Security Objective(s)

The security objectives are to—

- Develop baseline configurations of the applicable systems. The baselines include assessed component configurations.
- Authorize deviations to current configurations in the applicable system component inventory.
- Assess proposed changes for undocumented or undetected modification of desired security controls.

WECC Intent

The potential failure points and guidance questions help registered entities assess risks during the internal controls designing process. The registered entity may use this document to help uncover risk, but it is not WECC's intent to establish a standard or baseline for risk assessment or controls design.

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

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

Potential Failure Points and Guidance Questions

CIP-010-2 R2

Potential Failure Point: (Part 1.1) Failure to develop a complete list of cyber assets that require the development of baselines.

1. How does [the entity] ensure it has accounted for all related assets in its baseline development?

Potential Failure Point (Part 1.1): Failure to develop a method to document baseline configuration for applicable devices.

1. How does [the entity] ensure it addresses all applicable devices in its process?
    a. If [the entity] created baselines by group, how did it determine the proper level of detail or types of groups to develop a useful baseline configuration?
2. Does [the entity] use automated processes to develop baseline configurations?
    a. How does [the entity] verify that it has documented all related items (CIP-010-2 R1, sub-parts 1.1.1 through 1.1.5) with the baseline configuration?
    b. How does [the entity] decide what software to document?

        i. How does [the entity] document its reasons for software not included if (category, type) is not explicitly stated in requirement?
    c. How does [the entity] ensure automated tools used for baseline documentation are providing accurate information?
        i. How does [the entity] document the non-automated parts of the baseline that the automated tool does not capture?
3. How does [the entity] determine the documentation it must collect from a vendor?
    a. How does [the entity] verify that the information it gets from the vendor contains all the elements needed for its baseline?
    b. How does [the entity] verify that documentation accurately shows the status of the device?

Potential Failure Point (Part 1.2): Failure to define type or category of changes considered to be deviations from a baseline configuration.

1. Has [the entity] defined what types or categories of changes are governed by the CIP-010 change process?
    a. How does [the entity] document and communicate this?

Potential Failure Point (Part 1.2): Failure to develop a procedure on authorizing and documenting changes that deviate from the baseline configuration.

1. What is the process for authorizing and documenting a change that deviates from the baseline configuration?
    a. Does [the entity] use a tool for the process or is there a documented, manual process?
    b. Has [the entity] identified all attributes that must be documented and determined how and where the documentation will be stored?
    c. Has [the entity] determined who, or what role, is responsible for reviewing and authorizing changes?
    d. Has [the entity] developed a process for authorizing/documenting emergency changes?
    e. Does [the entity] have criteria it must meet to authorize a change?
2. Does [the entity] have a trigger that shows when authorization for a change is required?
    a. How does [the entity] ensure that no changes are made without authorization and proper documentation of the change?

Potential Failure Point (Part 1.3): Failure to clearly define or communicate start and end dates used to establish timeframes for changes and updates.

1. Has [the entity] defined a method for establishing the start date for completing a change, beginning the 30-calendar-day period?
2. Has [the entity] identified who is responsible for the notification of completing the change?
3. How does the entity ensure that updates to baseline configurations occur within the required period?

a. If updates are not completed on schedule, is the issue escalated or identified before the 30-calendar-day deadline?

Potential Failure Point (Part 1.3): Failure to develop a process that outlines how to update the baseline configuration.

1. Has [the entity] used any automated tools or processes to monitor for all changes to developed baseline configurations?
    a. Are there multiple ways to track changes (e.g., automated monitoring on some devices and manual processes for others)?
    b. What methods does [the entity] use for notification of changes?
2. How does [the entity] assign the task of updating a baseline configuration? How does [the entity] ensure that the person assigned has the proper knowledge to perform the task?
    a. Is work status (complete/incomplete) tracked?
    b. Describe any review process intended to prevent or detect errors in updates.
    c. How is the updated baseline stored? Does [the entity] have a process for managing baseline documentation?

Potential Failure Point (Part 1.4.1): Failure to develop a process that outlines how to evaluate proposed changes for impact to CIP-005 and CIP-007 security controls.

1. Does [the entity] have documented device capabilities to show what cybersecurity controls may be impacted?
2. Do [the entity]'s evaluation criteria cover all device types?
    a. How does [the entity] document the evaluation of impact to CIP-005 and CIP-007 controls?
3. How does [the entity] verify if other cyber assets' security controls may be affected by the proposed change?

Potential Failure Point (Part 1.4.2): Failure to develop a process that shows how to assess whether CIP-005 and CIP-007 controls have been adversely affected by a change.

1. Describe any procedures or work aids that ensures consistent verification.
    a. Does [the entity] identify what documentation or tool it uses to compare current security controls to the security controls following the change?
2. How does [the entity] ensure that verification of CIP-005 and CIP-007 controls occurs after the change?
    a. How does [the entity] ensure that the person verifying controls is trained and qualified?
    b. Describe any review process(es) intended to prevent or detect errors in the verification process.
        i. Do the verification criteria cover all device types?

3. Does [the entity] have a process that addresses security controls adversely affected by the change?

Potential Failure Point (Part 1.4.3): Failure to develop a process that outlines how to document CIP-005 and CIP-007 controls verification.

1. Does the documentation require a list of specific verified controls?
2. Does the documentation require a date?
3. Is there a specific tool or repository that stores the verification results?

Potential Failure Point (Part 1.5): Failure to define criteria used to determine technical feasibility.

1. Has [the entity] established a threshold or set of criteria for determining technical feasibility?

Potential Failure Point (Part 1.5.1): Failure to develop a change process that outlines how to assess changes in a test or production environment.

1. How does [the entity] determine which BES Cyber System is technically feasible to test the baseline configuration before making the change?
2. If using a production environment, how does [the entity] identify and minimize possible adverse effects?
3. How does [the entity] determine what changes it should test in a test environment and what changes it should test in a production environment?

Potential Failure Point (Part 1.5.1): Failure to define a test or production environment.

1. How has [the entity] developed a test environment that models baseline configurations?
2. How does [the entity] ensure the test environment is reflective of the production environment at the time of testing?
3. How does [the entity] determine the scope of the production environment that it will use for testing?

Potential Failure Point (Part 1.5.1): Failure to define what constitutes minimization or criteria necessary to determine adverse effects.

1. How has [the entity] established what constitutes minimization of adverse effects?

Potential Failure Point (Part 1.5.2): Failure to develop a procedure on how to identify differences between the test environment and production environment.

1. Describe [the entity]'s process for identifying and documenting differences between the test and production environments?
2. Describe [the entity]'s process to determine whether a test environment was used?

Potential Failure Point (Part 1.5.2): Failure to develop a process to decide which measures it uses to account for differences.

1. How does [the entity] document and communicate measures it can use to account for differences?
1. What criteria from the results of a test has [the entity] decided to document?
2. Has [the entity] identified criteria that show whether the change should go into full production?

CIP-010-2 R2

Potential Failure Point (Part 2.1): Failure to define criteria for how monitoring of baseline configuration should occur.

1. Does [the entity] use automated or manual processes to watch for changes to the baseline configuration?
2. If automated processes are used, how does [the entity] monitor those processes to make sure they are functioning properly? How would the entity become aware of a failure?
3. If manual processes are used, how does [the entity] ensure that those responsible know the manual process?

Potential Failure Point (Part 2.1): Failure to clearly define or communicate start and end dates used to establish periods for monitoring.

1. Are there any alerts or reminders configured to help personnel see when tasks are due?
2. How does [the entity] ensure the monitoring is done correctly? Is there a review process?
3. If the individual fails to monitor within the required period, is there an escalation process to ensure the issue is seen and corrected?

Potential Failure Point (Part 2.1): Failure to develop a procedure to detect and investigate unauthorized changes.

1. If an unauthorized change is detected, what training, processes, or work aids are available to help personnel document and investigate the issue?
2. If automated processes are used to monitor for changes, who is notified of unauthorized changes and how are they notified?
3. If manual processes are used to monitor for changes, who is notified of unauthorized changes and how are they notified?
4. How does [the entity] know if a detected change has been authorized?