WECC
Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

PRC-027-1

Entity Coordination

Protection Systems

November 2023

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 North American Electric Reliability Corporation (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: The purpose of specified controls; control objectives address the risks related to achieving an entity's goals.

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 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, and
- Monitoring.

Quality Assurance/Quality Control (QA/QC): How an entity *verifies* whether 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 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

Entity Coordination: Coordination, internally and externally, as with third-party suppliers and contractors before making changes to the system or taking any actions with the potential to affect another entity and, in turn, affect Bulk Power System (BPS) reliability and security. Coordination should address the risk associated with operating horizon, planning horizons, and during emergencies. Failure to coordinate may affect BPS reliability and security.

System Protection: BPS reliability and security require adequate generation supplies to meet existing load during steady-state and expected dynamic conditions. When faults or failures occur, the system must isolate the problem but maintain BPS integrity as much as possible. Protection systems must identify the type and location of the problem and isolate the appropriate part of the BPS while minimizing the disturbance to the remainder of the system. This requires Protection Systems associated with the generation, transmission, and load to accurately detect system properties and respond appropriately to unsafe conditions. Protection System settings must allow control systems to provide a full range of control and allow the system to "ride-through" expected transients. Owners of interconnecting BPS devices and systems must coordinate their system settings with neighboring systems to ensure they achieve the desired outcome and prevent unnecessary disconnection of equipment. Protection Systems must also respond to Misoperations of primary protection. Entities must identify and correct the source of operational failures.

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 PRC-027-1. You may want to consider these four objectives:

Control Objective 1: Develop, review, and update a short-circuit model of the system (System Protection)

Control Objective 2: Develop new and revised Protection System settings (System Protection)

Control Objective 3: Coordinate Protection System settings with electrically joined Facilities (Entity Coordination)

Control Objective 4: Perform Protection System Coordination Studies (System Protection, Entity Coordination)

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: Develop, review, and update a short-circuit model of the system.

Control Activity A: Validate all model data and assumptions (Relates to risk associated with R1, R3)

1. How does your entity obtain data for the short-circuit model?
2. Has your entity automated the process of moving protection data between the asset database and the model?
3. Does your entity verify relevant impedances?
    a. Generator
    b. GSU transformer
    c. Tie-line
    d. Transmission line including mutual coupling (dispersed generating resources)
    e. Power transformer (dispersed generating resources)
4. Does your entity validate interconnections with neighboring utilities?
5. How does your entity verify neighboring utility projects are included in the model?

Control Activity B: Ensure planned projects are considered in the model. (Relates to risk associated with R1, R3)

1. How does your entity ensure planned construction (both yours and your neighbors') is accounted for in the model?
2. How does your entity ensure planned generator retirements (both yours and your neighbors') are accounted for in the model?

Control Activity C: Review and update the short-circuit model. (Relates to risk associated with R1, R3)

1. How frequently does your entity review the short-circuit model?
    a. How do you document the reviews for future reference?
2. Does your entity periodically conduct a review of event reports to compare relay fault current analysis data with short-circuit model expectations?
3. What change tracking has your entity implemented for the short-circuit model?

a. How does your entity ensure only authorized personnel make changes?

Control Activity D: Mitigate any issues found in the model before developing new or revised settings.

1. What processes does your entity have in place to correct any issues found in the model before developing new or revised settings?
2. Does your entity perform any additional review to confirm all issues are corrected?

Control Objective 2: Develop new and revised Protection System settings.

Control Activity A: Document a relay-setting calculation process with clear step-by-step procedures and examples. (Relates to risk associated with R1)

1. Do your entity's procedures outline special cases such as:
   a. Reclosing?
   b. Inverter-based resource interconnections?
   c. Nuclear interconnections?
2. Do your entity's procedures include specific steps to coordinate settings with other applicable NERC compliance standards such as:
   a. PRC-019-2 Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection?
   b. PRC-023-4 Transmission Relay Loadability?
   c. PRC-024-2 Generator Frequency and Voltage Protective Relay Settings?
   d. PRC-025-2 Generator Relay Loadability?
   e. PRC-026-1 Relay Performance During Stable Power Swings?
3. Does your entity use technology (spreadsheets, databases, workflow) to track the status of open protection system settings development projects?
4. How does your entity coordinate settings during unforeseen circumstances such as
   a. Misoperations?
   b. Emergency replacements?
   c. Changes during commissioning?
5. What review or verification steps does your entity use to ensure relay calculations are accurate and consistent?
   a. What tools (e.g., checklists, workflow) are used to document the completion of peer or self-review?
   b. Does the review confirm that the settings are modeled correctly and coordinated with neighboring Transmission Owners?
   c. Is the review conducted by personnel not directly involved with the primary modeling, settings, and coordination process?

Control Activity B: Ensure Protection System Engineers are knowledgeable.

1. Does your entity facilitate training specifically for the relays installed at a facility?

   a. How do you ensure that the Protection System Engineers are receiving sufficient training?
2. Does your entity use authorized Relay protection vendors to provide training?

Control Activity C: Document Protection System settings (Relates to risk associated with R3)

1. Does your entity use templates for recording:
   a. Relay calculations?
   b. Relay setting data?
2. Does your entity use a relay asset database to serve as the database of record for protective relay settings?
   a. Is it one consolidated source of equipment data or are multiple systems used to manage asset data (e.g., settings, maintenance records)?
      i. If multiple systems, is there an integrated interface?
   b. Who enters the settings in the database?
   c. How does your entity prevent user error?
      i. Locked-down settings templates?
      ii. "Compare settings" functionality in manufacturer settings software?
      iii. Using automated techniques to transfer settings from vendor-specific data files?
      iv. "Compare settings" functionality in an electronic/digital automated historical archive to flag when settings at the relay are set or changed?
3. Does your entity use standards-based formats such as the Common Information Model (CIM) to represent the primary network to allow for easier exchange of data with other entities?
4. What review or verification steps does your entity use to ensure relay setting documentation is accurate and up to date?
   a. How frequently are existing relay settings reviewed to ensure they are documented correctly?

Control Objective 3: Coordinate Protection System settings with electrically joined Facilities.

Control Activity A: Implement a process for receiving data from neighboring utilities. (Relates to risk associated with R1, R3)

1. Who is responsible for responding to relay setting coordination requests?
   a. Do you have a backup engineer available for urgent requests if the responsible engineer is not available?
      i. How do neighboring entities know to contact that individual?
      ii. Do you use a shared mailbox to ensure requests are received?
2. Does your entity use a checklist or other tool to ensure all pertinent information is considered and appropriate steps (such as updating the short-circuit model) are completed?
   a. Do you have a review process?
3. Does your entity use technology (spreadsheets, databases, workflow) to track the status of open

protection system coordination?

4. Does your entity have a separate process for urgent changes or unforeseen circumstances?

Control Activity B: Ensure neighboring entities receive relay settings communication. (Relates to risk associated with R1, R3)

1. Who is responsible for sending relay settings to neighboring entities?
2. How does your entity ensure contact information is up to date for neighboring entities?
3. Does your entity use a template, DocuSign, or other agreement to document that the other entity has no issues (or that the coordination issue was acceptable or resolved)?
4. Does your entity have a defined approach for reconciling differences in protection system setting philosophy?
5. Does your entity have controls in place to ensure a response is obtained before implementing changes?
    a. Do you have a process to follow up with the neighboring entity to verify there is no coordination issue if a timely response is not received?

Control Activity C: Verify relay settings with neighboring utilities.

1. Does your entity have a process to periodically verify relay settings with neighboring utilities?
    a. Who is responsible for initiating that process?
    b. Is it time-based or is it triggered by an event?

Control Objective 4: Perform Protection System Coordination Studies

Control Activity A: Develop tools for Protection System Coordination Studies

1. Does your entity work with your vendors to develop automated tools for protection studies?
2. Does your entity use visualization and summarization tools to handle the data?

Control Activity B: Timely perform Protection System Coordination Studies (Relates to risk associated with R2)

1. Does your entity perform Protection System Coordination Studies based on time interval, deviation in Fault current values, or a combination?
2. If your entity performs studies based on deviation in fault current values:
    a. How frequently do you review fault current values to determine whether a study is required?
    b. How do you ensure the correct model is used for fault analysis?
3. Does your entity have documented guidance or a philosophy for performing Protection System Coordination Studies?
    a. Does the guidance contain all assumptions used in the study?
    b. Does the guidance contain criteria for making determinations for relay setting changes or equipment replacement?

c. How do you define the network boundary for the study?
d. How are system scenarios and configuration selected?
e. Are all protection systems including backup systems included?

Control Activity C: Mitigate any protection issues found (System Protection)

4. How do you ensure any protection system coordination issues are mitigated?
   a. Do you repeat the studies when issues are found to demonstrate mitigation?
   b. Does a third party review the mitigations?

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 document a process for developing new and revised Protection System settings that addresses the items in R1.

1. Does your entity periodically review your Protection System setting process to verify it effectively addresses all the items in R1?

Potential Failure Point (R1.1, R3): Failure to review and update short-circuit model data.

Potential Failure Point (R1.2, R3): Failure to review Protection System settings before implementation.

1. How does your entity verify Protection System settings meet your entity's technical criteria?

Potential Failure Point (R1.3, R3): Failure to coordinate with electrically joined Facilities before implementing new or revised Protection System settings.

Potential Failure Point (R2): Failure to perform a Protection System Coordination Study in a time interval not to exceed six calendar years.

1. How does your entity ensure the six-calendar-year interval is not exceeded?

Potential Failure Point (R2): Failure to identify an appropriate fault current baseline for use in determining the need for a Protection System coordination Study.