Security Objective(s)

To identify and address vulnerabilities of the environment. Those vulnerabilities inherent to the environment as well as those introduced due to an authorized or unauthorized change.
Where technically feasible and does not impact reliability, scans for vulnerabilities in the applicable systems. Analyzes vulnerability reports and remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and shares information obtained from the vulnerability assessment process and security control assessments with stakeholders to address vulnerabilities in the environment.

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

WECC Intent

The potential failure points and guidance questions provide general 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 and it is not WECC's intent to establish a standard or baseline for entity risk assessment or controls design.

Note: *Guidance Questions serve to aid an entity in understanding and/or documenting its controls. Any responses, including lack of affirmative feedback, will have no consequences to an entity's demonstration of compliance at audit.*

**Please feel free to provide feedback to* ICE@WECC.org *with suggestions on Potential Failure Points & Guidance Questions.*

Potential Failure Points and Guidance Questions

CIP-010-2 R3

Potential Failure Point: (Part 3.1) Failure to develop a process on how to conduct vulnerability assessments.

1. How do you track milestones and timelines to ensure that paper or active vulnerability assessments are conducted within the required timeframes?
2. Does that process identify roles and responsibilities of process owners, assessment executers, risk owners, and business stakeholders?
3. Do you have a process that identifies methods paper and active vulnerability assessments are to follow?
4. How are the paper vulnerability assessments documented?
5. How are the active vulnerability assessments documented?

6. How do you determine what BES Cyber Systems will have Vulnerability Assessments?
7. Do you have documented criteria of what the output of the Vulnerability Assessment will include?

Potential Failure Point: (Part 3.1) Failure to develop a process/procedure on how to identify and address vulnerabilities.

1. How do you ensure that the process for conducing vulnerability assessments is in aligned with criterion outlined in CIP-010-2 R3 (Guidelines and Technical Basis)?
2. Do you use additional standards (i.e. NIST SP800-115) or methods to conduct vulnerability assessments?
3. Do you have documented criteria to be used when performing a Vulnerability Assessment?
4. How do you ensure that the person assigned has the appropriate knowledge to perform the task?
5. How do you ensure that the person performing this task is trained and qualified?

Potential Failure Point: (Part 3.2) Failure to develop a procedure on how to perform the active vulnerability assessment in a test environment that models the baseline configuration of the production environment.

1. Do you have a documented procedure for conducting vulnerability assessments in the testing environment?
    a. Does the process describe the differences between the test environment and the production environment?
    b. Do you have a process to determine any differences between the test and production environment?
    c. Does the process describe the measures used to account for any differences in operation between the test and production environments?
2. Do you have criteria of what the active vulnerability assessment will consist of?
    a. What tools and resources will be used by you to conduct an active vulnerability assessment?
3. Do you have documented criteria of what the output of the Vulnerability Assessment will include?

Potential Failure Point: (Part 3.2) Failure to define what constitutes due care while performing an active vulnerability assessment.

1. Do you have a process for conducting active vulnerability assessment in a production environment?
2. How do you ensure it minimizes adverse effects?

Potential Failure Point: (Part 3.3) Failure to develop a policy that requires an active vulnerability assessment prior to adding a new applicable Cyber Asset to a production environment.

1. Do you have a policy that requires conducting active vulnerability assessment prior to adding a new applicable Cyber Asset to a production environment?
2. Do you have criteria as to what the active vulnerability assessment will include?

Potential Failure Point: (Part 3.3) Failure to develop a policy that outlines the criterion and/or conditions that must exist to qualify for exception under CIP Exceptional Circumstances.

1. Do you have a policy that outlines the criterion and/or conditions that must exist to qualify for exception under CIP Exceptional Circumstances?
2. Do you have any follow-up actions after a change that qualified for CIP Exceptional Circumstances?

Potential Failure Point: (Part 3.3) Failure to develop a process that outlines criterion and method used to determine how a baseline configuration models an existing configuration of a previous or other existing Cyber Asset.

1. How does the subject matter expert determine how a baseline configuration models an existing configuration of a previous or other existing Cyber Asset?
2. Do you go through an authorization process that determines if an active vulnerability assessment is needed?

Potential Failure Point: (Part 3.4) Failure to ensures vulnerability Assessment process outlines development and management of the action plan.

1. Ho do you classify and prioritize risks associated with identified vulnerabilities?
2. How does the process manage remediation or mitigation dates?
3. Does the process address action-plan line-item ownership?
4. Does the process have sufficient accountability for sign-off/approval of completed action plan line items?
5. Does the process have a risk exception provision?
    a. If so, how are these approved and documented?

Potential Failure Point: (Part 3.4) Failure to clearly define or communicate start/end dates used to establish timeframe(s) for plan management.

1. How does the start and end dates get documented in plans?

Potential Failure Point: (Part 3.4) Failure to develop criterion for action plans that ensure remediation or mitigation occurs upon plan completion.

1. How do you ensure completion of remediation or mitigating activities for vulnerabilities identified in the assessment?

Potential Failure Point: (Part 3.4) Failure to develop criterion for documentation of the results that meet all the requirements of Parts 3.1, 3.2, and 3.3.

1. How do you ensure documentation is complete?
2. How have you determined where documentation will be tracked and stored?