Controls Guidance and Compliance Failure Points

PRC-002-5
February 2026

Disturbance Monitoring and Reporting Requirements

Asset System Identification
Long-term Studies/Assessments
System Protection

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

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

Asset/System Identification: Identifying and tracking assets and Bulk Electric System (BES) Facilities is critical to BPS security and reliability. Failure to correctly identify, document and track items may result in gaps and compromise the integrity, reliability, or security of the BPS.

PRC-002 requires the identification of assets and elements critical to understanding large scale system disturbances.

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.

Analysis and reconstruction of BES events requires sequence of events recording (SER) and fault recording (FR) data from key BES buses. The purpose of Reliability Standard PRC-002 is to capture event data to understand large scale system disturbances occurring on the BES.

System Protection: BPS reliability and security requires 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 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 PRC-002-5. You may want to consider these four objectives:

Control Objective 1: Identify equipment and Elements for data collection (Asset/System Identification, Long-term Studies/Assessments)

Control Objective 2: Ensure that the owners of the respective BES Elements are aware of their data recording responsibilities (Asset/System Identification)

Control Objective 3: Record and maintain SER, FR, and dynamic disturbance recording (DDR) data to support event analysis. (System Protection)

Control Objective 4: Provide data to the Reliability Coordinator (RC), Regional Entity, or NERC (Long-term Studies/Assessments)

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: Identify equipment and Elements for data collection

Control Activity A: Identify BES buses for which SER and FR data are required (Relates to risk associated with R1) (TO)

1. How does your entity determine who is responsible for performing the BES bus identification?
   a. How do you ensure reevaluation is completed when necessary?
2. How does your entity apply the methodology in PRC-002-5, Attachment 1?
   a. How do you ensure you are using the appropriate MVA?
   b. Do you use a standardized calculation methodology to ensure consistency?
   c. Are you maintaining documentation that the Attachment 1 steps were completed?
3. If applicable, how does your entity ensure additional BES buses are selected to provide maximum wide-area coverage for SER and FR data?
   a. Do you prioritize any of the recommendations in Step 8 of Attachment 1?
   b. Do you have any additional considerations to avoid gaps in critical coverage and provide coverage of BES Elements that could propagate a Disturbance? (e.g., High-impact corridors or areas prone to cascading or widespread disturbances?)
   c. How does your entity document or record the rationale when engineering judgement is used?
      i. Does more than one engineer have input into the decision?
      ii. Is there a review process?

Control Activity B: Identify BES Elements for which DDR data is required to ensure adequate data to facilitate accurate event analysis (Relates to risk associated with R5) (RC)

1. How are asset inventories maintained to ensure accurate data for analysis of BES Disturbances?
   a. Does your entity have documented guidance on determining which BES Elements out of multiple require collection of DDR data?
   b. How do you ensure engineering judgement is technically sound?
2. How does your entity work with interconnected RCs to determine how to monitor the BES Elements that require DDR data?
   a. Do you maintain records of this coordination?
3. How does your entity determine which entity will provide DDR data for an interconnection between two Transmission Owners (TO), or a TO and a GO?
   a. Do you discuss the decision with the applicable entities?
4. Does your entity have a review process to ensure the selected Elements are reasonably expected to facilitate accurate event analysis?
   a. Are there multiple reviewers or SMEs involved?
   b. How do you document the review process?

Control Activity C: Reevaluate the identifications to address System changes since the previous evaluation. (Relates to risk associated with R1, R5)

1. What controls does your entity have in place to ensure the evaluations are conducted at least once every five calendar years?
2. Do you elect to conduct the evaluations more frequently than required?
3. Does your entity conduct any triggered reevaluations? If so, what would trigger a reevaluation?
   a. Significant new BES Elements?
   b. Changes in flows?
   c. Events?
   d. Other?
4. How do you track reevaluation deadlines and completion?

Control Objective 2: Ensure that the owners of the respective BES Elements are aware of their data recording responsibilities

Control Activity A: Determine responsibility for collection of SER or FR data for BES Elements directly connected to identified BES buses (Relates to risk associated with R1)

1. How does your entity determine whether an owner of a BES Element connected to an identified bus is required to collect SER or FR data or if you, as TO, have sufficient data?
2. Where there are multiple owners of equipment that comprise a BES bus, how does your entity determine which entities are responsible for collecting SER or FR data?
   a. How do you determine ownership of those BES Elements?
   b. How are shared responsibilities or boundaries between owners clearly defined?
3. Is there a technical review of the responsibilities around collection of SER or FR data?

4. Does your entity have a process or guidance on reassessing data collection responsibilities when ownership, configuration, or system topology changes?
   a. How are these changes communicated internally and to affected BES Element owners?

Control Activity B: Notify all owners of identified BES Elements within 90 calendar days of identification of BES buses or BES Elements for monitoring, that their respective BES Elements require SER, FR, or DDR data (Relates to risk associated with R1, R5)

1. What controls does your entity have in place to ensure the notifications are sent within the prescribed time frame?
   a. Do you use any technical controls?
   b. Do you have manual quality control checks?
   c. Do you elevate the tasks as the due date approaches?
2. How does your entity ensure the notifications were received?
   a. Do you require confirmation of receipt or use read receipts?
   b. How does your entity ensure the notification is understood?
   c. Is there ever a follow-up communication?
3. Does your entity have a tool for tracking notifications?
4. What documentation is retained to demonstrate that notifications were sent and received?

Control Objective 3: Record and maintain SER, FR, and DDR data to support event analysis.

Control Activity A: Ensure devices are installed and configured to collect required data. (Relates to risk associated with R2, R3, R6, R7)

1. How does your entity ensure devices are installed at the correct location to collect required data?
   a. Does your entity have a quality control step (e.g. reconciliation between notifications and devices)?
2. How does your entity document device configurations (e.g., single design standards, actual data recordings, station drawings)?
3. When notified of a new BES Element to monitor for disturbance data, how does your entity ensure devices are installed timely?
4. Is there a review or quality control step to ensure identified monitoring requirements are met with installed devices?
5. How does your entity ensure configuration documentation remains current after changes or maintenance?
6. How does your entity confirm newly installed devices are recording required data?

Control Activity B: Ensure record length and recording or sampling rate is sufficient to support disturbance analysis. (Relates to risk associated with R4, R8, R9)

1. How does your entity determine record length and sampling or recording rates?
   a. Do you configure devices for longer record length or more frequent recording or sampling rate than specified in the standard?

   b. Is the record length and sampling or recording rate consistent across your system?
   c. How do you identify configuration deviations?
2. Does your entity periodically check devices to ensure record length and recording rate are properly configured and functioning?
   a. If so, how often?

Control Activity C: Where data recording is not continuous, ensure appropriate triggers are set to yield useful data for disturbance analysis. (Relates to risk associated with R3, R4, R8)

1. Has your entity determined any additional triggers beyond those required by standard?
   a. If so, what triggers?
2. How do selected triggers support accurate disturbance analysis?
3. How do you validate triggers are functioning as intended at device commissioning?
4. Does your entity periodically check devices to ensure the triggers are properly configured and functioning?
   a. If so, how often?
5. How are trigger failures addressed?

Control Activity D: Ensure device clocks are synchronized and accurate (Relates to risk associated with R10)

1. How frequently does your entity review device clocks to ensure they are synchronized and accurate?
2. Does your entity use any technical controls to ensure device clocks are synchronized and accurate?
   a. Do you have alerts or alarms?
   b. Are there any automations to detect clock drift or synchronization issues?
3. How are clock accuracy issues documented and corrected?

Control Activity E: Ensure sufficient data is retained to allow for disturbance analysis. (Relates to risk associated with R11)

1. Does your entity periodically confirm data is being held for a minimum of 10 days?
   a. How often is retention capability verified?
   b. How do you ensure data is not overwritten or lost?
2. Does your entity proactively hold data for longer than 10 days based on the detection of an event, disturbance, or misoperation?

Control Activity F: Maintain Disturbance Monitoring Equipment.

1. How is DME maintenance managed?
   a. Is maintenance performed in conjunction with PRC-005 maintenance?
2. What criteria are used to define maintenance activities and timelines (e.g. IEEE, OEM recommendations)?
   a. Is verification of configuration files included in the maintenance activities?
   b. Are these maintenance results reviewed and documented?

Control Activity G: Timely restore recording capability after a failure (Relates to risk associated with R12)

1. How does your entity monitor for failure of recording capability?
   a. Do you have technical controls or a manual process?
   b. Do you monitor for changes to configured settings as well as recording capability?
2. How does your entity make decisions on repairing or replacing Disturbance Monitoring Equipment?
   a. Does your entity maintain a warehouse with spare DME for replacements?
3. How does your entity ensure the Regional Entity has received your Corrective Action Plan (CAP)?
   a. Do you require acknowledgment of receipt?
4. If the recording capability cannot be restored quickly, does your entity coordinate with your TO or RC to ensure appropriate coverage of the system until the capability can be restored?
5. How does your entity monitor implementation of CAP activities?
   a. Do you have periodic reviews to ensure milestones are being met?

Control Objective 4: Provide data to the RC, Regional Entity, or NERC

Control Activity A: Provide recorded data within 30 calendar days of a request unless an extension is granted by the requestor (Relates to risk associated with R11)

1. How does your entity ensure data is provided timely?
2. How are responsibilities assigned for fulfilling data requests?
3. Does your entity retain all data until confirmation of receipt is provided?
4. How are extensions requested, documented, and tracked?

Control Activity B: Ensure data is provided in the required format (Relates to risk associated with R11)

1. Does your DME provide data in the required format or does your entity need to use a conversion program to convert files into the required format?
   a. If conversion is required, how do you validate data integrity after the conversion?
2. Does your entity review data before sending it to the requesting entity to ensure all requested data is provided in the required format?
   a. How are errors identified and corrected before data submission?

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 accurately use the method in Attachment 1 to identify BES buses for which SER and FR data is required.

1. Does your entity have a review process to ensure the Attachment 1 methodology was correctly applied?

2. How do you ensure appropriate MVA values and system data are used?
3. Are multiple reviewers or engineers involved with utilizing the Attachment 1 methodology?
4. How are errors or discrepancies identified and corrected?

Potential Failure Point (R1): Failure to notify other owners of BES Elements directly connected to BES buses that SER or FR data is required for those BES Elements where the TO does not have SER or FR data within 90 days.

1. What controls does your entity have in place to ensure the notifications are sent within the prescribed time frame?

Potential Failure Point (R1): Failure to reevaluate all BES buses at least every five calendar years.

1. What controls does your entity have in place to ensure the evaluations are conducted at least once every five calendar years?
2. How do you ensure reevaluations include all applicable BES buses?

Potential Failure Point (R2): Failure to record and maintain the required SER data.

1. How does your entity detect loss of SER recording capability?
2. How is SER data retained and protected from loss?

Potential Failure Point (R3): Failure to record and maintain the FR data for each triggered FR as required.

1. Does your entity review triggered FR data to ensure recordings occurred as expected?
2. How are missed or incomplete FR recordings detected?

Potential Failure Point (R4): Failure to record FR data for the required length, recording cycle, and trigger settings.

1. How often are FR configurations reviewed or validated?
2. How are configuration deviations identified and corrected?

Potential Failure Point (R5): Failure to accurately identify BES Elements for which DDR data is required according to R5.1 and R5.2

1. Does your entity have a review process to ensure the R5.1 and R5.2 sub requirements were correctly applied?
2. How is coordination with interconnected entities documented?

Potential Failure Point (R5): Failure to notify owners of BES Elements within 90 days of determining DDR data is required.

1. What controls does your entity have in place to ensure the notifications are sent within the prescribed time frame?
2. How are notification records retained?

Potential Failure Point (R5): Failure to reevaluate all BES elements within the RC area at least every five calendar years.

1. What controls does your entity have in place to ensure the evaluations are conducted at least once every five calendar years?
2. How do you ensure reevaluations consider system changes?
3. How are reevaluation results reviewed and documented?

Potential Failure Point (R6): Failure to record and maintain DDR data to determine the electrical quantities listed in R6 for each BES Element it owns for which it received notification.

1. Does your entity have a control to detect loss of required DDR data channels?
2. How is DDR data retained and protected?

Potential Failure Point (R7): Failure to record and maintain DDR data to determine the electrical quantities listed in R7 for each BES Element it owns for which it received notification.

1. How does your entity validate DDR data accuracy?

Potential Failure Point (R8): Failure to have continuous data recording and storage of DDR data for equipment stalled after the effective date of PRC-002-2 (July 1, 2016 in the US).

1. How does your entity verify continuous recording capability is enabled and functioning?
2. How are interruptions in continuous recordings detected and addressed?

Potential Failure Point (R8): For equipment installed prior to the effective date of PRC-002-2 which does not have continuous data recording capability, failure to have triggered data recording that meets the specifications laid out in R8.

1. How does your entity confirm triggered recordings capture sufficient data?
2. How often are trigger configurations reviewed?

Potential Failure Point (R9): Failure to configure DDR recording device at the required input sampling rate and output recording rate.

1. How does your entity ensure DDR devices meet required input and output rates?
2. How are deviations identified and corrected?

Potential Failure Point (R10): Failure to time synchronize all SER, FR, and DDR data to Coordinated Universal Time (UTC) with clock accuracy within ± 2 milliseconds of UTC.

1. Are automated alerts or alarms used to detect synchronization issues?

Potential Failure Point (R11): Failure to configure SER, FR, and DDR devices such that data is retrievable for a minimum of 10 days.

1. How does your entity prevent data overwrite during disturbances?

Potential Failure Point (R11): Failure to provide SER, FR, and DDR data to the RC, Regional Entity, or NERC within 30 calendar days of a request unless an extension is granted by the requestor.

1. How does your entity ensure timely delivery?

Potential Failure Point (R11): Failure to provide SER, FR, and DDR data to the RC, Regional Entity, or NERC in the required format and with the required naming convention.

1. If data is converted from another format, how does your entity verify data for integrity before submission?

Potential Failure Point (R12): Failure to either restore recording capability or submit a CAP to the Regional Entity within 90 calendar days of discovering a failure of SER, FR, or DDR recording capability.

1. How are restoration timelines tracked and when required, how is a CAP developed and submitted?

Potential Failure Point (R12): Failure to implement a CAP within the timeline specified in the CAP.

1. How do you track CAP milestones?
2. Who is accountable for CAP implementation?
3. How is progress monitored and reported?

Potential Failure Point (R13): Have SER, FR, or DDR recording capabilities as applicable within three calendar years of either completing a reevaluation or receiving notification of identified BES Elements.

1. How do you track implementation timelines?
2. How is progress monitored towards completion?