Security Objective

- Continuously acquire, assess, and act on new information to identify and remediate, and reduce opportunities for attackers.
- Review proposed configuration-controlled changes to the information system and approve or disapprove changes with consideration for security impact analyses.
- Proactive monitoring and addressing known security vulnerabilities in software before they can be exploited to gain control of or render inoperable a Bulk Electric System (BES) Cyber Asset or BES Cyber System.

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

WECC Intent

The potential failure points and guidance questions give direction to registered entities for risk assessment 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 understand and document its controls. Any response or lack of feedback will have no consequences to an entity's demonstration of compliance at audit.

Potential Failure Points and Guidance Questions

Potential Failure Point: Failure to have a procedure to update the patch management process whenever there are changes to the entity's applicable Cyber Assets.

1. How do you ensure that a responsible person is informed about changes to the applicable Cyber Assets (decommissioning of old Cyber Assets, addition of new Cyber Assets, adding applications to the existing cyber assets, etc)?
2. What process does the responsible person have to make appropriate changes to the patch management process to ensure that changes to the Cyber Assets follow the patch management process?
3. Do you have anyone assigned for monitoring implementation and maintenance of the patch management process?

Potential Failure Point: (Part 2.1) Failure to develop a complete list of Cyber Assets that require a process to identify and track sources of patches.

1. How does the entity ensure all applicable assets are included in the identification and tracking process?

Potential Failure Point: (Part 2.1) Failure to develop a process/procedure on how to identify and track sources of patches for applicable systems.

1. How does [the entity] ensure all applicable Cyber Assets, Systems, associated software, firmware, and drivers are included in the patch tracking process?
2. How does [the entity] ensure it is using appropriate sources to track patches for applicable Cyber Assets, associated software, firmware, and drivers?
3. How does [the entity] ensure the process to monitor patch sources is adequate to make sure patch monitoring occurs in a timely manner?

Potential Failure Point: (Part 2.1) Failure to have a process/procedure on how to evaluate patches for all applicable Cyber Assets, Systems, associated software, firmware, and drivers.

1. How does [the entity] ensure that patches are correctly evaluated?
   a. Are there any processes in place to review or validate the results of the evaluation?
2. How has [the entity] incorporated the information provided in the CIP-007-6 Guidelines and Technical Basis to define its evaluation criteria?
   a. Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems."
   b. Department of Homeland Security document "Recommended Practice for Patch Management of Control Systems."

Potential Failure Point: (Part 2.1) Failure to have a process/procedure on how to install patches for all applicable Cyber Assets, Systems, associated software, firmware, and drivers.

1. How does [the entity] ensure patch installation is completed in a timely manner?
2. How does [the entity] document updates of patches installed?

Potential Failure Point: (Part 2.1) Failure to develop a procedure on how updates of installed patches are documented in baseline configurations.

1. How does [the entity] update baseline configurations to reflect installed patches?

Potential Failure Point: (Part 2.2, 2.4) Failure to define or communicate start/end dates for monitoring and mitigation timeline(s).

1. How has [the entity] identified dates of significance in its timelines concerning R2?
2. How does entity escalate the urgency to perform the evaluation to ensure the timeframe for patch management process is followed?

3. What is [the entity's] process for monitoring mitigation timeframes to ensure they are implemented as planned?
4. How does [the entity] identify mitigation plans that will require an extension?
5. How has the entity identified what constitutes a revision to a mitigation plan?
6. How does [the entity] ensure that the Critical Infrastructure Protection (CIP) Senior Manager or delegate completes the review process before the end date of the original mitigation plan?

Potential Failure Point: (Part 2.3) Failure to have a process for creating a mitigation plan to mitigate properly the vulnerabilities addressed by each security patch.

1. What is [the entity] process to create mitigation plans?
   a. Does [the entity] have a process and escalations for approval to ensure that the mitigation plan is necessary and it has a timeline to mitigate the vulnerabilities?
   b. Does [the entity] have a process to monitor vulnerabilities to ensure that the mitigation plan is effective?
   c. How are the verifications of vulnerability mitigations documented?