RELIABILITY FIRST

Generator Welcome Package

March 2025

TABLE OF CONTENTS

Introduction

General Considerations for Generator Owners (GOs) or Generator Operators (GOPs) Preparing for NERC Registration

ReliabilityFirst (RF) applies risk-based compliance monitoring to entities. Many risks have been identified under NERC's risk-based compliance monitoring approach and these have changed over the two decades of the NERC compliance program as the Bulk Electric System[1] (BES) has changed. The following package provides entities with a framework to prepare a Generator Owner (GO) and Generator Operator (GOP) for its compliance obligations and to internally assess the GO's and GOP's state of compliance. RF developed this package based on experiences with new GOs and GOPs, and while the package covers a variety of past problem areas and provides helpful guidance, it does not guarantee that compliance will be achieved. However, with proper planning and a framework for assessing the state of compliance, a GO/GOP is better prepared for compliance responsibilities which begin on its registration date. With this in mind, consider the following points when preparing to bring a new generator online and registering with NERC.

- ❑ **Compliance obligations begin on an entity's[2] effective registration date with NERC. Entities are expected to be audit-ready at that time.**
- ❑ When bringing a new generator online, involve the entity's compliance department early in the process. Consider that preparing a new GO or GOP for compliance may take 6-12 months of preparation before NERC registration, depending on the maturity of the existing compliance program. Entities should ensure they have a sufficient amount of time to develop and implement business processes to address the applicable Reliability Standards[3]. Much of the evidence gathering and evaluation, however, will likely occur close to the NERC registration date.

[1] Capitalized terms are in the NERC Glossary of Terms throughout this document and have specific meanings that are important to understand. https://www.nerc.com/pa/stand/glossary%20of%20terms/glossary_of_terms.pdf
[2] *Entity* is used to describe the owner or operator of the generator and includes companies, government agencies, cities, etc.
[3] The Standards referenced throughout this Welcome Package were active Standards when the Welcome Package was posted as of February 1, 2025. ReliabilityFirst will periodically update the Welcome Package as Standards are improved. If there are any questions, please contact ReliabilityFirst Entity Engagement or Assist Visit Team.

- ❑ Consider developing a method of tracking preparations through the first year after registration to ensure all initial compliance tasks are completed. The GO/GOP Roadmap and Internal Controls Considerations tables, included within pages 16-46 of this document, provide high level timelines, best practices, and recommendations to aid entities in developing a company-specific tracking method.
- ❑ Reach out to RF's Entity Assist Visit department for assistance on self-assessment tools as needed. Tools exist for cybersecurity, training, and operational policies.
- ❑ A strong compliance program supports reliable operations, especially when utilizing operational best practices, and the demonstration of compliance should be the outcome of operational activities.
- ❑ Procedures and process documents should define and document the GO/GOP's business processes with compliance built in. Entities should refrain from writing generic procedures that reiterate the Standard language.
- ❑ Although a documented procedure is not always required, entities are encouraged to establish strong operational business processes with preventative, detective, and corrective internal controls for applicable NERC Reliability Standards and Requirements. The business processes should be designed around the GO's and GOP's needs. For example, COM-002-4 does not require a documented procedure explaining three-part communications training. However, entities should establish processes for identifying new operators who require three-part communications training, conduct training, and track training. These processes will be unique to the way the company does business.
- ❑ The control considerations noted in the Internal Controls Considerations tables provide observed best practices and common industry processes and are provided as a guide to help entities when developing internal controls. Similar to developing processes, a GO/GOP should develop internal controls appropriate for its organization.

Planning Stages

When bringing a new generator online or establishing a GO, think of compliance planning on a continuum, with a key milestone at NERC registration. There are "pre-registration" compliance activities, such as developing procedures and processes, establishing internal controls, commissioning equipment and Facilities, and performing initial compliance activities where necessary. The pre-registration stage ends once NERC registration is complete. As noted above, compliance obligations begin on the NERC registration date. "Post-registration" activities can be either event-driven or time-based, and entities should have processes in place to perform the compliance activities for both types. For example, automatic voltage regulator (AVR) status change notifications are event-driven, and entities are expected to make notifications for AVR status changes (VAR-002-4.1 Generator Operation for Maintaining Network Voltage Schedules) starting on the NERC registration date, while other Standards such as PRC-005-6 (Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance) and MOD-026-1 (Verification of Models and Data for Generator Excitation Control System or Plant Volt/VAR Control Functions) are time-based and entities need to plan ahead to ensure compliance.

Pre-Registration Compliance Considerations

Review the Interconnection Agreement (IA), which can provide useful information for determining applicability to various Standards and Requirements. Each of these pieces of information is required to comply with multiple Standards. The following information can typically be found in the IA:

- ❑ Interconnection Tie Line Length (useful for determining FAC-003-5 (Transmission Vegetation Management) applicability)
- ❑ Location of Point of Interconnection (POI)
- ❑ Generator type(s)
- ❑ Reactive devices
- ❑ MW and MVAR capabilities
- ❑ Protection System Component ownership
- ❑ Transmission Owner (TO), Transmission Operator (TOP), and Transmission Planner (TP) information
- ❑ Generation marketer or third-party control center to the extent that they act as an intermediary between the generator and the Balancing Authority (either PJM or MISO)
- ❑ Remedial Action Schemes of which the generator may be a part

Review Service Agreements. Examples of possible service agreements are listed below:

- ❑ Balance of Plant (BOP)
- ❑ Energy Management/Services Agreements
- ❑ Marketing Entity Agreements (may describe communication from PJM/MISO through an intermediate party)
- ❑ PJM Manuals or MISO Business Practices Manuals (as appropriate) – many of these lay out the procedures the GO/GOP is expected to follow for Modeling, Operations, Outages, and System Studies

Identify the roles and responsibilities based on the review of the services agreement.

- ❑ Entity responsible for GO or GOP compliance
  - The entity[4] that will be registered with NERC and who will be ultimately responsible for the state of compliance.
- ❑ Entity responsible for performing the functional obligations for the GO or GOP
  - If an entity has contracted with another company to perform the functional obligations of the GO or GOP, the NERC registered GO or GOP will be responsible for demonstrating compliance with the NERC Reliability Standards and will likely need to obtain and retain documentation from the contracted entity to demonstrate compliance.
- ❑ Entity responsibilities under a Joint Registration Organization (JRO)
  - Another entity may agree to be responsible for NERC compliance.
- ❑ Entity responsibilities under a Coordinated Functional Registration (CFR)
  - Entities may agree who is responsible for certain requirements, although both (or all) will be registered for the

[4] Usually a single entity agrees to be responsible to NERC for generators with multiple owners.

function.

Determine Applicability of NERC Standards, for example:

❑ PER-005-2 (**Note:** *Whether PER-005 is applicable to the GOP or not, GOPs are encouraged to develop a systematic training program that would include the training required by the NERC Standards*)

❑ PER-006-1

❑ FAC-003-5

❑ PRC-012-2 and other RAS related Requirements

❑ CIP-002-5.1a: Status of whether the entity has low-impact or medium-impact BES Cyber Assets (see Attachment 1[5])

Note: Entities are encouraged to develop and retain evidence to support determinations that specific Standards/Requirements are not applicable to the entity. This evidence can be gathered from the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), and internal justifications for why the Standard or Requirements do not apply. For example, PRC-002-4 R2 requires the GO to have SER (sequence of event recording) if the GO receives a notification from the TO. If the TO does not provide a notification to the GO, the GO should consider reaching out to the TO and request confirmation that SER is not required at the GO's plant. Another example is PER-005-2. If a GOP does not meet the applicability, the GOP should consider developing a justification for the determination of not being applicable and gathering evidence to demonstrate it is not applicable.

Additional pre-registration activities include:

❑ Writing procedures where required. For example, PRC-005-6 requires a Protection System Maintenance Program (PSMP).

❑ Commissioning equipment and Facilities. While there is no Reliability Standard that specifically addresses commissioning, it is important that technical rigor is applied during the commissioning process to prevent equipment failures and Misoperations when the Facility is placed in-service (see NERC Lessons Learned on *Verification of AC Quantities during Protection System Design and Commissioning* and FERC/NERC/ Regional Entity *Joint Review of Protection System Commissioning Programs*

[5] Attachment 1 and this document only cover low-impact BES Cyber Assets. If an entity has medium BES Cyber Assets, additional requirements apply and entities are encouraged to contact the RF Assist Visit Program for additional resources.

(FERC) under “Recommended Reading” below). Additionally, the initial due dates for maintenance of Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components under PRC-005-6 are based on the commissioning date of the Components so it is important to retain the commissioning documentation that is used to establish the initial due dates for maintenance activities.

❑ Perform initial compliance activities where required. For example, CIP-002-5.1a BES Cyber System Categorization needs to be completed prior to registration, as does the CIP Senior Manager approval of the identified categorizations.

❑ Develop processes for compliance activities due following NERC registration (i.e., time-based and event-driven compliance activities), such as MOD-025-2, PRC-004-6, and VAR-002-4.1.

❑ Determining who in your company will be the Primary and Alternate Compliance Contacts. These individuals will typically be the ones contacting and being contacted by ReliabilityFirst for various compliance actions.

NERC Registration

NERC registration is coordinated with ReliabilityFirst’s registration team, and submission of the registration package typically occurs 30 days prior to the planned registration date. Below are common activities that take place during the registration process:

❑ Consult the registration page on the ReliabilityFirst website: https://www.rfirst.org/registration-certification/registration/ for information pertaining to how to register as a new GO or GOP in RF and what documentation is required by the region to validate and approve a new registration.

❑ Review registration documentation provided on the NERC public website: https://www.nerc.com/pa/comp/Pages/Registration.aspx

❑ Review the following: Rules of Procedure Section 500, *Organization Registration and Certification*, Appendix 5A, *Organization Registration and Certification Manual, and* Appendix 5B, *Statement of Compliance Registry Criteria*.

❑ View CORES training as needed: https://vimeopro.com/nerclearning/cores-video-library/page/1

❑ Submit NERC registration package to ReliabilityFirst in the NERC ERO Portal/CORES application.

- ❑ Retain NCR Letter for records.
- ❑ Any questions pertaining to RF registration should be directed to compliance@rfirst.org.

Post-Registration Compliance Activities

Entities must be prepared to meet compliance obligations, which mostly begin the day of registration. Some compliance obligations can be planned such as Protection Systems Maintenance (PRC-005-6), but many will be event-driven, such as identification of Protection System Misoperations (PRC-004-6) and notification of AVR status changes (VAR-002-4.1). The list below includes common tasks that will be necessary to maintain and demonstrate compliance with the Reliability Standards as well as tasks associated with processes developed to support the reliability of the BES.

- ❑ Perform, or prepare to perform, event-driven compliance activities (e.g. PRC-004-6, VAR-002-4.1) and retain appropriate evidence.
- ❑ Identify key milestone dates (e.g., commissioning, Commercial Operations Date) to establish due dates for initial performance of time-based compliance activities (e.g., MOD-025-2, MOD-026-1, MOD-027-1).
- ❑ Perform initial, time-based compliance activities and retain appropriate evidence.
- ❑ Register for Electricity Information Sharing and Analysis Center (E-ISAC)
- ❑ Add the newly registered GO/GOP to NERC Alerts.
- ❑ Register for or add newly registered GO/GOP to Misoperation Information Data Analysis System (MIDAS) reporting (which is a 1600 data request and not specifically required for compliance with PRC-004-6), if required.
- ❑ Implement process for Generating Availability Data System (GADS) reporting.

What if I think something is non-compliant?

Following NERC registration, ReliabilityFirst encourages and expects self-reporting of instances of noncompliance with the Reliability Standards. Use the Align tool or contact ReliabilityFirst to Self-Report identified issues. Additionally, you will need to complete mitigating activities for each instance of noncompliance to return to compliance as soon as possible as well as reduce the likelihood of noncompliance recurrence. Critical self-assessment is the basis for the RF and NERC Compliance Programs, and self-reporting generally indicates that you take compliance obligations seriously and have effective internal controls.

Recommended Reading

The following is a list of recommended reading for newly registered GO/GOPs. This list is not exhaustive and focuses on higher risk areas.

Compliance Guidance

Compliance Guidance can be found on the NERC website under *Compliance Guidance*:

- ❑ Implementation Guidance developed by registered entities provides examples for implementing a Standard. ERO-Endorsed Implementation Guidance has been approved by NERC and RF for use, while the Proposed Implementation Guidance has not, but may still provide helpful information on lessons learned.
- ❑ Compliance Monitoring and Enforcement Program (CMEP) Practice Guides developed by ERO Enterprise CMEP staff provides direction to ERO Enterprise CMEP staff on approaches to carry out compliance monitoring and enforcement activities.
- ❑ Excel version of all Standards with references to implementation guidance, implementation plans for phased-in Standards and other information: https://www.nerc.com/pa/Stand/AlignRep/One%20Stop%20Shop.xlsx
- ❑ One-stop shop page for other compliance information such as periodic data submittal schedules, webinars, etc.: https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx

NERC Lessons Learned and Event Reports

Below is a brief list of some NERC Lessons Learned and Event Reports[6] that are relevant to new facilities and the emerging risks associated with new technologies and the changing resource mix. Registered entities are encouraged to review these reports and evaluate how the

[6] Event reports are sometimes Joint between FERC, NERC, and/or Regional Entities

recommendations and conclusions may apply to its Facility(ies) and operations. All Lessons Learned are posted here and may provide additional value for entities (e.g., winterization efforts in Lessons Learned 2011). These should be reviewed based on generation type (wind, combustion turbine, etc.). Additionally, all Event Reports are posted here and often provide additional materials that are beneficial to entities (e.g., February 2021 Cold Weather Outages, December 2022 Winter Storm Elliott Report, etc.).

NERC Lessons Learned*:*

- ❑ *Verification of AC Quantities during Protection System Design and Commissioning*
- ❑ *Substation Fires: Working with First Responders*
- ❑ *Joint Review of Protection System Commissioning Programs*
- ❑ *Loss of Wind Turbines due to Transient Voltage Disturbances on the Bulk Transmission System*

NERC Event Reports:

- ❑ *December 2022 Winter Storm Elliott Report*
- ❑ *July 2020 San Fernando Solar PV Reduction Disturbance*
- ❑ *April and May 2018 Fault Induced Solar Photovoltaic Resource Interruption Disturbances Report*
- ❑ *August 2016 1200 MW Fault Induced Solar Photovoltaic Resources Interruption Disturbance Report*

ReliabilityFirst Website Training:

- ❑ Tech Talk (GO and GOP O&P Standards (RF-GO-and-GOP-OP-Standards-Tech-Talk-May-2024.pdf)
- ❑ Internal Control 101 (Internal Controls 101 Training - ReliabilityFirst)
- ❑ Low impact BES Cyber System articles, (The Lighthouse: CIP low impact from the ground up - ReliabilityFirst)

❑ 2024 CIP Themes Report Preview 2024 CIP Themes Report Preview - ReliabilityFirst)
❑ Cold Weather Guidelines for Generating Units (Reliability_Guideline_Generating_Unit_Winter_Weather_Readiness_v4.pdf)
❑ RF winterization information (https://www.rfirst.org/tools-and-services/winterization/)
❑ PRC-027-1 (Coordination of Protection Systems) (https://www.rfirst.org/wp-content/uploads/2024/01/PRC-027-Presentation_19July2021.pdf)
❑ And many other great quick reference resources are available at www.rfirst.org, scroll to Resource Center

Align Training Resources

Align is the website used by ReliabilityFirst and NERC in the conduct of the Compliance Monitoring and Enforcement Program. Align provides a secure method of managing and storing data, alignment of business practices with the other regions, a standardized interface, easy real-time access to information. The NERC Align Project page and FAQ document contain helpful information for registered entities. Self-service training resources provided for registered entity staff, including training videos and user guides, are available on the NERC Training Site. NERC's training site provides training and materials on a variety of topics for Align and the Secure Evidence Locker (SEL) used by NERC, ReliabilityFirst, and registered entity staff. Your Primary Compliance Contact is the designated Access Approver for Align for your company. Remember to check out NERC's Align project page or reach out to AskAlign@NERC.net for additional information.

❑ Align Training videos: https://training.nerc.net/Home/ViewApplicationVideos?system=Align&role=Registered%20Entities

Additional Resources

The following is a list of resources the GO and GOP can consider participating in and reviewing. Many have virtual attendance options.

❑ ReliabilityFirst Workshops/Training, such as seasonal workshops, RF Tech Talks
❑ ReliabilityFirst Protection Subcommittee https://www.rfirst.org/get-involved/committees/reliability-committee/protection-subcommittee/ ,
❑ ReliabilityFirst Generation Subcommittee https://www.rfirst.org/get-involved/committees/reliability-committee/generator-subcommittee/ ,
❑ ReliabilityFirst Transmission Performance Subcommittee https://www.rfirst.org/get-involved/committees/reliability-committee/transmission-performance-subcommittee/
❑ ReliabilityFirst Critical Infrastructure Protection Committee (CIPC) https://www.rfirst.org/get-involved/committees/critical-infrastructure-protection-committee/ ,

- ❑ ReliabilityFirst Compliance Users Group (CUG) https://www.rfirst.org/get-involved/committees/compliance-user-group-cug/
- ❑ NERC Committee Meetings (https://www.nerc.com/Pages/SitemapCommittees.aspx)
- ❑ North American Generator Forum (NAGF). *Note: NAGF requires dues to participate and ReliabilityFirst does not require participation. Mentioning NAGF here is only to inform the GO or GOP that the NAGF is available as a resource and peer group for GOs and GOPs.* (https://generatorforum.org/)
- ❑ GridEx (https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx), GridSecCon (https://www.nerc.com/pa/CI/ESISAC/Pages/GridSecCon.aspx)
- ❑ MISO (https://www.misoenergy.org/) or PJM (https://www.pjm.com/) (as applicable) working groups and training portals
- ❑ ReliabilityFirst Assist Visit Program – free resource to ask technology, reliability, self-assessment, and compliance questions (https://www.rfirst.org/tools-and-services/assist-visit/)

Internal Controls Overview

Internal controls help companies operate effectively and efficiently, reduce the risk of noncompliance, and improve the reliability of the Bulk Electric System (BES). As part of the Compliance Audit, Spot Check, and Self-Certification process, auditors will review subsets of an entity's internal controls. Auditors will then provide feedback to the ReliabilityFirst Risk Assessment and Mitigation Group for the entity's Compliance Oversight Plan (COP) and to inform future engagement scheduling and engagement scopes.

ReliabilityFirst's experience is that many entities have internal controls, but do not always recognize their existing internal controls as "*internal controls."* Often, this is because the control is part of the company's normal business process and is not specifically called out as an internal control. The categories and examples that follow below is meant to help entities identify existing internal controls and provide a general overview for building out internal controls for applicable Standards and Requirements. More specific considerations are provided in the "Controls Consideration" column of the requirement included in the Internal Controls Considerations tables on pages 27-46 and revolve around the concepts of preventative, detective, and corrective internal controls. While it is not necessary to categorize controls, entities can use this framework to identify and establish business processes to meet their reliability objectives.

Internal controls can also be viewed from a management perspective. Inventory Management and change control are areas where effective controls greatly help compliance efforts and may encompass many Reliability Standards. Drawing a flowchart of a process can also assist in identifying where internal controls might be helpful.

No specific internal control is required by the Standards; rather the following are provided as examples of helpful controls.

Preventative Controls:

Preventative controls aim to reduce the risk of a negative event occurring. Preventative controls can be physical or administrative controls depending on the applicable Standard and may vary based on inherent risk and situation.

Badge readers on a Control Center door is a physical preventative control, since it prevents unauthorized physical access into the Control Center. Common administrative preventative controls are procedures, checklists, and training. These tools help personnel understand what needs to be done to prevent a negative event.

Detective Controls:

Detective controls seek to identify an issue that is occurring or has occurred. For example, the entity could establish alarms to alert operators to an AVR status change and the time that status change occurs. In other words, the alarm detects and alerts personnel to a change from normal operations. A detective control could also be a periodic review of AVR status changes to verify (1) that the appropriate notifications were made and (2) notifications to the TOP(s) meet the time requirement specified in VAR-002-4.1 R3.

Corrective Controls:

Corrective controls correct issues once they have occurred. In other words, corrective controls return a situation to its normal state. Using VAR as the example, a corrective control might include what actions, if any, a generator operator could take to restore (i.e., correct) the AVR status to normal. Can the Generator Operator reboot a server? Should the Generator Operator contact site personnel for assistance? Corrective controls can also be more compliance oriented. If a detective control identifies a potential noncompliance (PNC), the entity can remediate the issue and file a Self-Report with ReliabilityFirst. The entity can, furthermore, determine if additional actions are necessary according to its Internal Compliance Program (ICP).

Testing Internal Controls:

Once an entity has implemented an internal controls framework, the entity can test the controls to verify that they are performing as expected. In a sense, testing controls is a control for the controls.

Suggested Viewing: Internal Controls 101 Training - ReliabilityFirst

GO/GOP Roadmap

The table below is split into different sections based on the “type” of Requirement. It is intended to help newly registered entities focus efforts in developing expectations for its staff or processes needed to maintain reliability. For example, FAC-003 has a procedural type of requirement and performance requirements listed below. Entities may manage the procedural aspect internally but the performance requirements may require an outside contractor, which implies contract language, budgeting, and timing considerations to meet the needs. All contracted work can/should be reviewed because ultimately the entity is responsible for compliance (not the contractor). Setting expectations, clear work orders, and closing out the contract after all reviews and checkouts are complete are important parts of this process.

Procedural			
Standard Requirement	**Function**	**Procedural Requirement**	**Due Date**
EOP-004-4 R1	GO, GOP	Event Report Operating Plan	Initial Registration
FAC-003-5 R3[1]	GO	Documented maintenance strategies or procedures or processes or specifications it uses to prevent vegetation encroachments	Initial Registration
FAC-008-5 R1, R2	GO	Documentation for determining Facility Ratings and Facility Ratings methodology	Initial Registration
PRC-005-6 R1, R2	GO	Protection System Maintenance Program	Initial Registration
PRC-027-1 R1	GO	Process for developing new and revised Protection System settings	Initial Registration

Initial Performance

Standard Requirement	Function	Performance Requirement	Due Date
CIP-002-5.1a R1	GO, GOP	Implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above **1.1** Identify each of the high impact BES Cyber Systems according to **Attachment 1, Section 1**, if any, at each asset; **1.2** Identify each of the medium impact BES Cyber Systems according to **Attachment 1, Section 2**, if any, at each asset; and **1.3** Identify each asset that contains a low impact BES Cyber System according to **Attachment 1, Section 3**, if any (a discrete list of low impact BES Cyber Systems is not required). **Note: If the CIP-002-5.1a Assessment identifies high and/or medium impact BES Cyber Systems, consider contacting ReliabilityFirst's Entity Engagement for additional assistance.** https://www.rfirst.org/tools-and-services/assist-visit/	Initial Registration

Standard Requirement	Function	Performance Requirement	Due Date
CIP-002-5.1a R2	GO, GOP	**2.1** Review the identifications in Requirement R1 and its parts (and update them if there are changes identified), even if it has no identified items in **2.2** Requirement R1 and have its CIP Senior Manager or delegate approve the identifications required by Requirement R1, even if it has no identified items in Requirement R1.	Initial Registration
CIP-003-8 R1	GO, GOP	Review and obtain CIP Senior Manager approval for one or more documented cyber security policies that collectively address the topics found in 1.1 (1.1.1 - 1.1.9) for high and medium impact BES Cyber Systems (if any) and 1.2 (1.2.1-1.2.6) for low impact BES Cyber Systems **Note: If the CIP-002-5.1a Assessment identifies high and/or medium impact BES Cyber Systems, consider contacting ReliabilityFirst's Entity Engagement for additional assistance.** https://www.rfirst.org/tools-and-services/assist-visit/	Initial Registration
CIP-003-8 R2	GO, GOP	Implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1 Sections 1-5. Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. (However, it is highly encouraged, as success without a list is extremely difficult.)	Initial Registration
CIP-003-8 R3	GO, GOP	Identify a CIP Senior Manager by name.	Initial Registration

Standard Requirement	Function	Performance Requirement	Due Date
CIP-003-8 R4	GO, GOP	Implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	Initial Registration
COM-001-3 R8	GOP	Have Interpersonal Communication capability with the BA and TOP	Initial Registration
COM-001-3 R12	GOP	Have internal Interpersonal Communication capabilities for the exchange of information necessary for the Reliable Operation of the BES, including includes communication capabilities between Control Centers within the same functional entity, and/or between Control Center and field personnel.	Initial Registration
COM-002-4 R3	GOP	Conduct initial training (three-part communication) for each of its operating personnel who can receive an oral two-party, person-to-person Operating Instruction	Prior to an individual operator receiving an oral two-party, person-to-person Operating Instruction
FAC-008-5 R6	GO	Establish Facility Ratings consistent with the Facility Ratings methodology or documentation for determining its Facility Ratings	Initial Registration

Standard Requirement	Function	Performance Requirement	Due Date
IRO-010-4 R3	GO	Satisfy obligations of RC data specification	Initial Registration
MOD-032-1 R2	GO	Provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1	Initial Registration
PER-005-2 R6	GOP	Use a systematic approach to develop and implement training to its personnel identified in Applicability Section 4.1.5.1 of this Standard, on how their job function(s) impact the reliable operations of the BES during normal and emergency operations	Initial Registration
PER-006-1 R1	GOP	Provide training to personnel identified in Applicability section 4.1.1.1. on the operational functionality of Protection Systems and Remedial Action Schemes (RAS) that affect the output of the generating Facility(ies) it operates	Prior to an individual being staffed in a position that is responsible for the Real-time control of a generator and can receive Operating Instruction(s)
PRC-019-2 R1	GO	Verify coordination of voltage regulating controls, limit functions, equipment capabilities and Protection System settings.	Initial Registration
PRC-024-3 R1, R2	GO	Set frequency and voltage protective relays to not trip for voltage excursion in “no trip zone”	Initial Registration

Standard Requirement	Function	Performance Requirement	Due Date
PRC-025-2 R1	GO	Apply settings that are in accordance with PRC-025-2 – Attachment 1	Initial Registration
PRC-027-1 R2	GO	Establish Fault current baseline	Initial Registration (if using Option 2 or Option 3)
TOP-003-5 R5	GOP	Satisfy obligations of TOP data specification	Initial Registration
VAR-002-4.1 R1	GOP	Operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator	Initial Registration
VAR-002-4.1 R2	GOP	Maintain the generator voltage or Reactive Power schedule (within each generating Facility's capabilities) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator	Initial Registration

Time-Based Performance

Standard Requirement	Function	Performance Requirement	Due Date
FAC-003-5 R6[2]	GO	Perform a Vegetation Inspection of 100% of its applicable transmission lines	Within first calendar year following registration, not to exceed 18 calendar months from registration
FAC-003-4 R7[3]	GO	Complete 100% of its annual vegetation work plan of applicable lines to ensure no vegetation encroachments occur within the MVCD	Within first 12 calendar months or by end of first calendar year following registration
MOD-025-2 R1, R2	GO	Provide Transmission Planner with verification of Real and Reactive Power capability	Within 12 calendar months of commercial operation date
MOD-026-1 R2	GO	Provide a verified generator excitation control system or plant volt/var control function model to Transmission Planner	Within 365 calendar days after the commissioning date
MOD-027-1 R2	GO	Provide a verified turbine/governor and load control or active power/frequency control model to Transmission Planner	Within 365 calendar days after the commissioning date
PRC-005-6 R3, R4	GO	Maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components in accordance with Table 1 through Table 5	Four calendar months to 12 calendar years following initial commissioning dates

PRC-012-2 R8[4]	GO	Participate in performing a functional test of each of its RAS to verify the overall RAS performance and the proper operation of non-Protection System components	• At least once every six full calendar years for all RAS not designated as limited impact, or • At least once every twelve full calendar years for all RAS designated as limited impact
PRC-027-1 R2	GO	• Option 1: Perform a Protection System Coordination Study; or • Option 2: Compare present Fault current values to an established Fault current baseline and perform a Protection System Coordination Study when the comparison identifies a 15 percent or greater deviation in Fault current values (either three phase or phase to ground) at a bus to which the BES Element is connected, all in a time interval not to exceed six calendar years; or • Option 3: Use a combination of the above.	In a time interval not to exceed six calendar years

[1] Generator Owners that own generation Facilities defined in 4.3.
[2] Generator Owners that own generation Facilities defined in 4.3.
[3] Generator Owners that own generation Facilities defined in 4.3.
[4] For Generator Owners that own all or part of a RAS

Event-Based Performance

Standard Requirement	Function	Performance Requirement	Due Date
COM-001-3 R11	GOP	Detects a failure of its Interpersonal Communication capability shall consult each entity affected by the failure, as identified in Requirement R8 to determine a mutually agreeable action for the COM-001-3 Communication until the restoration of the Communication capability.	Real-time Operation
EOP-004-5 R2	GO/GOP	Entities shall report events per their event reporting Operating plan by no later than 24 hours of recognition of meeting an event. See Attachment 1	24 hours after an event
EOP-005-6 R13	GOP	A GO Blackstart Resource shall notify its Transmission Operator of any known changes to the capabilities of that Blackstart Resource affecting the ability to meet the Transmission Operator’s restoration plan within 24 hours following such change	Within 24 Hours
FAC-003-5 R4	GO	Without any intentional time delay, shall notify the control center holding switching authority for the associated applicable line when the applicable Generator Owner has confirmed the existence of a vegetation condition that is likely to cause a Fault at any moment.	Real-time Operation

Standard Requirement	Function	Performance Requirement	Due Date
MOD-032-1 R3	GO	Upon receipt of written notification from its Planning Coordinator or Transmission Planner regarding technical concerns with the data submitted under Requirement R2 each GO, shall respond to the notifying Planning Coordinator or Transmission Planner.	90 Calendar Days
PRC-004-6 R1/R2	GO	Document and submit in MIDAS and share with owners that are also in the protection scheme.	120 Calendar Day
PRC-004-6 R3	GO	Receives notification, pursuant of R2, identify whether its protection system components caused the Misoperation.	120 Calendar days after the event or 60 Calendar days after notification, which ever happen first.
PRC-027-1 R3	GO	Develop new and revised Protection System setting for BES elements as described in process established in R1.	Time as agreed with neighboring entity
TOP-001-6 R6	GOP	Shall inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority	Real-time Operation

Standard Requirement	Function	Performance Requirement	Due Date
VAR-002-4.1 R3	GOP	Shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change.	30 Minutes
VAR-002-4.1 R4	GOP	Shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability.	30 Minutes
VAR-002-4.1 R5	GOP	Shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request • Tap settings. • Available fixed tap ranges. • Impedance data.	30 Calendar Days
VAR-002-4.1 R6	GO	R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.	Real-time Operations

Internal Controls Considerations Tables

The tables below provide some best practices that have been observed by ReliabilityFirst for some Standards and Requirements. It should not be considered an exhaustive list. Instead, entities can consider it as a starting point. A newly registered entity is encouraged to leverage existing controls within its organization and establish internal controls tailored to its business processes. These are not Requirements but are provided as a resource to facilitate compliance obligations. In the current risk-based environment, compliance engagements examine whether an entity can demonstrate past compliance, as well as the internal controls an entity has developed and implemented to maintain ongoing compliance. Internal controls help develop the strong foundation of an auditor's sense of reasonable assurance that compliance obligations will continue to be met in the future. ReliabilityFirst's Entity Assist Visit Program has additional resources available that can help with further developing internal controls (https://www.rfirst.org/tools-and-services/assist-visit/).

CIP-002-5.1a (Cyber Security – BES Cyber System Categorization)

Standard Requirement	Control Considerations
CIP-002-5.1a R1 and R2	***Preventative Controls*** ▪ Train personnel on requirements. ▪ Develop a procedure for categorization, review, and approval. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Evaluate all BES assets and Cyber Assets using the impact rating criteria (Attachment 1), BES reliability operating services, and NERC Glossary of Terms. ▪ Document justifications for each identification of BES assets and Cyber Assets. ▪ Inventory all BES assets and Cyber Assets for CIP applicable identifications: • BES Cyber Assets (BCA) • BES Cyber Systems • Electronic Access Control or Monitoring Systems (EACMS) • Physical Access Control Systems (PACS) • Protected Cyber Assets (PCA) • Transient Cyber Asset (TCA) ▪ Ensure the CIP Senior Manager understands and approves the identifications prior to the due date. ▪ Retain all evidence associated with evaluations, justifications, and approvals. ▪ Establish a Cyber Assets lifecycle program that includes a robust procurement process, change management program, and proper decommissioning to help identify Cyber Assets that could change the inventory (i.e., increase or decrease) between inventory assessments.

Standard Requirement	Control Considerations
CIP-002-5.1a R1 and R2 (continued)	***Detective Controls*** ▪ Reminders for periodic review and update of identifications or accuracy before annual due date. ▪ Utilize a passive or active discovery tool to identify Cyber Assets connected to the network including alerting. ***Corrective Controls*** ▪ Actions required to remediate any late reviews or approvals and update identifications and inventory. ▪ Utilize a tool to quarantine or remove unauthorized Cyber Assets from the network in a timely manner including alerting.

CIP-003-8 (Cyber Security – Security Management Controls)

Standard Requirement	Control Considerations
CIP-003-8 R1	***Preventative Controls*** ▪ Train personnel on cyber security policies. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Ensure the CIP Senior Manager understands and approves the cyber security policies prior to the due date. ***Detective Controls*** ▪ Reminders for periodic review before annual due date. ***Corrective Controls*** ▪ Actions required to remediate any late reviews or approvals.
CIP-003-8 R2 Section 1	***Preventative Controls*** ▪ Train personnel on cyber security awareness reinforcement. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Utilize multiple methods of reinforcement (direct and indirect communications, etc.). ▪ Retain all evidence associated with reinforcement. ***Detective Controls*** ▪ Reminders for periodic cyber security awareness reinforcement before annual due date. ***Corrective Controls*** ▪ Actions required to remediate any late reinforcements.

Standard Requirement	Control Considerations
CIP-003-8 R2 Section 2	***Preventative Controls*** ▪ Train personnel on physical access controls. ▪ Utilize layered (multiple) physical access controls. ▪ Utilize key management controls for locks, doors, etc. ▪ Utilize a visitor access control program. ▪ Document Physical Security Perimeter diagrams. ***Detective Controls*** ▪ Reminders for periodic review of physical access controls. ▪ Utilize alarms and alerting for unauthorized physical access. ***Corrective Controls*** ▪ Actions required to remediate any non-working physical access controls. ▪ Actions required to remediate any unauthorized physical access.

Standard Requirement	Control Considerations
CIP-003-8 R2 Section 3	***Preventative Controls*** ▪ Train personnel on electronic access controls. ▪ Utilize defense in depth electronic access controls applying the concept of least privilege. ▪ Evaluate and document all justifications for inbound and outbound electronic access. ▪ Utilize controls for malicious code and communications. ▪ Utilize controls for vendor remote access. ▪ Document network diagrams. ***Detective Controls*** ▪ Reminders for periodic review of electronic access controls. ▪ Utilize alarms and alerting for unauthorized electronic access and malicious code and communications. ***Corrective Controls*** ▪ Actions required to remediate any broadly defined electronic access controls. ▪ Actions required to remediate any unauthorized electronic access and malicious code and communications.

Standard Requirement	Control Considerations
CIP-003-8 R2 Section 4	***Preventative Controls*** ▪ Train personnel on Cyber Security Incident response. ▪ Incorporate both the IT and OT personnel including O&P personnel when implementing or testing the Cyber Security Incident response plan(s). ▪ Subscribe to DHS CISA industry alerts. ▪ Retain all evidence associated with testing or actual Reportable Cyber Security Incidents. ***Detective Controls*** ▪ Reminders for periodic testing of the Cyber Security Incident response plan(s). ▪ Utilize security event logs, alarms, and alerting of detected Cyber Security Incidents. ***Corrective Controls*** ▪ Actions required to remediate any late testing. ▪ Actions required to contain, eradicate, or have recovery/incident resolution of Cyber Security Incidents.
CIP-003-8 R3 and R4	***Preventative Controls*** ▪ *Train personnel on the identification and documentation of the CIP Senior Manager and delegate(s).* ▪ *Document the "specific actions" delegate(s) have been granted authority to do,* ▪ *Retain all evidence associated with CIP Senior Management and delegates identification and changes.* ***Detective Controls*** ▪ *Reminders for periodic review of the identified CIP Senior Manager and delegates* ▪ *Reminders to document changes within 30 calendar days.* ***Corrective Controls*** ▪ *Actions required to remediate any undocumented changes within 30 calendar days of a change.*

COM-002-4 (Operating Personnel Communications Protocols)

Standard Requirement	Control Considerations
COM-002-4 General Controls Considerations	***Preventative Controls*** ▪ Training on different types of communication (person-to-person, burst communication, etc.) and definitions. ▪ Develop a method to track training. ***Detective Controls*** ▪ Process to verify the effectiveness of the training. ▪ Process to review and ensure all personnel (within the company or third-party operating personnel) are trained according to the Standard. ***Corrective Controls*** ▪ Provide additional training as necessary based on detective controls.
COM-002-4 R3 COM-002-4 R3 (continued)	***Preventative Controls*** ▪ Develop onboarding process to identify new operating personnel who require three-part communication training prior to receiving an Operating Instruction. ▪ Develop a process to determine when operating personnel receive their first Operating Instructions to demonstrate that training was conducted prior to receiving an Operating Instruction. ▪ Process to identify and collect evidence of received Operating Instructions. ***Corrective Controls*** ▪ Establish a process to review records and verify that operating personnel use three- part communication when receiving Operating Instructions. ▪ For entities with a marketing agreement or a third-party operator, consider a process to

	verify periodically that all operating personnel at the marketer or third-party operator have received three-part communication training prior to receiving an Operating Instruction.
COM-002-4 R6	***Detective Controls*** ▪ Process to identify and collect evidence of received Operating Instructions. ***Corrective Controls*** ▪ Establish a process to review records and verify that operating personnel use three- part communication when receiving Operating Instructions.

MOD-026-1 (Verification of Models and Data for Generator Excitation Control System or Plant Volt/VAR Control Functions)

Standard Requirement	Control Considerations
MOD-026-1 R2	***Preventative Controls*** ▪ System to track compliance obligation due dates and ensure the verified model is submitted to TP within 365 days after commissioning date and on or before the 10-year anniversary of the last transmittal. ▪ Functional mapping for each applicable generating unit to ensure appropriate entities receive model submissions. ***Detective Controls*** ▪ Process to identify changes to the excitation control system or plant volt/var control function that alter the equipment response characteristic and require the GO provide revised model data or plans to perform model verification under MOD-026-1 R4. ***Corrective Controls*** ▪ Process to perform internal reviews of work performed by third-party contractors and verify the work and documentation is sufficient to demonstrate compliance with NERC Reliability Standards.

PRC-004-6 (Protection System Misoperation Identification and Correction)

Standard Requirement	Control Considerations
PRC-004-6 R1	***Preventative Controls*** ▪ Training for personnel responsible for analyzing BES interrupting device operations on process to make determination of whether the entity's Protection System components caused a Misoperation. ▪ Standardized analysis form with fields to capture information required to demonstrate the entity determined whether its Protection System components caused a Misoperation within 120 days of the BES interrupting device operation. ***Detective Controls*** ▪ Automated notification to personnel responsible for analyzing BES interrupting device operations when a BES interrupting device operation occurs. ▪ Process to submit BES interrupting device operation and Misoperation data to MIDAS and verify MIDAS submission data is consistent with internal data. ▪ Process to analyze all BES interrupting device operations to determine if the entity's Protection System components caused a Misoperation within 120 days of the BES interrupting device operation. ***Corrective Controls*** ▪ Management review of analysis forms to verify timeliness, accuracy, and completeness. ▪ System to track BES interrupting device operation dates and Misoperation determination dates.

Standard Requirement	Control Considerations
PRC-004-6 R5	***Preventative Controls*** ▪ Process to develop a Corrective Action Plan (CAP) for the identified Protection System component(s). ▪ Training for responsible personnel on process to develop CAPs and perform evaluation of applicability to the entity's other Protection Systems including other locations. ▪ System to track date cause of Misoperation was identified and date CAP was developed. ▪ Standardize CAP forms with fields to capture information required to demonstrate development of CAP and evaluation of applicability within 60 calendar days of first identifying a cause of the Misoperation. ***Detective Controls*** ▪ Process to track and document evaluation of CAPs applicability to entity's other Protection Systems. ▪ Perform an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations within 60 calendar days of first identifying a cause of the Misoperation. ▪ Develop a control to evaluate Standards and requirements that are affected as a result of implementing the CAP, especially if relay setting changes are made. ***Corrective Controls*** ▪ Management review of CAP forms to verify timeliness, accuracy, and completeness.

Standard Requirement	Control Considerations
PRC-004-6 R6	***Preventative Controls*** ▪ Process to proceed with implementation of CAPs following development and update each CAP if actions or timetables change, until completed. ▪ System to track implementation status of CAPs and timetables for implementation identified in CAPs. ***Detective Controls*** ▪ Automated notification when approaching dates associated with timetables for implementation identified in CAPs. ***Corrective Controls*** ▪ Periodic review of CAP implementation status and timetables identified in CAPs to verify CAPs are on schedule to be implemented within timetables identified in CAP, or if actions or timetables need to be changed.

PRC-005-6 (Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance)

Standard Requirement	Control Considerations
PRC-005-6 R3	***Preventative Controls*** ▪ Inventory of applicable Protection System Components with mapping of each Component to prescribed maintenance activities. ▪ System to track past maintenance dates and next maintenance due date for each Component. ▪ System to store maintenance records. ▪ Contractual agreements with third-party contractors hired to perform maintenance with specifications to perform prescribed maintenance activities. ***Detective Controls*** ▪ Automated notification when Components are approaching due date for maintenance activities. ▪ Ensure maintenance activities recorded have associated underlying maintenance records. ▪ Substation changes are appropriately included in maintenance programs. ***Corrective Controls*** ▪ Process to review maintenance records and ensure records demonstrate performance of prescribed maintenance activities. ▪ Escalation process when approaching due dates for maintenance activities are not addressed. ▪ Review of protection system tests by peer or supervisor

PRC-024-2 (Generator Frequency and Voltage Protective Relay Settings)

Standard Requirement	Control Considerations
PRC-024-3 R1, R2	***Preventative Controls*** ▪ Protection System design process or relay setting philosophy with identification of applicable functions and components (e.g. volts per hertz relays evaluated at nominal frequency, control systems within turbines or inverters that directly trip or provide tripping signals) and specifications to either set protective relays outside of "no trip zone" or document and communicate equipment limitations. *Note: GOs should account for projection of generator voltage protective relay settings to a corresponding POI voltage within the process. PRC-024-2 R2 specifies generator voltage protective relaying shall be set such that it does not trip the generating units as a result of a voltage excursion at the point of interconnection (defined as high voltage side of the generator step-up or collector transformer) that remains within the "no trip zone" of PRC-024 Attachment 2.* ▪ Inventory of all generator protective relays (including protective functions within control systems that directly trip or provide tripping signals to the generator) with identification of frequency and voltage settings on the relays. ***Detective Controls*** ▪ Review of relay level one-line diagrams and other design documentation to ensure applicable relays are accounted for within inventory. ▪ Process to identify, document, and communicate equipment limitations to the Planning Coordinator and Transmission Planner. Accurate functional mapping is critical to ensure appropriate entities receive the required communication.

PRC-024-3 R1, R2	▪ Change management process for relay setting changes to ensure changes do not cause generators to trip within "no trip zone" of Attachment 1 or Attachment 2. ***Corrective Controls*** ▪ Review of settings to verify protective relaying is not set to trip generator in "no trip zone" of Attachment 2, and review of relay setting documentation to verify accurate settings are documented.

VAR-002-4.1 (Generator Operation for Maintaining Network Voltage Schedules)

Standard Requirement	Control Considerations
VAR-002-4.1 General Controls Considerations	***Preventative Controls*** ▪ Train Generator Operators on developed processes and expectations pertaining to the applicable VAR requirements. ***Detective Controls*** ▪ Establish alarms and perform periodic reviews of events to verify compliance with established processes. ▪ Utilize a sheet such as the one on the ReliabilityFirst website to periodically check performance. https://www.rfirst.org/att-c-var-002-4-1-r2/?_rt=M3wxfHZhci0wMDJ8MTczNjQ0OTg0NA&_rt_nonce=f62fd65226 ***Corrective Controls*** ▪ Actions required to restore the equipment status to normal.
VAR-002-4.1 R1	***Detective Controls*** ▪ Process to verify the generator is in required control mode. ***Corrective Controls*** ▪ Establish internal controls for detecting AVR status changes and corrective control for restoring AVR to normal operations.

Standard Requirement	Control Considerations
VAR-002-4.1 R2	***Preventative Controls*** ▪ Train personnel on conditions of notification. ▪ Disseminate and develop process to notify TOP of voltage schedule deviations per conditions of notification. ***Detective Controls*** ▪ Process to verify seasonal voltage schedule and to implement any voltage schedule changes. ▪ Establish detective (e.g., alarms) internal controls for voltage schedule deviations. ***Corrective Controls*** ▪ Establish corrective internal controls for voltage schedule deviations. ▪ Evaluate personnel on conditions of notification.
VAR-002-4.1 R2.1	***Preventative Controls*** ▪ Develop a strategy to maintain voltage schedule when AVR is out of service. ***Detective Controls*** ▪ Collect evidence of maintaining the voltage schedule when the AVR is out of service.

Standard Requirement	Control Considerations
VAR-002-4.1 R2.2	***Preventative Controls*** ▪ Develop a business process for responding to voltage change directives and making notifications when the new schedule cannot be met. ▪ Develop a process to coordinate with the TOP to establish expectations for when a voltage change directive (setpoint change) cannot be met and the TOP requires notification. ***Corrective Controls*** ▪ Develop internal control for reviewing received voltage change directives and verifying voltage change directive process was followed.
VAR-002-4.1 R2.3	***Detective Controls*** ▪ Determine location from which voltage is being monitored and determine if it is at the same location as specified in the voltage schedule. ▪ Implement monitoring at location specified in voltage schedule or develop method for converting voltage values to the point being monitored.
VAR-002-4.1 R3	***Preventative Controls*** ▪ Process to notify TOP(s) of AVR status changes and track time of notification. ***Detective Controls*** ▪ Identify AVR status changes and time of status change. ***Corrective Controls*** ▪ Develop internal control for identifying and reviewing AVR status changes and verifying the reporting process was followed.

Standard Requirement	Control Considerations
VAR-002-4.1 R4	***Preventative Controls*** ▪ Identify conditions that could lead to a change in reactive capability ▪ Develop process to identify and report to the TOP(s) changes in reactive capability. ***Detective Controls*** ▪ Develop methods to identify conditions that could lead to a change in reactive capability when they occur. ***Corrective Controls*** ▪ Develop internal control for identifying and reviewing changes in reactive power capability and verifying the reporting process was followed.
VAR-002-4.1 R5	***Preventative Controls*** ▪ Establish process to identify and track requests from the TOP and TP to ensure responses are provided within 30 calendar days of a request. ▪ Process to retain and evaluate evidence for compliance.
VAR-002-4.1 R6	***Preventative Controls*** ▪ Establish a process to determine if tap settings would violate safety, an equipment rating, or a regulatory or statutory requirement. ▪ Process to document, notify, and provide a technical justification to the TOP if GO cannot meet specifications. ▪ Process to retain and evaluate evidence for compliance.

Contact Information

ReliabilityFirst
3 Summit Park Drive
Suite 600
Cleveland, Ohio 44131
(216) 503-0600

Entity Assist Visit Program: https://www.rfirst.org/tools-and-services/assist-visit/

Entity Assist Visit Coordinators:
Mike Hughes, Manager Entity Engagement, Mike.Hughes@rfirst.org, 216-503-0617
Ron Ross, Principal Reliability Consultant, Ron.Ross@rfirst.org, 216-503-0609
Joseph Jagodnik, Senior Reliability Consultant, Joseph.Jagodnik@rfirst.org, 216-503-0606

Welcome Package Coordinator:
Greg Sorenson, PE, Principal Technical Auditor, Greg.Sorenson@rfirst.org, 216-503-0686