NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

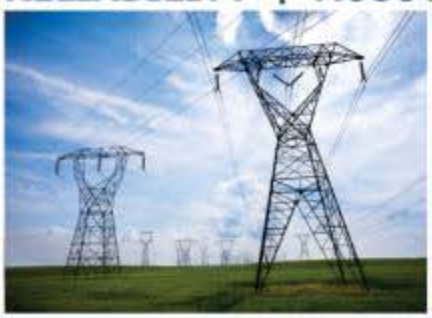
ERO Case Studies

Three Registered Entities

December 2012

RELIABILITY | ACCOUNTABILITY






3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Purpose

The purpose of these Electric Reliability Organization (ERO) case studies is to provide examples of compliance processes and tools (internal controls) utilized by various registered entities to manage specific compliance risk and reliability risk controls. It is the North American Electric Reliability Corporation (NERC) staff's opinion, based on the review of the selected processes and tools, that the creation and use of these tools enhanced the registered entities' overall operations and compliance with NERC Reliability Standards.

These case studies are a collaborative effort between NERC, the applicable Regional Entities (RE), and registered entities with the intent to share compliance insights, perspectives, and lessons learned for the benefit of all registered entities.

Internal Controls

Internal controls are methods of organization in which a company protects itself and ensures that it has control over its operations, engineering, planning, accounting, daily and business procedures, and that these policies are being followed. It consists of different checks, procedures, investigations and systems to ensure that the company is running smoothly and in adherence with applicable standards and good reliability and business practices. Internal control essentially protects the company from itself and seeks to safeguard against high impact grid events or cascading outages. Companies generally adapt their own definition of internal control and structure a program that suits their individual needs and concerns. Figure 1 provides a classic graphic representation of attributes regarding internal controls specifically in the areas of prevention, detection, and correction internal controls. For example, requiring periodic self-assessments would be a "detection" internal control and training would be a "prevention" internal control and lastly a corrective action program would be a "correction" internal control.[1]

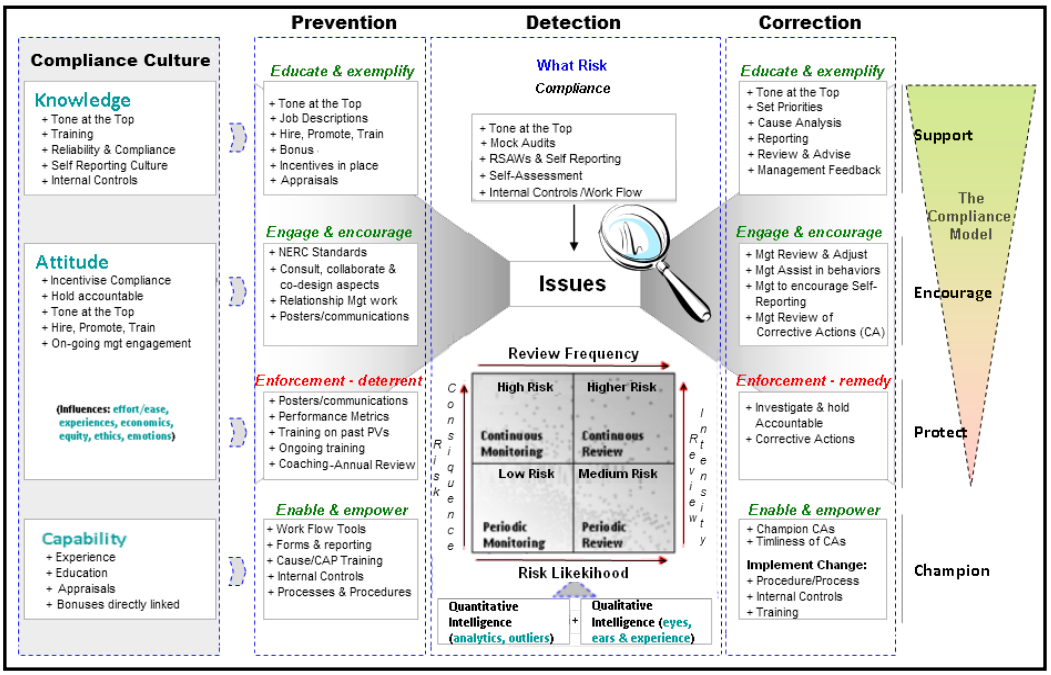


Figure 1: Internal Controls: Prevention, Detection, and Correction model

[1] Diagram adopted from: [LINK]

Executive Summary

These case studies are being presented to the users, owners, and operators of the bulk power system (BPS) in order to show examples of certain processes and tools (internal controls) being utilized by selected registered entities.

The selected registered entities are two small and one large entity, all with consistent operating and compliance histories. The first small registered entity (Registered Entity #1) is a small generation and transmission (G&T) company. The second is a large registered entity (Registered Entity #2) that is registered in multiple RE footprints and owns numerous generation, transmission, and distribution facilities. Lastly, Registered Entity #3 operates and owns transmission in a relatively small footprint.

It is NERC staff's opinion that the use of the internal controls identified in this report has contributed to the three registered entities' consistent operating and compliance histories and that the industry could benefit from the use of similar processes and tools. However, NERC staff recognizes that one size does not fit all and that these internal controls, with the suggested further improvements, should be considered on a case-by-case basis to determine the best fit for each company's individual business and operating model. Additionally, the use of any process or tool presented in these case studies does not guarantee compliance with the NERC Reliability Standards.

The following is an overall summary of the processes and tools specific to the three selected registered entities:

Registered Entity #1 – Registered Entity #1 has utilized outside contractor and industry peer support in order to assess its compliance capabilities by doing mock audits, auditor training, and procedure development. Registered Entity #1's Internal Compliance Program (ICP) is available to company staff on the corporate internal site. The Compliance Manager has direct access to the CEO and Board of Directors and has the authority to directly supervise all subject matter experts (SMEs). Lastly, SMEs and other staff who impact compliance have compliance accountability built into their job descriptions; this includes vice presidents and managers.

Registered Entity #2 – NERC staff has identified two areas that contributed to Registered Entity #2's compliance program: 1) a decentralized internal compliance process, where tone at the top is understood throughout the organization and individual compliance responsibilities are practiced by the line organization, and 2) a corrective internal control that utilizes a compliance condition reporting process (CCR) for communicating and managing compliance issues.

Registered Entity #3 – Registered Entity #3's "Process for the Reporting of Compliance with NERC Reliability Standards" (compliance procedure) defines the processes Registered Entity #3 uses to comply with NERC's mandatory standards and to review and report compliance issues to the RE or NERC, as appropriate. The compliance procedure also addresses periodic reporting, data submittals, non-scheduled reporting that may occur as a result of an investigation due to a system event, self-reporting, exception reporting, and response to an investigation resulting from a complaint or spot check.

Registered Entity #1 Case Study – Small Registered Entity

Entity Background

Registered Entity #1 (Entity #1) is a small generation and transmission entity that delivers power through a transmission network that provides service to fewer than 300,000 residential and commercial customers.

Entity #1's Operating and Compliance History

NERC staff performed a review of Registered Entity #1's previous audits, compliance programs, operating history (disturbance reporting, Generation Availability Data System (GADS), and Transmission Availability Data System (TADS)), and interviewed the RE's compliance manager. It is NERC staff's opinion that Registered Entity #1 has a consistent operating and compliance history.

Basis for Inclusion in this Case Study

After completing Entity #1's operating and compliance history review, NERC staff identified elements of Entity #1's ICP that contribute to their operating and compliance performance. These components are as follows:

- Internal RSAW Procedure,
- Audit-Ready Internal RSAW and Document Management Process,
- Standard methodology training by an outside vendor,
- Auditor training using outside vendors,
- Procedures for maintaining policy, plans, and procedures that highlight elements within each document that directly comply with the NERC Standards and Requirements,
- Risk assessment and mock-audit program using external vendors,
- Development and piloting of an automated reliability assessment that uses a state-of-the-art Learning Management System (LMS),
- Collaboration efforts with other entities, and
- Enhanced recordkeeping and auditing capabilities with respect to Critical Cyber Assets.

Details and Positive Attributes Regarding Entity #1's Internal Control(s)

Entity #1 monitors and maintains compliance with NERC Reliability Standards through its ICP. The ICP is owned by the manager of compliance and is made available to company staff on the corporate internal site, which is sponsored by Entity #1's applicable vice presidents. The Compliance Manager has direct access to the CEO and Board of Directors and has authority to directly supervise SMEs. The ICP follows whistle-blowing protection and disciplinary policy. Additionally, SMEs and any staff—including vice presidents and managers—who impact compliance have compliance accountability documented into their job descriptions.

Internal RSAW Procedures

Entity #1 procedures include 29 guidelines that are followed by the SMEs. Seven of these are mandatory; the remaining 22 are applied as needed. Criteria for inclusion are based on complexity and the risk associated with each requirement in a specific standard. The seven mandatory guidelines include the following:

- Update Narrative Response to NERC RSAWS,
- Provide "internal use only" comments for Narrative Response,
- Update Narrative Response to NERC assessment approach,
- Update Narrative Response to additional Entity #1 assessment approach items,

- List Current Evidence Documents, which are primary evidence (90%) submitted with an audit package,
- List Supporting Documents, which are secondary evidence (10%) not submitted with an audit package, and
- List Archived Evidence Documents.

Two examples of the 22 additional guidelines:

- Assessing impact of CANs (if they exist), and
- Assessing additional internal controls needed to reduce risk (if elevated levels of risk exist).

Audit-Ready Internal RSAW and Document Management Process

Entity #1's internal RSAWs are part of a process to be audit-ready at any time. Sample situations include:

- Spot check requested by the RE, and
- Entity #1 triggers an internal spot check audit using an outside vendor.

Being audit-ready is accomplished by:

- Maintaining revision control of the internal RSAWs. These require SMEs to at a minimum:
  - Update the narrative response required in NERC RSAWs,
  - Maintain "internal use only" comments for each narrative response,
  - Evaluate and supplement, when needed, each assessment approach item in the NERC RSAWs and provide internal comments,
  - Maintain an inventory of Evidence Documents used to directly comply with requirements (Primary Evidence), and
  - Maintain an inventory of Supporting Evidence (Secondary Evidence) that is intentionally not submitted with an audit package but provided if subsequently requested by evidence request without delay.
- Bookmarking reference links on the first page of each policy, plan, or procedure to elements within such documents that directly comply with requirements, thus reducing or even eliminating the need to bookmark documents traditionally completed in preparation for a scheduled audit or spot check,
- Maintaining Direct (Primary) Evidence submitted with an audit independently from Supporting (Secondary) Evidence that is intentionally not submitted in an audit. This reduces the need to use exhaustive PDF bookmarking in preparation for a scheduled three-year audit because:
  - An audit team can identify 90% of what is needed for compliance using the existing bookmarking built into the electric PDF copy of the executed plan, and
  - Entity #1 is in a position to provide any additional evidence in which the audit team identifies what additional supporting evidence is needed to show completeness.

  Note: This document management process follows a 90/10 rule and is simple for Entity #1 to maintain. In many cases they intentionally submit evidence that fulfills 90% of what is needed for compliance documentation. The remaining 10% is maintained in the Supporting (Secondary) Evidence area and can be accessed as needed.

Standard Methodology Training by an Outside Vendor

Entity #1 SMEs and other staff who impact compliance were trained by an outside vendor. This training breaks down each requirement into components (mostly known as directives, evidence, and attributes) that are easy to understand. Attributes of this training are as follows:

- Distinguish between what is and is not needed for compliance,
- Thoroughly analyze the attributes of the root requirement,
- Identify what components need industry input to establish baseline, interpretation, CANs, and other sources,

- Identify when internal corporate definitions and their basis are needed,
- Determine what level of evidence is minimal, thorough, or corroborate, and
- Determine type of evidence based on requirements that are conditional or event-driven that must be addressed in a formal plan or procedure.

Auditor Training using Outside Vendor

Entity #1's SMEs and staff who impact compliance were trained by an outside vendor on auditor knowledge and skills to further enhance their ability to comply with NERC Standards and understand internal controls/compliance culture.

Process for Maintaining Policy, Plans, and Procedures

SMEs follow a process where internal policies, plans, and procedures contain elements that directly comply with various requirements, such as:

- Include bookmark links on the first page of each policy, plan, or procedure that map directly to areas within the document that provide thorough evidence of compliance with the corresponding NERC Requirement,
- Such areas are additionally highlighted with red font.

This process reduces or eliminates the need to bookmark PDF documents, which can require significant resources, in preparation for a scheduled audit or spot check since the bookmarking and red font are already built in to an executed policy, plan, or procedure. The auditor is also instructed by the RSAW narrative response to go to the first page of a given policy, plan, or procedure and select the appropriate bookmarked reference link to locate the area of the text within the procedure (in red font) that provides thorough evidence of compliance.

Other benefits of this process include:

- Staff will know what areas of a policy, plan, or procedure are critical to compliance (red font),
- Staff will focus on policies, plans, and procedures as an operational tool when areas critical to compliance are identified with red font. This is particularly useful for staff with limited exposure to compliance (non-SME),
- Bookmarking and identification by red font identifies additional areas used for training, assessing risk, and strengthening internal controls,
- The first page includes a Title Block, Entity #1's logo, compliance reference links, version history, and filename,
- The Title Block in the header of each page includes the version number and effective date,
- The last page, which is the signature page, is replaced with a scanned signature page once signed. The approved package is then bundled together as a fully text-searchable PDF document,
- The link that ends with "A1" means that it is evidence for an attribute within a root requirement. For example, Attribute 1 of R1 of EOP-008 is EOP8A1. "A2" would mean the second attribute in a root requirement.

Risk Assessment and Mock Audit Program Using External Vendors

Preparation for Entity #1's recent 693 audits included the following:

- Outside vendor #1 with expertise in identifying directives, evidence, and attributes conducted gap analysis of 693 standards. The objective of this vendor was to ensure that Entity #1 covered requirements in detail. For example, they analyzed every prepositional phrase of every requirement.
- Outside vendor #2 conducted a risk assessment of 693 standards. However, this vendor included staffing with experience in the utility industry that included power markets, Regional Transmission Organization (RTO), control centers, and planning. This was done in order to thoroughly cover all 10 functional areas that Entity #1 is registered for. This risk assessment included classification of risk as low, medium, or high by requirement.
- Once the risk assessment was completed, outside vendor #2 and Entity #1's compliance staff worked with SMEs to mitigate risk identified as medium or high.
- Once the medium and high risks were mitigated, vendor #2 conducted a mock audit in which the mock audit:

- Tested an SME's knowledge,
- Identified more risk or areas of concern, and
- Prepared the SME with audit room experience.

Piloting the Automation of Risk Assessments uses Learning Management System (LMS)

Entity #1 utilizes a state-of–the-art LMS to automate a risk assessment process and internal self-certification. The piloted standard tested was FAC-008-3, which has a FERC enforcement date of 1/1/13. The SME was required to select the state of compliance of each requirement as either one of the following:

- Thorough,
- Minimal,
- Needs improvement, or
- I do not understand the requirement

The SME provided a narrative response that supported each selection. Lastly, the SME answered supplemental questions that tested their knowledge of the subject matter and highlighted important issues, such as the recent Southwest Blackout.

Collaboration Efforts with Other Entities

Entity #1 participates in an organized collaborative group of about 20 similar entities across the country. Collaboration includes an annual meeting, quarterly webinars, and webinars on lessons learned from audits (after an entity has completed an RE audit). Several staff members provide a variety of compliance services for all of the members, including a first cut of assessing standard development with recommendations, balloting with recommendations, other issues with recommendations, and training in the LMS that currently provides courses for over 50 NERC Standards.

Enhanced Auditing Capabilities with Respect to Critical Cyber Assets

Entity #1 contracted a vendor to develop and incorporate a software solution in an effort to automate its change control and configuration management practices in order to create enhanced recordkeeping and auditing capabilities with respect to Critical Cyber Assets. Before this project, Entity #1 relied on manual change control and configuration management practice. Deliverables of the project included the following:

- Establishing and enforcing repeatable processes that provide an auditable trail of historical data for easy reporting,
- Maintaining complete visibility of every component within Entity #1's Electronic Security Perimeters in terms of cyber assets, software configuration, and deficiencies,
- Eliminating the need to manually document and maintain information,
- Reducing the risk of human error,
- Alerting Entity #1's information technology staff of unauthorized network changes/access,
- Maintaining an audit trail of change activities,
- Preventing changes going undocumented/unapproved,
- Providing Entity #1 with a robust configuration management database, and
- Automation of Entity #1 change control and configuration management will assist the audit team's monitoring of Entity #1's compliance to the CIP standards.

Entity #1 developed a daily automated system scanner solution that could see all required aspects of their Windows-based machines from open network ports to the services that use them. Lastly, system administrators routinely receive a summary report of all changes that are identified from the daily scans.

Further Improvements

While it is NERC staff's opinion that the use of Entity #1's compliance procedure contributed to its operating and compliance history, NERC staff has identified two areas for Entity #1's consideration that could further strengthen its compliance program.

Observation Number 1: It is suggested that Entity #1 consider a corporate strategy that ensures compliance-related corporate goals are well communicated and aligned within the organization.

Basis: Guidance from FERC Order on a rigorous compliance program:

> "…As to employees engaged in misconduct, the issue of whether disciplinary action is appropriate (e.g., reprimand, suspension, reduction in pay or **bonus**, termination, etc.) depends on the circumstances surrounding the offense and the involvement of supervisory personnel or senior management. Similarly, the question of whether new or modified prospective controls are needed to prevent a recurrence is highly fact-specific."

Observation Number 2: Consider providing additional guidance regarding the coordination and management approval of a systematic approach to causal analysis for purposes of mitigation plans prior to submittal to the RE. Areas for consideration are:

- Does the mitigation plan address the "cause" of the possible violation versus the symptom?[2]
- Do the corrective actions address the following:
  - Immediate mitigation of the possible violation, and
  - Specific actions to correct the cause of the possible violation and to prevent recurrence of the possible violation

Basis: The NERC Rules of Procedure Appendix 4C "Uniform Compliance Monitoring and Enforcement Program" Section 6.2 provides, in part, the following criteria for mitigation plans:[3]

- The Possible, Alleged, or Confirmed Violations of reliability standards the mitigation plan will correct,
- The cause of the Possible, Alleged, or Confirmed Violations,
- The registered entity's action plan to correct the Possible, Alleged, or Confirmed Violations,
- The registered entity's action plan to correct the cause of the Possible, Alleged, or Confirmed Violations,
- The registered entity's action plan to prevent recurrence of the Possible, Alleged, or Confirmed Violations,
- The anticipated impact of the mitigation plan on BPS reliability and an action plan to mitigate any increased risk to the reliability of the BPS while the mitigation plan is being implemented,
- A timetable for completion of the mitigation plan, including the date the mitigation plan will be fully implemented and the Possible, Alleged, or Confirmed Violations corrected, and

Implementation milestones are no more than three months apart for mitigation plans with expected completion dates no more than three months from the date of submission. Additional violations could be determined for not completing work associated with accepted milestones.

[2] NERC has provided guidance in the systematic approach to Root Cause Analysis on the NERC website at [LINK]
[3] *See* Rules of Procedure, Section 6.2 of Appendix 4C at [LINK]

Registered Entity #2 Case Study – Large Registered Entity

Entity Background

Registered Entity #2 (Entity #2) is an investor-owned utility generating electricity at both regulated and non-regulated stations in three Regional Entities that owns transmission and distribution systems in two Regional Entities and markets electricity products in six Regional Entities.

Entity #2's registered functions in the NERC Compliance Registry are: Balancing Authority (BA), Distribution Provider (DP), Generator Owner (GO), Generator Operator (GOP), Interchange Coordinator (IC), Load Serving Entity (LSE), Planning Coordinator (PC), Purchasing and Selling Entity (PSE), Resource Planner (RP), Transmission Owner (TO), Transmission Operator (TOP), Transmission Planner (TP), and Transmission Service Provider (TSP).

Entity #2's Operation and Compliance History

NERC staff performed a review of Registered Entity #2's previous audits, compliance programs, and operating history (disturbance reporting, GADS, and TADS), and interviewed the RE's compliance manager. It is NERC staff's opinion that Registered Entity #2 has a consistent operating and compliance history.

Details and Positive Attributes Regarding Entity #2's Internal Control(s)

NERC staff identified two areas that contributed to Registered Entity #2's compliance program: 1) a decentralized internal compliance process, where tone at the top is understood throughout the organization and individual compliance responsibilities are practiced by the line organization, and 2) a corrective internal control that utilizes a compliance condition reporting process (CCR) for communicating and managing compliance issues.

Entity #2 implemented a decentralized compliance process and holds the line organization accountable for compliance by utilizing the following controls:

- Compliance is verified via the team's review of each Internal Compliance Control Package (ICCP package):
    - The ICCP package requires applicable line managers to demonstrate compliance using RSAWs (for Tier 1 standards)[4] and internally developed RSAW-type documents for non-Tier 1 standards, and
    - Each responsible line manager/SME must present his or her ICCP package annually for review by peers and corporate compliance staff.
- Corporate compliance holds weekly meetings with responsible managers within the line organization where compliance issues are addressed and accountability to deliverables is discussed,
- Executive management holds weekly meetings with directors and compliance staff to discuss compliance activities and other issues identified by management,
- Executive management holds weekly meetings to discuss a preselected issue (compliance and business) with representatives from each business line,
- Entity #2 is actively involved with the industry in the following areas:
    - Standard development and approval,
    - Peer assist mock audits,
    - RE compliance workshops, industry stakeholder meetings and training, and
- Corporate goals have compliance deliverables instead of touting zero-tolerance criteria. Identified areas are: (1) the need to self-report potential compliance issues, (2) status reporting and timeliness, (3) mitigation plan accountability/support, and (4) CCR status.

[4] Tier 1 NERC Standards are identified in the applicable actively monitored list (AML) on the NERC website at [LINK]

Further Improvements

While it is NERC staff's opinion that the use of Entity #2's compliance procedure contributed to its operating and compliance history, NERC staff has identified two areas for Entity #2's consideration that could further strengthen its compliance program.

Observation Number 1: Consider a communication strategy that aligns compliance-related corporate goals within the organization.

Basis: Basis: FERC's Policy Statement on Compliance provides the following guidance:[5]

> "…As to employees engaged in misconduct, the issue of whether disciplinary action is appropriate (e.g., reprimand, suspension, reduction in pay or **bonus**, termination, etc.) depends on the circumstances surrounding the offense and the involvement of supervisory personnel or senior management. Similarly, the question of whether new or modified prospective controls are needed to prevent a recurrence is highly fact-specific."

Observation Number 2: It was noted by NERC staff that the number of CCR items entered into the process has declined. Therefore, consider expanding the CCR process to capture compliance process improvements that are not associated with direct reporting to the applicable RE as Possible Violations. These items could be addressed, characterized, and closed by the line organization (shortened approval process).

Basis: The following excerpt from the FERC Policy Statement on Compliance provides a basis for this suggestion:

> "Implementation of an aggressive compliance program and strong direction by senior management to search out and report regulatory compliance issues may result in an increase of violations self-reported to the Commission. If a company demonstrates that such self-reported violations are the result of implementing increased compliance measures, the Commission will take these circumstances into account."

[5] The FERC Policy Statement on Compliance can be found on the FERC website at [LINK]

Registered Entity #3 Case Study – Small Registered Entity

Entity Background

Registered Entity #3 (Entity #3) is an investor-owned utility that delivers electricity to residential and industrial customers in a small footprint.

Entity #3's registered functions in the NERC Compliance Registry are:[6] Transmission Operator (TOP), Transmission Owner (TO), Transmission Provider (TP), Transmission Service Provider (TSP), Load-Serving Entity (LSE), and Distribution Provider (DP).[7]

Entity #3's Operation and Compliance History

NERC staff performed a review of Registered Entity #3's previous audits, compliance programs, and operating history (disturbance reporting, GADS, and TADS), and interviewed the RE's compliance manager. It is NERC staff's opinion that Registered Entity #3 has a consistent operating and compliance history.

Details and Positive Attributes Regarding Entity #3's Internal Control(s)

It is Entity #3's corporate policy to be compliant with all NERC Reliability Standards that apply to the functions for which it is registered. Entity #3's compliance procedure is a consistent internal controls document with the following key features:

- The compliance procedure is owned by Entity #3's manager of compliance and approved by the director of compliance, three vice presidents, and the senior vice president.
- The compliance procedure identifies the expectations for compliance responsibilities within Registered Entity #3's organization:
    - Entity #3 has listed responsibilities for each line manager and SME. Entity #3 provides a chart that identifies the NERC Reliability Standards that apply to each functional area;
    - Entity #3 has listed responsibilities for each director and his or her overall compliance responsibilities for review and approval of compliance materials are submitted by the manager or SME; and
    - A "Dash Board" is maintained and continually improved by Entity #3's compliance staff to provide instant access to company staff and senior management on progress of any specific regulatory requirement or milestone. It is configured to flag progress with appropriate colors that isolate risk-carrying requirements.
- The compliance procedure utilizes the NERC Self-Certification process to aid in monitoring the organization's ability to comply with all applicable Tier 1 and self-certifiable NERC Reliability Standards:
    - Entity #3 lists all applicable Tier 1 and reliability standards subject to self-certification by self-assessment and reporting due date, applicable function, and applicable NERC Reliability Standard.
- The compliance procedure calls for management notification of any possible violation of a NERC Reliability Standard:
    - Senior management must be notified,
    - Self-reporting to the RE is required, and
    - Mitigation plans must be developed.
- The compliance procedure provides a timeline diagram outlining the following:
    - Specific milestone actions that are required for the self-assessment are identified,
    - Timeline due dates for each milestone action are noted,

[6] The NERC Compliance Registry is found on the NERC website at [LINK]
[7] The NERC Functional Model is found on the NERC website at [LINK]

- Applicable tools required for each milestone are described, and
- Scheduled improvements to the compliance procedure for application of information are:
  - Lessons learned from Event Analysis[8]
  - Address future changes to the NERC and Regional Reliability Standards
  - Compliance Application Notices (CAN)[9]
  - Compliance Analysis Report (CAR)[10]

Further Improvements

While it is NERC staff's opinion that the use of Entity #3's compliance procedure contributed to its consistent operating and compliance history, NERC staff has identified three areas for Entity #3's consideration that could further strengthen its compliance program.

Observation Number 1: Consider applying an internal control regarding the remaining non-Tier 1 and non-self-certified NERC Standards and Requirements. For example, each responsible manager or SME would develop a streamlined report for the compliance lead that documents a self-assessment on the following attributes relative to the NERC Standards and Requirements that apply to them:

- Applicable NERC Standard and Requirement,
- Internal Controls (procedure title and revision),
- Last review of internal control(s),
- Any recommended changes, challenges, improvements, or future challenges—such as up-and-coming changes to the NERC Standards—and the plan for implementation,
- Manager attestation that entity is or is not in compliance, and
- Periodicity equal to the audit cycle (six months before the scheduled audit to allow for self-identification of any possible violations)

Basis: From the NERC Rules of Procedure[11]

> "…all BPS users, owners, and operators are required to comply with all applicable ERO governmental authority-approved reliability standards at all times. RE reliability standards and RE variances approved by NERC and the applicable ERO governmental authority are enforceable and apply to all registered entities responsible for meeting those reliability standards within the RE boundaries, whether or not the BPS user, owner, or operator is a member of the RE."

Observation Number 2: Consider having the compliance staff report directly to the chief executive officer and the Board or to a committee thereof instead of the vice president of engineering.

Basis: On October 16, 2008, the Federal Energy Regulatory Commission (FERC) issued its "Policy Statement on Compliance."[12] FERC stated, "The purpose of this Policy Statement is to provide additional guidance to the public on compliance with our governing statutes, regulations, and orders." Regarding independence, the Commission also stated, "Compliance official independence is an important hallmark of a strong commitment to compliance. For example, compliance officials should be able to bring compliance matters directly to the Board of Directors or a committee of the Board (or equivalent governance of other organizations)."

[8] Event Analysis program and lessons learned can be found on the NERC website at [LINK]
[9] Compliance Application Notices (CANs) are found on the NERC website at [LINK]
[10] Compliance Analysis Reports (CARs) are found on the NERC website at [LINK]
[11] *See* Rules of Procedure, Section 401.2 at [LINK]
[12] The FERC Policy Statement on Compliance can be found on the FERC website at [LINK]

Additionally, please note the second bullet below where the Commission suggests specific actions to aid companies in the development of their compliance programs:

- Prepare an inventory of current compliance risks and practices,
- Create an independent Compliance Officer, who reports to the Chief Executive Officer and the Board, or to a committee thereof,
- Provide sufficient funding for the administration of compliance programs by the Compliance Officer,
- Promote compliance by identifying measurable performance targets,
- Tie regulatory compliance to personnel assessments and compensation, including compensation of management,
- Provide for disciplinary consequences for infractions of Commission requirements,
- Provide frequent mandatory training programs, including relevant "real-world" examples and a list of prohibited activities,
- Implement an internal hotline through which personnel may anonymously report suspected compliance issues, and
- Implement a comprehensive compliance audit program that includes the tracking and reviewing of any incidents of noncompliance and submits the results to senior management and the Board.

Observation Number 3: Consider providing additional guidance regarding the coordination and management approval of subsequent mitigation plans prior to submittal to the RE's portal. Areas for consideration are:

- Does the mitigation plan address the "cause" of the possible violation?
- Do the corrective actions address the following:
    - Immediate mitigation of the possible violation, and
    - Specific actions to correct the cause of the possible violation and to prevent recurrence of the possible violation

Basis: The NERC Rules of Procedure Appendix 4C "Uniform Compliance Monitoring and Enforcement Program" Section 6.2 provides, in part, the following criteria for mitigation plans:[13]

- The Possible, Alleged, or Confirmed Violations of reliability standards the mitigation plan will correct,
- The cause of the Possible, Alleged, or Confirmed Violations,[14]
- The registered entity's action plan to correct the Possible, Alleged, or Confirmed Violations,
- The registered entity's action plan to correct the cause of the Possible, Alleged, or Confirmed Violations,
- The registered entity's action plan to prevent recurrence of the Possible, Alleged, or Confirmed Violations,
- The anticipated impact of the mitigation plan on BPS reliability and an action plan to mitigate any increased risk to the reliability of the BPS while the mitigation plan is being implemented,
- A timetable for completion of the mitigation plan, including the date the mitigation plan will be fully implemented and the Possible, Alleged, or Confirmed Violations corrected, and

An implementation milestone no more than three months apart for mitigation plans with expected completion dates more than three months from the date of submission. Additional violations could be determined for not completing work associated with accepted milestones.

[13] *See* Rules of Procedure, Section 6.2 of Appendix 4C at [LINK]
[14] NERC has provided guidance in the systematic approach to Root Cause Analysis on the NERC website at [LINK]

Summary and Contact Information

Summary

These case studies are a collaborative effort between the ERO and other registered entities to provide the industry with compliance insights, perspectives, and lessons learned for the benefit of all entities. To that end, NERC staff encourages the industry to consider the application of these processes and tools (internal controls) into their own internal compliance programs.

Please contact Earl Shockley or Jim Hughes if you have any questions.

Contact Information

Earl Shockley
Senior Director Compliance Operations
Earl.Shockley@nerc.net

Jim Hughes
Manager of Compliance Projects and Initiatives
Jim.Hughes@nerc.net