Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points

CIP-014-3

Asset/System Identification
Identity Management and Access Control
Asset/System Physical Protection
Long-term 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.

Critical Transmission stations and Transmission substations: *For the purpose of this document*, transmission stations, and substations that, if rendered inoperable or damaged by a physical attack, could adversely affect BPS reliability and security.

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

Asset/System Identification: Identifying and tracking assets and Bulk Electric System (BES) Facilities is critical to Bulk Power System (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.

Identity Management and Access Control: Entities must develop controls to prevent or mitigate malicious or unintentional access to BES Cyber Assets. Failure to develop controls may compromise the integrity and operability of the BPS. The three major security control tenets are confidentiality, integrity, and availability (CIA).

Asset/System Physical Protection: Failure to physically protect BES assets could lead to access by unauthorized personnel leading to actions resulting in instability, uncontrolled separation, or Cascading within an interconnection.

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 System Operating Limits (SOL) and transfer capabilities, analysis of disturbances and misoperations, proper design of underfrequency load shedding (UFLS) and undervoltage load shedding (UVLS) programs, and response to Geomagnetic Disturbance (GMD) events. Failure will likely result in gaps and may compromise BPS reliability and security.

Identifying and protecting Transmission stations, Transmission substations, and their associated primary control centers prevents instability, uncontrolled separation, or Cascading within an interconnection that could result from a physical attack.

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 CIP-014-3. You may want to consider these four objectives:

Control Objective 1: Identify critical Transmission stations and Transmission substations (those that, if rendered inoperable or damaged by a physical attack, could adversely affect BPS reliability and security). (Relates to Asset/System Identification)

Control Objective 2: Evaluate potential threats/vulnerabilities of a physical attack on critical

Transmission stations and Transmission substations and Control Centers. (Relates to Long-term Studies/Assessments)

Control Objective 3: Protect critical Transmission stations, Transmission substations, and associated control centers (Relates to Identity Management and Access Control and Asset/System Physical Protection)

Control Objective 4: Update risk assessments, threat evaluations, and physical security plans based on system or threat landscape changes. (Relates to Long-term Studies/Assessments)

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: Identify critical Transmission stations and Transmission substations (those that, if rendered inoperable or damaged by a physical attack, could adversely affect BPS reliability and security).

Control Activity A: Identify applicable Transmission stations and Transmission substations to include in risk assessments. (Relates to risk associated with R1)

1. How does your entity identify existing Transmission stations and Transmission substations that should be included in risk assessments?
2. How does your entity confirm you include all Transmission Facilities that could be subject to a common physical attack in the calculation of line weighting, such as:
   a) Jointly owned Transmission station(s) and Transmission substation(s).
   b) Physically adjacent separately owned Transmission station(s) and Transmission substation(s).
3. How does your entity ensure accurate Transmission line information is used for the calculation of line weighting, including lines at:
   a) Solely owned Transmission station(s) and Transmission substation(s),
   b) Jointly owned Transmission station(s) and Transmission substation(s), and
   c) Physically adjacent separately owned Transmission station(s) and Transmission substation(s)?
4. How does your entity identify applicable Transmission stations and Transmission substations planned to go into service within 24 months?
5. How does your entity remove Transmission stations and Transmission substations that are no

longer applicable to risk assessments?

6. What QA/QC does your entity perform to confirm all applicable Transmission stations and Transmission substations were included in risk assessments?

Control Activity B: Perform risk assessments to identify critical Transmission stations, Transmission substations, and associated control centers. (Relates to risk associated with R1)

1. How does your entity perform risk assessments to identify critical Transmission stations and Transmission substations?
2. What models/methods does your entity use to evaluate whether rendering a Transmission station or substation inoperable or damaging it by a physical attack could result in:
    a. Instability,
    b. Uncontrolled separation, or
    c. Cascading within an interconnection?
3. How does your entity ensure models are complete and accurate?
    a. How do you ensure neighboring entities' planned projects are included in your model as applicable?
    b. How do you ensure that your model accurately reflects the behavior of the interconnection? Does it include:
        i. Summer peak and winter peak load levels,
        ii. Shoulder peak load levels with system transfers,
        iii. Alternative generation dispatch assumptions or scenarios,
        iv. Alternative end-use consumer models, or
        v. Unavailability of BES Facility that has an impact on risk assessment?
4. How does your entity identify associated control center(s) of critical Transmission stations and Transmission substations?
5. How does your entity remove Transmission stations and Transmission substations that are no longer deemed critical?
6. How does your entity verify that selected models were appropriate, and the assessment was performed correctly? (i.e., What internal QA/QC does your entity perform on the assessment?)

Control Activity C: Ensure the third party chosen to verify a risk assessment has the proper skills to perform a satisfactory review. (Relates to risk associated with R2)

1. How does your entity determine the third party chosen to verify your risk assessment has the proper skills to perform a satisfactory review?
2. What QA/QC does your entity perform to verify the third party has the proper skills to achieve a satisfactory review?
    a. Do you verify affiliation, experience, or registration?

Control Activity D: Ensure the third party verifying the risk assessment properly assessed the risks.

(Relates to risk associated with R2)

1. How does your entity determine whether the third-party risk assessment was conducted with sufficient rigor to assess the risk to the reliability and security of the BPS from rendering a given Transmission station or Transmission Substation inoperable or damaging it by a physical attack?
2. If the third-party reviewer's assessment methods differ from your entity's, how do you document and reconcile the differences?
3. What QA/QC does your entity perform to verify the third-party risk assessment was comprehensive?

Control Activity E: Respond to recommendations from the third party. (Relates to risk associated with R2)

1. How does your entity assess whether you should modify your identification of critical Transmission stations and Transmission substations consistent with the third party's recommendation?
2. How does your entity verify you appropriately responded to recommendations from the third party?

Control Activity F: Timely notify the Transmission Operator (TOP) with operational control of the primary control center of identified critical Transmission station(s) and Transmission substation(s). (Relates to risk associated with R3)

1. How does your entity notify the TOP with operational control of the primary control center of identified critical Transmission station(s) and/or Transmission substation(s) (if your entity does not operate the control center)?
    a. What QA/QC do you have in place to verify you timely notified the TOP?
1. How does your entity timely notify the TOP with operational control of the primary control center of a critical Transmission station and/or Transmission substation that is no longer deemed critical in your risk assessments?
    a. What QA/QC do you have in place to verify you timely notified the TOP?
2. How does your entity track the correct contact(s) to notify when you identify control centers and ensure your contact information is up to date?

Control Objective 2: Evaluate potential threats/vulnerabilities of a physical attack on critical Transmission stations and Transmission substations and control centers.

Control Activity A: Select a method to evaluate potential threats/vulnerabilities of a physical attack on critical Transmission stations, Transmission substations, and control centers. (Relates to risk associated with R4)

1. What methods does your entity use to evaluate potential threats/vulnerabilities?
    a. Does your analysis include the possibility, probability, and impact of physical attack vectors?
    b. Do you develop or define a way to assess physical threats/vulnerabilities and threat sources to identify physical attack scenarios?

   c. How do you determine appropriate threat sources?
   d. How do you ensure threat sources are not too narrowly or too broadly defined to provide meaningful and timely information?
   e. Do you use established tools like Design Basis Threat (DBT), CARVER, or adversary sequence diagrams?
   f. Do you include the unique characteristics of individual site topography, external business, and criminal activities in defining vulnerabilities?

Control Activity B: Identify potential threats/vulnerabilities of a physical attack on critical Transmission stations, Transmission substations, and control centers. (Relates to risk associated with R4)

1. How does your entity ensure appropriate resources are consulted for the threat evaluation?
   a. What internal groups are involved in identifying potential threats and vulnerabilities?
   b. How do you document and assess a history of physical security incidents of your own Transmission stations and Transmission substations or those of adjacent or partner entities or on a regional basis?
   c. Do you identify unique sites or facility-specific threats/vulnerabilities?
   d. Does your process include local, statewide, and national data regarding the history of physical attacks?
   e. Do you use established threat sources (ERO, ES-ISAC, government, etc.) for intelligence or threat warnings?
2. How does your entity communicate identified vulnerabilities for inclusion in your physical security plan?
3. What QA/QC does your entity perform to verify you properly evaluated potential threats/vulnerabilities of a physical attack to critical Transmission stations, Transmission substations, and associated control centers?

Control Objective 3: Protect critical Transmission stations, Transmission substations, and associated control centers.

Control Activity A: Develop and implement a physical security plan (Plan) addressing the threats/vulnerabilities identified for critical Transmission stations, Transmission substations, and associated control centers. (Relates to risk associated with R5)

1. How does your entity ensure the Plan examines and reasonably mitigates risks to *each identified asset*?
2. How does your entity ensure it based its Plan on *the entire list of prioritized threats and vulnerabilities* in your evaluation of potential physical attack threats/vulnerabilities?
   a. How do you evaluate and document your rationale for including, excluding, and prioritizing potential physical attacks for further consideration?
3. How does your entity select physical security systems or solutions that address the

threats/vulnerabilities identified in your evaluation and that

a. Do not consist of standard corporate security solutions (e.g., a security feature exists, but its purpose is undefined, and you have no criteria to determine its effectiveness)?

b. Do not simply document maintenance/repair of existing security measures without an identifiable purpose?

c. Are based on effectiveness, not least cost?

4. How does your entity ensure physical security measures collectively deter, detect, delay, assess, communicate, and respond to threats/vulnerabilities identified in your evaluation of potential physical attack threats/vulnerabilities?
   a. Do you develop physical attack countermeasures at the asset and site levels?
   b. Does your Plan include a matrix, narrative, or both that accurately describe the solutions' effectiveness based on specific attack scenarios?
   c. How do you ensure the Plan includes best practice principles (defense in depth, differing but complementary security measures, etc.)?
5. How does your entity account for threats or vulnerabilities that may increase due to external conditions (e.g., weather; time of day; social, political, or economic pressures)?
6. How does your entity ensure personnel assigned responsibilities in the Plan have the authority and resources to design, deploy, and maintain their parts of the security plan?
   a. Does your Plan address the budget for system testing, maintenance, and end of life?
7. How does your entity ensure personnel asked to design, deploy, and maintain parts of the security plan are qualified, trained, certified, and supported for relevant ongoing training and education?
8. How does your entity ensure selected security solutions (people, process, technology, physical barriers) are appropriate to mitigate identified threats and vulnerabilities?
9. Has your entity developed a process to critically evaluate and verify your Plan through external expertise, industry benchmarking, or best practices?
10. How does your entity ensure the Plan accounts for unmitigated risks and contains a process for future mitigation as solutions become available?
11. Does your entity conduct penetration testing based on identified threats and vulnerabilities?
    a. Do you conduct tabletop exercises based on identified threats and vulnerabilities?
    b. Do you verify the proper performance of your Plan in some way?
12. What QA/QC processes does your entity have in place with your Plan?

Control Activity B: Coordinate assessment and response activities with internal and external resources (law enforcement, neighboring entities, vendors, etc.). (Relates to risk associated with R5)

1. How does your entity communicate and coordinate before, during, and after a physical attack?
2. How does your entity ensure your Plan optimizes first responders' safety, familiarity, response time, and capability?
3. How does your entity train personnel or exercise/validate your Plan?

4. How does your entity coordinate a response plan for physical attacks?
5. What QA/QC does your entity perform in connection with the above-referenced activities?

Control Activity C: Ensure meaningful third-party Plan review. (Relates to risk associated with R6)

1. How does your entity select the third party to review your Plan?
   a. How do you ensure the third party has the proper expertise to perform a satisfactory review of your Plan?
   b. How do you ensure the reviewer is fair but critical, unbiased, and unaffiliated?
   c. What verification do you perform to ensure the selected third party has the proper skills to perform a satisfactory review?
2. How does your entity ensure the third party chosen to review your Plan performed a satisfactory review?
   a. Do you require reviewers to conduct an on-site physical security assessment?
   b. Do you have a defined review process to ensure the review consists of more than a certification that the third-party reviewed your Plan and identified no problems?
   c. Is the reviewer required to document the breadth of expertise and credentials of internal and external SMEs contributing to the review?
3. How does your entity ensure the third-party reviewer conducted a detailed security analysis and, when appropriate, made recommendations to augment weak or non-existent security solutions?
   a. Do you define criteria for review to ensure the third-party review is substantive and not simply an attestation the third-party performed a review?
   b. Do you have a process to ensure a review or evaluation includes a detailed narrative or rationale supporting the Plan or justifications for declining to make recommendations for the Plan?
4. What QA/QC does your entity perform to ensure the third party that reviewed your Plan performed a satisfactory review?

Control Activity D: Respond to recommendations from the third party regarding the Plan. (Relates to risk associated with R6)

1. How does your entity determine whether you will modify your Plan consistent with Plan review recommendations?
   a. How do you ensure internal or external expertise to properly assess the third party’s recommendations?
2. How does your entity properly prioritize recommendations and adjust plans and solutions to solve potential security gaps?
   a. Do you define criteria for rejecting recommendations?
   b. Do you provide a rationale when you conclude proposed changes are unnecessary?
3. What QA/QC process does your entity employ to verify you appropriately responded to recommendations from the third party?

Control Activity E: Protect critical infrastructure information from disclosure when using a third-party reviewer/assessor. (Relates to risk associated with R2, R6)

1. How does your entity protect critical infrastructure information from disclosure?
    a. Do you have a method for identifying documents containing critical infrastructure information that require confidential treatment?
    b. Do you have procedures for protecting or exempting critical infrastructure information provided to third-party reviewers/assessors from disclosure?
        i. Do you use non-disclosure agreements?
        ii. Do you use information protection policies or training?
        iii. Do the policies include protections for data in transit?
2. How does your entity verify the third party adequately protects your critical infrastructure information from disclosure?

Control Objective 4: Update risk assessments, threat evaluations, and physical security plans based on system or threat landscape changes.

Control Activity A: Timely reevaluate your entity's system based on new equipment or topology changes. (Relates to risk associated with R1)

1. How does your entity timely reevaluate your identification of critical Transmission station(s), Transmission substation(s), and associated primary control center(s) based on new equipment or topology changes?
    a. What triggers have you identified that would require an updated risk assessment?
    b. Do you have a change control process that feeds this reevaluation?
    c. Do you monitor for changes to connected entities that could affect this identification?
2. How does your entity verify you timely reevaluate your system based on system changes?

Control Activity B: Timely reevaluate your entity's potential threats and vulnerabilities based on a new threat landscape. (Relates to risk associated with R4)

1. How does your entity timely reevaluate your entity's potential threats and vulnerabilities based on a new threat landscape?
    a. What triggers have you identified that would require an updated threat evaluation?
    b. Do you have a change control process that feeds this reevaluation when specified changes are made at critical Transmission station(s), Transmission substation(s), and associated primary control center(s)
    c. Do you monitor for emerging threats/vulnerabilities?
2. How does your entity verify you timely reevaluate your threat evaluation when changes in the threat landscape occur?

Control Activity C: Timely update your entity's physical security plan(s) based on updated evaluations, new equipment, or threat landscape changes. (Relates to risk associated with R5)

3. How does your entity timely update your physical security plans when relevant changes occur?
    a. What triggers have you identified that would require an updated physical security plan?
    b. Do you have a change control process that feeds an update of the physical security plan at critical Transmission station(s), Transmission substation(s), and associated primary control center(s)
4. How does your entity verify whether you timely updated your physical security plan(s) when relevant changes occur?

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, R5, R6): Failure to clearly define or communicate start and end dates used to establish time frame(s) for initiation, review, and approval processes.

1. How does your entity document time frames for:
    a. (R1) Stations and substations planned to be in service within 24 months?
    b. (R1.1) Subsequent risk assessments performed at least once every 30 calendar months?
    c. (R1.1) Subsequent risk assessments performed at least once every 60 calendar months?
    d. (R2) Verification completed within 90 calendar days following the completion of R1 risk assessment?
    e. (R2.3) Response to verification within 60 calendar days of completing the verification?
    f. (R3) Notify the Transmission Operator that has operational control within seven calendar days following completion of Requirement R2?
    g. (R5) Physical security plan(s) developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s)?
    h. (R6.2) Third-party review completed within 90 calendar days of completing the security plan(s) developed in Requirement R4?
    i. (R6.3) Response to third-party review within 60 calendar days of completing the unaffiliated third-party review?
2. How does your entity track deadlines for CIP-014?
3. If your processes involve multiple groups internally, how does your entity coordinate between the groups so that timelines dependent on other activities are not miscalculated?
4. What QA/QC mechanisms are in place to ensure deadlines are met?

Potential Failure Point (R1): Failure to identify one or more critical Transmission stations and Transmission substations.

1. How does your entity document your determination of applicable Transmission stations and

Transmission substations?
2. How does your entity document risk assessments?
3. How does your entity document the division of CIP-014 responsibilities when Transmission stations and substations are jointly owned?

Potential Failure Point (R2): Failure to respond appropriately to recommendations from the third-party verification.

1. How does your entity document your response to third-party verification recommendations?
2. If you opt not to modify your identifications consistent with the third party's recommendation, how does your entity document the technical basis for that decision?

Potential Failure Point (R4): Failure to develop a documented physical security plan(s) that correlates the specific threats and vulnerabilities identified in R4 with the entity's mitigation efforts.

1. Has your entity implemented a documented physical security plan(s) for all critical Transmission station(s), Transmission substation(s), and associated primary control center(s)?
2. If yes, does your entity's Plan include the following:
   a. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities;
   b. Law enforcement contact and coordination information;
   c. A timeline for executing the physical security enhancements and modifications specified in the physical security plan; and
   d. Provisions to evaluate evolving physical threats and their corresponding security measures to the Transmission station(s), Transmission substation(s), or primary control center(s)?

Potential Failure Point (R5): Failure to document one or more physical security plans containing all the elements in the standard requirement.

1. Do your entity's physical security plans cover all identified critical Transmission stations, Transmission substations, or primary control centers?
2. Are all potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4 mitigated in the physical security plan(s)?
3. Does your entity's physical security plan(s) include:
   e. Law enforcement contact and coordination information,
   f. A timeline for executing the physical security enhancements and modifications specified in the physical security plan, and
   g. Provisions to evaluate evolving physical threats and their corresponding security measures to the Transmission station(s), Transmission substation(s), or primary control center(s)?

Potential Failure Point (R6): Failure to respond appropriately to recommendations from the third-party review.

1. How does your entity document your response to recommendations from the third-party review to ensure all recommendations are considered?
2. If your entity opts not to modify your identifications consistent with the third party's recommendation, how do you document the technical basis for that decision?