Electric Reliability and Security for the West

Internal Controls
Failure Points and Guidance Questions
CIP-004-6 R4

Security Objective

Establishes conditions for group and role membership. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. Requires approvals by organization-defined personnel or roles for requests to create information system accounts as necessary to support organizational missions and business functions.

NIST Special Publication 800-53 (Rev. 4) AC-2, AC-3(7), AC-6

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.*

Potential Failure Points & Guidance Questions

Potential Failure Point: Failure to define "need" and ensure the definition is consistently applied throughout the business.

1. How have you defined criteria to determine whether access is needed?
   a. How do you consider an individual's role, function, or risk, when determining need?
2. Does your needs-based approach follow an industry standard?

Potential Failure Point: Failure to develop criteria to be used to define a CIP Exceptional Circumstance.

1. How have you defined CIP Exceptional Circumstances?
2. How do you communicate Exceptional Circumstances to the line of business?
3. How do you ensure that a CIP Exceptional Circumstance is officially determined before authorizing access based on need?

Potential Failure Point: Failure to define a process to authorize access.

1. Have you defined what constitutes a record of authorization?
    a. How do you ensure authorization records are documented consistently?
2. Have you defined workflows that show the authorization process?
3. How are the personnel responsible for authorizing access made aware of their responsibilities?

Potential Failure Point: Failure to develop a process for designating and identifying designated storage locations for BES Cyber System Information.

1. How have you defined physical storage locations?
2. How have you defined electronic storage locations?
3. What is your process for identifying information that qualifies as BES Cyber System Information?
4. What is your process to document designated storage locations for BES Cyber System Information?
    a. What is your process to ensure that the list of storage locations is kept up to date?
5. How do you ensure that all contractors or service vendors are aware of defined BES Cyber System Information?
    a. What controls are in place to ensure PRA and training have been conducted before access is granted?

Potential Failure Point: Failure to develop a procedure on how to perform quarterly and 15-calendar month verifications.

1. How have you established a method to determine authorized access?
    a. Does your procedure consider a separation of duties for verifications?
2. How have you established a method to determine actual access?
    a. How do you ensure all actual access is considered during the review process?
    b. How do you ensure the correct privileges are being reviewed?
    c. How do you document the results of the reviews?

Potential Failure Point: Failure to clearly define or communicate start and end dates used to establish timeframes in verification process.

1. How does each line of business establish these start and end dates?