Electric Reliability and Security for the West

Internal Controls
Failure Points and Guidance Questions
CIP-002-5.1a R1, R2

Security Objective

To develop and maintain an inventory of identified and categorized BES Cyber Systems (BCS) and associated BES Cyber Assets (BCA) to ensure protections are given as required by the CIP Reliability Standards.

NIST Special Publication 800-53 (Rev. 4) PM-5

WECC Intent

The potential failure points and guidance questions give direction to registered entities for assessment of risk, while designing internal controls specific to NERC Reliability Standards and Requirements. The Registered Entity may use this document as a starting point in determining entity risk. It is not WECC's intent to establish a standard or baseline for entity risk assessment or controls design.

Note: *Guidance questions help an entity understand and document its controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance at audit.*

**Please send feedback to ICE@WECC.org with suggestions on potential failure points and guidance questions.*

General Failure Point

Potential Failure Point (R1, R2): Failure to develop documentation guidelines for R1 R2 results

Potential Failure Points and Guidance Questions

CIP-002-5.1a R1

Potential Failure Point (R1): Failure to understand shared compliance responsibilities with another Responsible Entity.

1. How do you document your shared compliance responsibilities?
2. How do you document your shared responsibilities?

Potential Failure Point (R1): Failure to develop or implement a process that provides asset determination guidance.

1. How do your process for identifications ensure that all of asset types in Parts R1.i through R1.vi are considered during the determination process?
   a. How do you verify all asset types in Parts R1.i through R1.vi are evaluated?

2. How does your R1 process apply the Impact Rating Criteria to the asset types identified in Parts R1.i through R1.vi to develop your R1.1, R1.2, and R1.3 lists?
3. How are results documented?
    a. As applicable, how are null identifications (e.g., no high-impact BCS) documented?

Potential Failure Point (R1): Failure to evaluate and identify Cyber Assets that support one or more reliability tasks for the purposes of BES Cyber System identification.

1. How do you document the evaluation of BES reliability operating services (BROS) for the purposes of BCS and BCA identification?
    a. If applicable, have you evaluated the Voice Over Internet Protocol (VOIP) assets (per NERC Voice Communications in a CIP Environment—Implementation Recommendation, May 22, 2017) in the BES Asset identification process?
        i. How do you document the evaluation?
2. How do you track real-time operational uses of systems or data that may have an impact on asset classification? For example, uses of one or more of the BROS: Dynamic Response to BES conditions, Balancing Load and Generation, Controlling Frequency (Real Power), Controlling Voltage (Reactive Power), Managing Constraints, Monitoring & Control, Restoration of BES, Situational Awareness, and Inter-Entity Real-Time Coordination and Communication.

Potential Failure Point (R1): Failure to outline a method for updates.

1. How do you track future projects and asset development to ensure that assets are reviewed for identifications per R1?
2. How do you update R1 identifications?
    a. How do you communicate any changes to stakeholders?

CIP-002-5.1a R2

Potential Failure Point (R2): Failure to clearly define or communicate start and end dates used to establish a period for review and approvals.

1. How do you define review and approval periods?

Potential Failure Point (R2): Failure to outline a method for performing reviews .

1. How do you review the identifications in R1?
2. How do you ensure a review occurs at least every 15 calendar months?
    a. How is this review documented?
        i. What automated tools, if any, do you use to track periodic review and approval performance?

Potential Failure Point (R2): Failure to outline a method for approvals.

1. How do you ensure a CIP Senior Manager or approved delegate approves the identifications required by R1?
    a. How does this approval occur if there are no identified changes in R1 lists?
2. How do you ensure an approval occurs at least once every 15 calendar months?
    a. How do you document this approval?

Potential Failure Point (R2): Failure to clearly define delegated responsibility.

1. If applicable, how has delegation for the approvals been outlined, documented, and communicated?