Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

COM-001-3

Operational Studies/Assessments

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

Operational Studies/Assessments: Operational studies and assessments in the operations horizon evaluate whether the system can reliably operate in real time, including correct calculation of Area Control Error

(ACE) to ensure proper deployment of Regulating Reserve; correct methods to determine and communicate SOLs; ensuring capture of complete and comprehensive data for Real-time Monitoring and Analysis; proper design, operating plans and response to Geomagnetic Disturbance (GMD) events; Interpersonal Communication capabilities and protocols between entities to avoid uncontrolled separation, or cascading outages. Failure to produce operational studies and assessments used in the operations horizon to understand gaps may compromise Bulk Power System (BPS) reliability and security.

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 categories mentioned above and COM-001-3. You may want to consider these three objectives:

Control Objective 1: Establish primary and Alternative Interpersonal Communications capabilities.

Control Objective 2: Maintain primary and Alternative Interpersonal Communications capabilities.

Control Objective 3: Respond to failure of primary and Alternative Interpersonal Communications capabilities.

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: Establish primary and Alternative Interpersonal Communications capabilities.

Control Activity A: Identify all registered entities or internal functions that require Interpersonal Communication capabilities. (Relates to risk associated with R1, R3, R5, R7, R8, R12, R13)

1. How does your entity ensure relevant personnel participate in identifying the registered entities and internal functions that require Interpersonal Communications methods?
2. Does your entity include any other entities or locations in this program in addition to those required by the NERC standard?
3. How does your entity monitor for changes that would require updates to the list of required Interpersonal Communications capabilities (e.g., footprint or registration changes)?
    a. Does this include changes initiated by another entity?

Control Activity B: Select required primary and Alternative Interpersonal Communications capabilities. (Relates to risk associated with R1 - R8, R12, R13)

1. How does your entity select appropriate methods of Interpersonal Communications?
    a. What person or department selects communications methods?
    b. What risks are considered (e.g., unique topography, security, reliability) when selecting methods?
        i. Does the selected method vary by the needs of the entity to which you are connecting?
    c. Do you perform QA/QC to verify the appropriateness of the methods selected?

Control Objective 2: Maintain primary and Alternative Interpersonal Communications capabilities.

Control Activity A: Maintain communications with designated entities and internal functions. (Relates to risk associated with R1, R3, R5, R7, R8, R12, R13)

1. Does your entity have formal communications procedures or protocols that address operations of all interpersonal communications equipment or facilities?
2. Do those procedures or protocols address failures of both primary and alternate communications facilities.
3. Have Operations personnel been trained on operating all Interpersonal Communications equipment or facilities?
    a. Do you offer refresher training?
    b. Do you evaluate the training for efficacy?
4. Does the training include actions in case of failures of Interpersonal Communications equipment or facilities?
5. Are there any alarms or notifications to operators if a failure or trouble occurs with the communications systems?

Control Activity B: Test Alternative Interpersonal Communications capabilities. (Relates to risk associated with R9)

1. How does your entity ensure that personnel responsible for testing are aware of their responsibilities?
2. Are personnel trained on testing processes?
    a. Do you offer refresher training?
    b. Do you evaluate the training for efficacy?
3. How does your entity ensure "unsuccessful" tests are resolved?
    a. Does the process define what constitutes an "unsuccessful" test?
    b. How do you track the resolution of issues?
    c. Does the process include QA/QC or independent verifications to ensure a successful response to an "unsuccessful" test?

Control Activity C: Update required primary and Alternative Interpersonal Communications capabilities as needed. (Relates to risk associated with R1 - R8, R12, R13)

1. How does your entity monitor for changes to equipment that would require updates to Interpersonal Communications methods?
    a. Do you also monitor for changes to equipment made by other registered entities?

Control Objective 3: Respond to failure of primary and Alternative Interpersonal Communications capabilities

Control Activity A: Coordinate with designated entities in case of a communications failure. (Relates to risk associated with R10, R11)

1. How does your entity's notification process ensure that notifications are made to all affected entities?
2. Does your entity have defined process steps for notifying designated entities of communications failures?
3. **For the GOP/DP function:** If your entity's designated method of Interpersonal Communications is lost, how would your personnel communicate with your BA and TOP to determine actions for restoration? (i.e., do you have a backup method of Interpersonal Communication?)
4. Does your entity's process define which individuals are authorized to determine a "mutually agreeable action"? At each entity?
5. Does your entity have defined parameters for what constitutes a "mutually agreeable action"?

Control Activity B: Repair or replace Interpersonal Communication capability. (Relates to risk associated with R9, R10)

1. What specific steps does your entity take to initiate action to repair or designate a replacement Interpersonal Communication capability?
2. How does your entity determine whether a failure warrants a repair or replacement?
    a. Do you have documented troubleshooting guidelines? Are they equipment-specific? Are they location-specific?
    b. Have you assigned responsibility (person or department) for making repair or replace decisions?
    c. Have you documented guidelines for considering replacement Interpersonal Communication capability?
3. Does the process specify which personnel (e.g., department, contractor) should be contacted for repairs, including on-call contact information?
4. How does your entity track repair or replacement of Interpersonal Communications capability to completion?
5. Does your entity perform any QA/QC to verify the response is appropriate and completed?

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/R2/R3/R4/R5/R6/R7/R8): Failure to have primary and Alternative Interpersonal Communication capability with the applicable entities as specified in R1, R2, R3, R4, R5, R6, R7, and R8.

1. How does your entity identify the applicable entities?
2. How does your entity determine appropriate communications methods?
3. How are these methods documented?
    a. Do you maintain documentation showing that the methods are used?

Potential Failure Point (R9): Failure to perform Alternative Interpersonal Communication tests on schedule.

1. How does your entity track due dates for periodic testing?
2. Does your entity monitor whether the task is completed by the due date?

Potential Failure Point (R10, R11): Failure to meet timelines when equipment fails.

1. How does your entity ensure personnel are aware of deadlines?
    a. For making notifications if Interpersonal Communications fail?
    b. For initiating action to repair or designate a replacement Alternative Interpersonal Communication capability?
2. Has your entity defined start and end times for making notifications? Initiating action?
3. How does your entity track deadlines when equipment fails?
4. Has your entity established QA/QC methods to ensure responses meet deadlines and are completed appropriately?

Potential Failure Point (R12, R13): Failure to have internal Interpersonal Communication capabilities for the exchange of information necessary for the Reliable Operation of the BES.

1. Does your entity have communication capabilities between control centers and between a control center and field personnel?
2. How does your entity determine what other internal communication capabilities are required for the reliable operation of the BES?