Controls Guidance and Compliance Failure Points

MOD-031-3
February 2026

Demand and Energy Data

Long-term Studies/Assessments
Modeling Data

WECC Intent

The *Controls Guidance and Compliance Failure Points* document is intended to provide a starting point for registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. It contains examples supporting registered entities' efforts to design controls specific to operational risk *and* compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards. WECC does not intend for this document to establish a standard or baseline for entity risk assessment or control objectives.

> ***Note**: Guidance questions help an entity understand and document controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance during a Compliance Monitoring and Enforcement Program (CMEP) engagement.*
>
> ** Please send feedback to internalcontrols@WECC.org with suggestions on controls guidance and potential failure points questions.*

Definitions

Control Objective: The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's larger objectives.

Control Activities: The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Internal Control: The processes, practices, policies or procedures, system applications and technology tools, and skilled human capital that an entity employs to address risks associated with the reliable operation of its business. Internal control components include:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Risk Category: Type of operational and inherent risks identified by the Electric Reliability Organization (ERO) Enterprise for use in the Compliance Oversight Plan (COP). Entities should use Risk Categories to understand, monitor, and mitigate known and future risks.

Risk Category

Long-term Studies/Assessments: Long-term studies and assessments evaluate whether the system can reliably operate in real-time, including 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 methods 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 will likely result in gaps and may compromise BPS reliability and security.

Modeling Data: Simulation tools model individual components and their control systems, when applicable. The models form the building blocks of power system studies in the planning and operations horizons. Models that entities have verified as accurate are critical to a range of reliability studies, including transmission planning assessments and establishing SOLs and IROLs, as well as state estimation for Real-time Assessments (RTA) and Operation Planning Assessments (OPA). The validity of those assessments depends on modeling data, including, but not limited to, correct Facility Ratings, verified generator real and reactive capability, and knowing how control systems respond to dynamic system conditions. Failure to provide data in a timely manner and at intervals to ensure model accuracy during retirements and new construction may compromise BPS reliability and security.

MOD-031-3 specifically addresses the collection of Demand, energy and related data to support reliability studies and assessments.

Control Objectives

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help entities get started, WECC has identified generic control objectives to mitigate the risks associated with the risk categories mentioned above and MOD-031-3. You may want to consider these three objectives:

> **Control Objective 1**: Develop and issue a data request for Total Internal Demand, Net Energy for Load, and Demand Side Management data (PC, BA).
>
> **Control Objective 2**: Provide requested data.
>
> **Control Objective 3**: Ensure all received data is sound and usable.

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. When designing and strengthening controls, they should be tailored to meet the applicable objectives.

Below are examples of control activities based on good practices WECC has observed that are designed to meet the objectives listed above. WECC does not intend for these activities or the associated questions to be prescriptive. Rather, they should help your entity consider how you might meet your objectives in your own unique environment. They also may help your entity identify controls you did not realize you had.

Control Objective 1: Develop and issue a data request for Total Internal Demand, Net Energy for Load, and Demand Side Management data (PC, BA)

Control Activity A: Determine which data is required (Relates to risk associated with R1).

1. How does your entity determine the Demand, energy and related data needed to support reliability studies and assessments?
   a. What verification do you perform to confirm all necessary data is identified?
2. How does your entity collect the following data:
   a. Actual data?
      i. Normalized Demands from variable weather-related conditions?
   b. Forecast data?
3. How does your entity collect and notate applied assumptions and other summary data?

Control Activity B: Determine applicable entities (Relates to risk associated with R1).

1. How does your entity work with neighboring entities to define the boundaries of your PC or BA area?
2. Has your entity identified all the entities within your PC or BA footprint who own the data necessary to support reliability studies and assessments?
3. How does your entity ensure new applicable entities are included in future data requests?
4. How does your entity ensure contact information is up to date?
   a. Do you have a process for verifying contact information?
   b. Do you maintain a list of backup contacts?

Control Activity C: Determine a timetable for providing the data (Relates to risk associated with R1).

1. What factors does your entity consider when determining a timetable for data submission? (e.g., based on the timing of the studies to be performed or concurrent with the entity submitting other data)

Control Activity D: Ensure data request is designed to yield consistent data.

1. How does your entity ensure the level of detail required is clear?
   a. Do you periodically review the data request to ensure there is little to no ambiguity?
   b. Have you received agreement or acknowledgement from the data providers that they understand and agree they can provide the data requested in the specification?

Control Objective 2: Provide requested data

Control Activity A: Implement a process to provide requested data. (Relates to risk associated with R2, R3, R4)

1. Does your entity have a documented process for internal and external coordination?
   a. Does the process define roles and responsibilities for providing data?
   b. Does the documented process include a provision to request clarification if data requirements are not clear?

2. Does the process outline responses to periodic data requests as well as processes to receive on demand requests?
    a. Does the process address tracking requests?
    b. Does the process address internal coordination where the requested data is owned by different business units?
    c. How often is the documented process reviewed?

Control Activity B: Provide Total Internal Demand, Net Energy for Load, and Demand Side Management data to PC or BA on the prescribed timeline. (Relates to risk associated with R2)

1. Does your entity perform a review to ensure data is current, accurate, and in accordance with the request prior to submission?
2. Is data verification performed to ensure the data did not change due to weather-related conditions?
    a. Are weather-related variations for the prior year reviewed?
    b. Is an additional data set created for normalized annual peak hour actual Demand when weather-related Demand variations are found?
    c. How are assumptions approved and implemented for adjusting future forecasts?
    d. Do you confirm data is provided in the units stated in NERC Reliability Standard MOD-031?
3. What technical controls has your entity put in place to ensure timelines are met?

Control Activity C: Provide reliability assessment data upon request to Regional Entity or entity who has demonstrated a need for such data to conduct reliability assessments. (Relates to risk associated with R3, R4)

1. How does your entity ensure data is made available within the requested time frame?
2. How does your entity determine the basis for not providing data in response to a request?
    a. Have you developed guidelines for this determination?
    b. Who has the authority to make the determination?
    c. Are these determinations reviewed internally?
    d. If so, by whom?
3. What technical controls has your entity put in place to ensure timelines are met?

Control Objective 3: Ensure all received data is sound and usable

Control Activity A: Ensure responses are received.

1. How is contact information for the responsible party at your entity provided?
    a. Is it a mailbox or other form of communication that is monitored by multiple parties?
        i. Is this in a process document?
2. Does your entity have a process to confirm all responses have been received and are complete?
    a. Does it include follow up and/or escalation if responses are not received according to the stated timeline?

Control Activity B: Ensure responses are technically sound.

1. Does your entity have a process to review data that is received to ensure it is technically sound?

a. Who conducts this review?
b. Do you use any automated tools for this review?

Compliance Potential Failure Points

The control activities listed above are specifically targeted at mitigating risk to the reliability and security of the BPS but also promote compliance with the referenced standard. Your entity should also develop controls specifically to mitigate compliance risk. The following compliance potential failure points relate directly to compliance risk and warrant consideration.

Potential Failure Point (R1): Failure to identify need for reliability assessment data.

1. How does your entity ensure it has considered all applicable actual, forecast, or summary data needed for the reliability assessments?

Potential Failure Point (R1): Failure to identify applicable entities in the request.

Potential Failure Point (R1): Failure to identify a timeline equal to or greater than 30 calendar days in the request.

Potential Failure Point (R2, R3, R4): Failure to provide all the data requested within the required time frame.

1. How does your entity ensure your response is complete?
   a. Do you conduct any reviews prior to submitting the response?
   b. How and who monitors if a data request has been received?
2. How does your entity ensure your response is timely?
   a. Do you use any technical tools? (e.g., workflow)

Potential Failure Point (R4): Failure to provide a written response to the requesting entity stating the basis in the event the data is not being provided.

1. How does your entity identify the basis for not providing the requested data?