Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

EOP-004-4

Normal System Operations

September 2022

WECC Intent

The *Controls Guidance and Compliance Failure Points* document guides registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. WECC's intent is to provide examples supporting the efforts of registered entities to design controls specific to operational risk *and* compliance with the NERC Reliability Standards. The registered entity may use this document as a starting point in assessing risk and designing appropriate internal controls. Each registered entity should perform a risk assessment to identify its entity-specific risks and design appropriate internal controls to mitigate those risks; WECC does not intend for this document to establish a standard or baseline for entity risk assessment or controls 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 and Instructions

Control Objective: Aim or purpose of internal control to address identified risk or operational concern.

Control Activities: Policies, procedures, techniques, and mechanisms to achieve control objectives and mitigate related risks.

Quality Assurance/Quality Control (QA/QC): How an entity *verifies* it performed an activity or verifies an activity was performed *correctly* (examples include separation of duties, having a supervisor double-check someone's work, etc.).

Risk Category: Type of operational and inherent risks identified by the 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

Normal System Operations: Actions performed during real-time operations maintain Bulk Power System (BPS) security and reliability. Failure to consider the balancing resources within defined values,

appropriately capturing and reporting of defined events to required organizations, inability or inadequate capabilities to monitor and analyze data needed to perform reliability functions and ensuring proper communications with a predefined protocol may compromise BPS reliability and security.

EOP-004-4 mitigates risks to the reliable operation of the BPS by requiring event reporting to the ERO and other appropriate organizations.

Control Objective(s)

Your entity should perform a risk assessment and identify entity-specific control objectives to mitigate those risks. To help your entity get started, WECC has identified generic control objectives to mitigate the risks associated with the risk category mentioned above and EOP-004-4. You may want to consider these two objectives:

Control Objective 1: Prepare personnel to recognize and report events.

Control Objective 2: Submit appropriate report in response to a reportable event.

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. As you design controls, your entity should tailor them to entity-specific control 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: Prepare personnel to recognize and report events.

Control Activity: Identify organizations that receive event reports.

1. How does your entity determine which organizations (both internal and external) need to receive event notifications? (Relates to risk associated with R1)
    a. What is your process for developing and approving a list of organizations that should receive notifications about events?
    b. What person or group(s) are involved in determining who should receive notifications?
    c. How frequently is the list of organizations in the event reporting Operating Plan reviewed and updated?
2. How does your entity verify that the contact information listed in the event reporting Operating Plan is correct and up to date?
3. How does your entity ensure contact information is easily accessible in an emergency?

Control Activity: Ensure all relevant SMEs understand their roles and responsibilities.

1. How does your entity ensure all relevant SMEs (e.g., control center, field personnel, generation personnel) know how to recognize reportable events?
    a. Do you have documented guidance on how to recognize reportable events?
        i. How do you ensure those guidance documents include all reportable event types?
        ii. Do the guidance documents address reporting responsibilities when more than one entity is involved in the event?
    b. Do you have a training or communications program that focuses on recognizing reportable events?
        i. What person or group is responsible for developing and delivering training and communications?
        ii. Which employees are included in the training?
        iii. How frequently do personnel receive training/messaging?
        iv. Do you perform any QA/QC to verify the training/communications are effective?
2. How does your entity ensure relevant SMEs understand their roles and responsibilities for submitting the event report to organizations identified in the Operating Plan?
    a. Do you have documented guidance readily available for use in submitting an event report?
    b. Do you have a training or communications program that focuses on submitting event reports?
    c. Does the training or guidance include:
        i. Selecting the appropriate form?
        ii. When to submit each form?
        iii. How to fill out the form?
    d. How frequently do personnel receive training/messaging?
    e. Do you perform any QA/QC to verify the training/communications are effective?

Control Objective 2: Submit appropriate report in response to a reportable event.

Control Activity: Recognize reportable events. (Relates to risk associated with R2)

1. How does your entity monitor for operating conditions that might meet the event reporting thresholds?
2. Does your entity perform a shift turnover log review?

Control Activity: Submit event reports to identified organizations. (Relates to risk associated with R2)

1. If different people or work groups are responsible for preparing and communicating an event report, how does your entity ensure coordination between groups?
2. How does your entity verify that event report(s) were received by intended recipients?
    a. Do you have documented process steps for preserving evidence that communications have been completed?
3. Has your entity established QA/QC methods to verify that events are properly reported to the

identified organizations?

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 develop an Operating Plan that includes event reporting protocols.

1. Has your entity implemented a documented event reporting Operating Plan?
    a. If yes, does your plan include the following:
        i. Protocol(s) for reporting to the Electric Reliability Organization by event type; and
        ii. Protocol(s) for reporting to other organizations (e.g., company personnel, law enforcement) by event type?

Potential Failure Point (R2): Failure to report events within the timeframe specified by the standard.

1. How does your entity track the reporting time frame?
    a. How do you define what constitutes "recognition" that an event meets the reporting thresholds?
    b. How do you document the start and end times of the event reporting process?
    c. Once the event is recognized, do you have a method to track and communicate how much time remains to complete the reporting process?
2. Has your entity established QA/QC methods to verify that events are reported to the identified entities within the time frame specified by the standard?