Internal Controls
Failure Points and Guidance Questions
CIP-004-6 R3

Security Objective

The organization develops, applies, and manages an assessment program to understand individual risk profiles. By identifying each individual by organization-defined risk characteristic and management of individual status, the organization can establish authorization criteria to manage its access risk to protected systems.

NIST Special Publication 800-53 (Rev. 4) IA-4(4)

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 develop evaluation methodology or parameters for authorization process.

1. What criterion is used in the risk assessment process?
2. What criterion is used to determine acceptability in the authorization process?

Potential Failure Point: Failure to develop a process for performing the personnel risk assessment (PRA).

1. How do you ensure all elements of R3 are addressed in the PRA process?
   a. How do you ensure that the evaluators consistently and effectively apply the documented criteria or processes?
   b. What specialized training or qualifications do you have to perform this evaluation?

Potential Failure Point: Failure to develop a process to track PRA before giving access.

1. How do you verify completion of the PRA before giving electronic or unescorted physical access?
    a. Who, or what role, is responsible for provisioning access?
    b. How is that individual trained or made aware of the process to give access?
    c. If the individual who normally performs this task is not available, how do you ensure that that person has qualified backup?
2. Describe any oversight of this activity (such as peer review or manager sign-off) designed to prevent or detect an error in provisioning access.

Potential Failure Point: Failure to develop a personnel risk assessment (PRA) process that addresses contractors or service vendors.

1. How do you ensure that all contractors or service vendors are evaluated?

Potential Failure Point: Failure to clearly define or communicate start and end dates used to establish a timeframe for management of PRA process.

1. How do you ensure that individuals who need an updated PRA are identified before the seven-year deadline?
2. Describe your process for scheduling PRAs to ensure that the process is completed before the due date.
3. What measures do you have in place to detect and correct PRAs not completed by the seven-year deadline?
    a. Is there an escalation process to revoke authorized electronic and authorized unescorted physical access before the deadline?
    b. Is there an escalation process to revoke contractor or vendor authorized electronic and authorized unescorted physical access before the deadline?