## Internal Controls Maturity Self-Assessment

[Internal Control Maturity Self-Assessment | Western Electricity Coordinating Council](#)

## Internal Compliance Program Self-Assessment

[Internal Compliance Program Self-Assessment | Western Electricity Coordinating Council](#)

## Controls Guidance and Compliance Failure Points

[Compliance - United States | Western Electricity Coordinating Council](#)

## Oversight Trends Update

[Oversight Trends Update | Western Electricity Coordinating Council](#)



**ENGAGE WITH WECC**





[engage@wecc.org](mailto:engage@wecc.org)



[www.wecc.org](http://www.wecc.org) | 801-582-0353



155 N 400 W, Salt Lake City, Utah 84103, USA