Transmission System Planned Performance for Geomagnetic Disturbance Events

Long-Term Studies/Assessments

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 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; 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

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 Underfrequency Load Shedding (UFLS) and Under-voltage Load Shedding (UVLS) programs, and response to Geomagnetic Disturbance (GMD) events. Failure will likely result in gaps and may compromise BPS reliability and security.

During a GMD event, geomagnetically induced currents (GIC) may cause transformer hot-spot heating or damage, loss of Reactive Power sources, increased Reactive Power demand, and Misoperation(s), the combination of which may result in consequences such as low voltages, frequency decay, islanding, instability, uncontrolled separation, or Cascading within an Interconnection and blackout. TPL-007-4 establishes requirements for planning for GMD events so that shortcomings can be mitigated and the most severe potential impacts reduced or avoided.

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 TPL-007-4. You may want to consider these six objectives:

Control Objective 1: Identify and obtain data necessary to support the System models, GIC System models, and vulnerability assessments.

Control Objective 2: Maintain accurate System models and GIC System models of the planning area.

Control Objective 3: Complete GMD Vulnerability Assessments of the Near-Term Transmission

Planning Horizon.

Control Objective 4: Provide data and assessments in support of GMD planning.

Control Objective 5: Develop Corrective Action Plans (CAP) addressing how your system will meet performance requirements for the steady state planning GMD event.

Control Objective 6: Prepare to manage operations during a GMD event.

Reliability and Security Control Activities

Control activities are how your entity meets your control objectives. When designing and maturing 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 and obtain data necessary to support the System models, GIC System models, and vulnerability assessments. (PC, TP)

Control Activity A: Implement a process(es) to obtain data from Transmission Owners (TO) and Generator Owners (GO). (Relates to risk associated with R1)

1. How does your entity identify required data to support the System models, GIC System models, and vulnerability assessments.?
   a. Who is responsible for identifying the data required?
   b. Are there peer reviews (i.e., checks and balances) for data identification?
2. Is any additional GMD data (not specified in MOD-032-1 Attachment 1) collected as part of your MOD-032-1 data reporting process?
3. If not, what process is used to maintain specifications or criteria for the needed data to ensure consistent data across sources?
   a. How frequently are specifications reviewed?
4. How frequently does your entity request data be updated?
   a. Is it periodic (e.g., annually) or event-driven?
5. Do you identify a point in time when no further changes are incorporated into the system model to be used for a vulnerability assessment?

Control Activity B: Implement a process to obtain GMD measurement data (Relates to risk associated with R12, R13)

1. Where does your entity obtain GIC Monitor data?

   a. What criteria did you use to select the GIC monitor location(s)?
   b. How have you determined the data you collect is sufficient to validate the GIC model attributes used for a benchmark or supplemental event?
   c. Do you also use this data to predict the effects of specific geomagnetic storms that may occur?
2. From what source does your entity obtain geomagnetic field data?
   a. Do you validate the data with other sources (if available)?
3. What does your entity use for its ground conductivity models?
   a. How did you determine that this would be the most accurate ground model available?
   b. If your footprint overlaps ground models, how do you approach that within your assessment?

Control Activity C: Manage System model and vulnerability assessment data (Relates to risk associated with R1)

1. How does your entity maintain/track the data received?
   a. Do you use spreadsheets, databases, or other tracking tools?
   b. Do you have any alarms or alerts to ensure the timely collection and updates of information?
2. What QA/QC does your entity perform to ensure it obtains valid data? (i.e., steps taken to review data)
3. How does your entity address situations when it does not receive valid or updated data?

Control Objective 2: Maintain accurate System models and GIC System models of the planning area

Control Activity A: Develop and update System models and GIC System models of the responsible entity's planning area (Relates to risk associated with R2)

1. Does your entity have a documented process, checklist or other job aid to ensure completion of the tasks associated with maintaining accurate models of the planning area?
2. Does your entity have a control that triggers completion of these tasks to ensure they are completed timely?
3. Does your entity have a trained back-up SME identified who can perform the tasks?
4. Is there a process to do a quality check once the tasks are completed to ensure accuracy?

Control Activity B: Ensure the model represents the Facilities accurately for the period being studied for the GMD Vulnerability Assessments

1. How does your entity ensure the model represents a complete list of facilities in your planning area?
2. How frequently does your entity update Facilities included in the model?

Control Objective 3: Complete GMD Vulnerability Assessments of the Near-Term Transmission Planning Horizon

Control Activity A: Determine criteria for acceptable System steady state voltage performance for your entity's System during the GMD events (Relates to risk associated with R3)

1. Is there a documented process or checklist for these tasks?
    a. Is this the same as your FAC-014 planning assessment process?
    b. If not, what are the differences in the performance expectations?
2. Is there a process to do a quality check once the tasks are completed to ensure accuracy?

Control Activity B: Compute and provide benchmark and supplemental GIC flow information (Relates to risk associated with R5, R9)

1. How does your entity ensure GIC flows for benchmark and supplemental cases are calculated according to Attachment 1?
    a. Do you have a checklist or job aid to ensure considerations are properly applied?
2. How does your entity ensure GIC flows are useful for the thermal impact assessment of transformers?
    a. Do you coordinate with the respective TOs and GOs to ensure complete information is included?
3. How does your entity respond to and track requests for the effective GIC time series?
    a. Do you use any technical controls to track requests?
4. What process does your entity have in place to ensure all applicable TOs and GOs are provided with GIC flow information?
    a. Do you encrypt information in transit?
    b. Do you confirm receipt?
    c. What controls are in place to ensure contact information is current?

Control Activity C: Determine whether the system meets the performance requirements for the specified GMD cases. (Relates to risk associated with R4, R8)

1. What controls does your entity have in place to ensure the vulnerability assessment is based on accurate system models?
2. How does your entity ensure the system load conditions in R4.1 and R8.1 are met?
3. How does your entity determine reasonable study assumptions?
    a. What criteria is used to determine assumptions applied to vulnerability assessments?
    b. What differences are there between these criteria and other planning assessment assumption criteria?
    c. What assumptions are made about availability of Inverter-Based Resources?
    d. What generation and transmission outage criteria are used for the vulnerability assessments?

   e. Do you consider the differences in sensitivity or settings between protection systems?

4. How does your entity determine whether the System meets the performance requirements?
   a. What criteria determines the implementation of protection systems that may mitigate the impact to transformers?

Control Activity D: Document the vulnerability assessment and distribute it to relevant entities.

1. What quality control does your entity have in place to ensure all the required elements of the vulnerability assessment are documented in the assessments?
2. What method does your entity use to distribute the vulnerability assessments to relevant entities?
   a. Do you post it in a referenced place or send it directly to a contact at the entity?
   b. How do you ensure the entity receives the report?
3. What process does your entity have in place to receive requests for the report?
   a. How would an entity know who to contact to request the report?
4. What process does your entity have in place to receive comments and track responses?
   a. Do you use any technical controls to track comments and their responses?

Control Objective 4: Provide data and assessments in support of GMD planning (TO/GO)

Control Activity A: Provide requested information. (Relates to risk associated with R1, R6, R10)

1. Has your entity identified its Transmission Planner(s) (TP) and Planning Coordinator(s)(PC)?
2. Have your entity's PC(s) or TP(s) identified you as being a responsible party (data holder) in their PC/TP GMD planning process (per R1)?
   a. If you own applicable transformers and have not been asked by a PC or TP to provide data, how do you identify the appropriate TP/PC for inclusion in the assessment?
3. Does your entity have a documented process for providing information? Does it include:
   a. Responsibilities for data identified in the R1 process?
   b. The thermal impact assessments?
   c. Providing comments on the vulnerability assessment?
   d. Providing comments on CAPs?

Control Activity B: Conduct Thermal Impact Assessments. (Relates to risk associated with R6, R10)

1. Does your entity have a documented process to conduct thermal impact assessments?
   a. Do you have a checklist or other job aid?
2. How does your entity identify jointly owned facilities?
   a. How do you coordinate with joint owners to conduct the assessments?
3. What criteria does your entity use to determine assumptions applied to thermal impact assessments?
   a. What is the difference between that criteria and other planning assessments?

4. What criteria does your entity use to determine mitigation efforts based on the results of the thermal impact assessments?
5. Does your entity have a review or quality control step to ensure the completeness and quality of the resulting assessment?

Control Objective 5: Develop Corrective Action Plans (CAP) addressing how your system will meet performance requirements for the steady state planning GMD event.

Control Activity A: Define a process with responsibilities for developing a CAP. (Relates to risk associated with R1, R7, R11)

1. Which registered entities are responsible for developing a CAP if the system does not meet the performance requirements?
    a. Is there a coordination process for CAP development when multiple parties need corrective actions?
    b. Do affected parties that are not responsible for the development of the CAP have input into the development?
2. What resolution process is in place where corrective action considerations may vary between parties?
3. Are procedures and timelines for completion, distribution, comments, and response to comments documented?

Control Activity B: Ensure the CAP is complete and mitigates the identified vulnerability (Relates to risk associated with R7, R11)

1. Is there documented process or checklist for the development of a CAP?
2. Does your CAP also include Operating Procedures for emergency response in the case of a GMD event?
3. Does your entity have any review or quality control steps to ensure the CAP is complete and meets the stated objective?

Control Activity C: Implement and track the CAP to completion. (Relates to risk associated with R7, R11)

1. Does your entity have a resolution process to address disagreements regarding a CAP developed by another party that affects your entity?
2. How does your entity track a CAP to completion?
    a. Do you utilize any technical controls?
3. Does your entity establish timelines for CAP completion?
4. Does your entity understand and follow the CEA process to submit a CAP to the CEA if a request for extension of the time is required?
    a. What internal controls does your entity have in place to support the CEA CAP process?

Control Objective 6: Prepare to manage operations during a GMD event

Control Activity A: Establish Operating Procedures to provide operations personnel and all other affected personnel with detailed and clear instructions on how to respond during GMD events.

1. Does your entity have defined responsibilities to prepare for predicted GMD events?
    a. Have you defined data specifications and responsibilities for monitoring GMD data?
    b. Do you have any displays for operations personnel for GIC flow/data information?
    c. What methods and tools do you use to predict and receive early warnings of upcoming GMD events?
2. Has your entity developed checklists or other job aids for personnel with responsibilities to respond during events?
3. Do your Operating Procedures include coordination activities with other interconnected entities, TOs, TOPs, BAs, and Reliability Coordinators (RC) before and during GMD events to maintain the reliability of the BPS?
4. How are operations personnel and all other affected personnel trained to respond during GMD events?

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 responsibilities of the PC and TP.

1. Have the PC and all associated TP been identified?
2. Is there a document (process or MOU) that:
    a. Identifies all responsible parties?
    b. Identifies joint and individual tasks and the timetable for completing each task?
    c. Identifies the owner of the document?
    d. Is approved or signed by all identified responsible parties?
    e. Has an identified review and revision process included in the document?
3. Is the party responsible for maintaining the GIC model identified along with the associated tasks?
4. Are the responsible parties that are required to implement processes to obtain GMD measurement data clearly identified?

Potential Failure Point (R2): Failure to maintain System models and GIC System models of the responsible entity's planning area.

Potential Failure Point (R3): Failure to maintain criteria for acceptable System steady state voltage

performance for its System during GMD events.

Potential Failure Point (R4, R8): Failure to complete a benchmark and supplemental GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon at least once every 60 calendar months.

1. Is there a trigger to initiate the benchmark and supplemental assessments every 60 calendar months? Who is responsible to maintain the trigger?
2. Is there a backup SME who is also getting the notification to start this process (if the Primary SME is gone/sick)?
3. Are there job aids to ensure the assessment(s) are completed at least once every 60 calendar months?

Potential Failure Point (R4, R8): Failure to include the conditions outlined in Requirement R4 Part 4.1, Requirement R8 Part 8.1, and Attachment 1 in the GMD Vulnerability Assessments.

Potential Failure Point (R4, R8): Failure to provide the GMD Vulnerability Assessment to the RC, adjacent PCs, and adjacent TPs within 90 calendar days of completion or to other entities within 90 days of receipt of a written request.

1. Is there a process to document and maintain contacts with the RC, adjacent PCs, and adjacent TPs?
2. Is there a process to document delivery of the assessment to required parties within 90 days of completion and/or response to any request for the assessment?

Potential Failure Point (R4, R7, R8, R11): Failure to provide a documented response within 90 calendar days of receipt of comments on the GMD Vulnerability Assessment or CAP.

1. Is there a process to document delivery of the response to required parties within 90 days of receipt of the comments?
2. Does your entity use a technical control to track the progress and delivery of the response to ensure the timeline is met?

Potential Failure Point (R5, R9): Failure to provide GIC maximum effective GIC value to each TO and GO that owns an applicable Bulk Electric System (BES) power transformer in the planning area.

Potential Failure Point (R5, R9): Failure to provide the effective time series, GIC(t) calculation in response to a written request from the TO or GO within 90 calendar days of receipt of the request.

Potential Failure Point (R6, R10): Failure to conduct a thermal impact assessment for applicable BES power transformers where the maximum effective GIC value is 75 A (benchmark) or 85 A (supplemental) per phase or greater.

Potential Failure Point (R6, R10): Failure to provide thermal impact assessment to the PC/TP (from Requirement R1) within 24 calendar months of receiving GIC flow information.

1. Does your entity use a technical control to track the progress and delivery to ensure the timeline is met?

Potential Failure Point (R7, R11): Failure to develop a CAP where the System does not meet the performance requirements within one year of completing the GMD Vulnerability Assessment.

Potential Failure Point (R7, R11): Failure to include a timetable for implementing the selected actions specifying the implementation of non-hardware mitigation, if any, within two years of development of the CAP; and implementation of hardware mitigation, if any, within four years of development of the CAP.

Potential Failure Point (R7, R11): Failure to request approval from the Compliance Enforcement Authority (CEA) for any extension required.

Potential Failure Point (R7, R11): Failure to provide CAP to the RC, adjacent PC(s), adjacent TP(s), and functional entities referenced in the CAP within 90 calendar days of development or revision or to other entities within 90 calendar days of receipt of a written request.

Potential Failure Point (R12): Failure to implement a process to obtain GIC monitor data from at least one GIC monitor located in the PC planning area or other part of the system included in the PC GIC System model.

Potential Failure Point (R13): Failure to implement a process to obtain geomagnetic field data for the planning area.