Electric Reliability and Security for the West

Internal Controls
Failure Points and Guidance Questions
CIP-004-6 R2

Security Objective

- Develops, documents, and disseminates a Cyber Security Training Program to organization-defined personnel or roles. The program must address—
  - Purpose;
  - Scope;
  - Roles;
  - Responsibilities;
  - Management commitment;
  - Coordination among organizational entities; and
  - Required compliance.
- Develop procedures to put in place the Cyber Security Training Program, training controls, reviews, and updates.

NIST Special Publication 800-53 (Rev. 4) AT-1, 2

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 and deliver cybersecurity training that includes all required contents.

1. How do you review processes to make sure that the training program is comprehensive and relevant (Part 2.1)?
   a. How does your training program adapt to changing cybersecurity risks?
2. How do you track cybersecurity training progress (Part 2.1)?

a. How do you ensure an individual's training status (complete or incomplete) is documented?

Potential Failure Point: Failure to develop a process to verify training is complete before giving access.

1. How do you verify all elements of the training course are complete?
   a. If you are using role-based training, how do you ensure the correct training is given?
      i. Where is the training being conducted?
2. How do you describe the process flow of initiation and verification of completion of cybersecurity training before giving electronic or unescorted physical access?
   a. Who, or what role, is responsible for giving access?
   b. How is that individual trained or made aware of the process to give access?
   c. If the person who normally performs this task is not available, how do you ensure that there is qualified backup?
   d. Describe any oversight of this activity (such as peer review or manager sign-off) designed to prevent or detect an error in giving access.
   e. How do you protect training records from loss or unauthorized change?

Potential Failure Point: Failure to develop criterion to be used to qualify a CIP Exceptional Circumstance.

1. How do you ensure that a CIP Exceptional Circumstance is officially determined before being used by personnel giving access?

Potential Failure Point: Failure to develop a procedure to identify personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.

1. What is your process to ensure that applicable personnel are identified and tracked as needing recurring training?

Potential Failure Point: Failure to clearly define or communicate start and end dates used to establish a time for training.

1. Describe your process for scheduling training to ensure that personnel receive cybersecurity training before the due date.
   a. How are people notified that they need training? The individual's supervisor or manager?
   b. Are there any notifications or reminders that ensure people are aware of scheduled training?
   c. If the person does not attend or complete training as scheduled, describe the follow-up process to ensure that training is rescheduled before the deadline.
2. Do you have a process to escalate the reminders for completion of the training according to the due date?
3. What process do you have for personnel who have not completed the training on the due date?
   a. How do you ensure access is disabled if training is not complete before the due date?