NERC Compliance and Organization Structure

Considerations for Managing NERC Compliance

May 2010

Table of Contents

- The Current State of NERC Compliance
- NERC Compliance Maturity Model
- Organizational Options
- Advantages/Disadvantages of Governance Models
- Organization Design
- Key Processes
- How ScottMadden Can Help

The Current State of NERC Compliance

- The $25 million fine to FPL, along with myriad other penalties issued across the country, continues to keep utilities' executives focused on NERC compliance
  - The lack of specificity in the stipulation agreement has left the industry speculating about what FERC is trying to communicate; FPL did not admit to having violated any reliability standards
- Upon approval of the recent omnibus filing, FERC stated that "an increasing level of compliance with the standards" would be expected in the future*
  - Penalties assessed in 2009 were nearly three times the number in 2008
  - FERC is now participating in NERC audits and FERC leadership is focusing on enforcement
  - FERC has re-opened NERC penalty assessments and recently fined an RRO
- Many companies have worked diligently to prepare for early audits, develop auditable documentation, and ensure that they meet the standards, but much work remains
  - What sufficed in early audits for compliance and evidence is no longer adequate
- Companies are now considering how best to organize NERC compliance activities within the enterprise to enable them to meet evolving requirements. Over time they want to ensure that:
  - Self-reports are made in a timely manner
  - Corporate-wide processes supporting compliance activities are in place and effective (i.e., document management, procedure updating)
  - Standards development activities are coordinated
  - Compliance work and expertise are not duplicated throughout the organization

The most successful companies will ensure that their organization and processes can evolve to meet changing NERC and FERC priorities

*Sources: NERC proposes to assess another $591,000 in reliability standard violation penalties, SNL 1/5/10

                 FL Reliability Council fined $350,000 for role in February '08 blackout, SNL 3/5/10

                 Industry interests to FERC: Don't second guess NERC on reliability standard violation penalty, SNL 3/30/10

NERC Compliance Maturity Model

It has been our observation that companies pass through several stages on their way to becoming top performers in NERC reliability standards compliance

Ongoing Compliance
- Continuous cycle (as standards evolve, procedures are updated, and personnel are trained)
- Ongoing management of key compliance indicators
- Demonstrated culture of compliance
- Active regulatory relationships
- Flexibility to respond to evolving NERC/FERC priorities

Integration and Automation
- Requirements seamlessly coordinated by all business units
- Documents managed electronically
- Workflow and metrics automated
- Compliance dashboard defined

Accountability
- Dedicated compliance organization established
- Key compliance indicators identified and monitored
- Individual standard owners assigned
- Annual updating requirements defined

Defined Processes
- Dependencies identified
- Compliance requirements defined
- Results measured
- Mitigation activities established

Maturity Level

Low   High

Key to moving through the stages of maturity is implementing an appropriate organization design for managing the work

scottmadden
MANAGEMENT CONSULTANTS

Organizational Options

There are multiple options for organizing NERC compliance activities—each comes with advantages and disadvantages

Centralized to Decentralized

Centralized

- Subject matter expertise on NERC compliance resides in a central "shared" function, usually in the Compliance organization

- NERC compliance may be grouped with other types of compliance

- This group is responsible for all self-certifications, self-reports, and managing preparation for audits

- This organization manages all standards development activities

- The group has a clear line of sight to CEO, BOD

Hybrid

- A central group performs oversight for NERC compliance, but compliance work is done in the business units

- Expertise in standards resides in the central group; expertise in operations resides in the business units

- Standards development work (participating in standards development, balloting) is centrally coordinated; priorities are set by a central group

- Participation in standards development teams is managed by the business units

- The approach leverages the expertise of the subject matter experts (SMEs) in the business units

Decentralized

- Expertise and responsibility for compliance reside in the business units

- Business units retain both operational and compliance/ standards expertise

- Participation in standards development is managed by the business units

Advantages/Disadvantages of Governance Models

Centralized — **Hybrid** — **Decentralized**

Advantages

- All NERC SMEs reside in a single, centralized group ensuring consistent responses to audits, processes, and documentation
- All activities are coordinated through a single group ("one throat to choke")
- Corporate group has access to CEO, BOD as needed
- All standards development activities are prioritized for the corporation

Disadvantages

- The NERC compliance work is grouped with dissimilar functions at the corporate level; expertise for NERC compliance is usually much more technical
- As SMEs move away from the operating groups, operating groups need to backfill positions
- May lead to duplication of functions

Advantages

- Minimizes duplication of work; a central group provides oversight while the business units ensure the work is compliant
- Corporate oversight group has access to CEO, BOD as needed

Disadvantages

- Without clear roles, responsibilities, and processes, the oversight role is challenging
- Not always clear who is responsible when a violation occurs; greater risk of finger-pointing if something goes awry
- Standardization of documentation and processes is more difficult

Advantages

- Expertise in standards resides with operational expertise
- The people doing "the work" also ensure the work is compliant with standards

Disadvantages

- Without oversight, this may lead to divergent views and interpretations of standards across the enterprise
- Participation in standards development may be ad hoc and not coordinated across the enterprise
- Difficult to judge the effectiveness of business unit programs without an "external" perspective
- Potential duplication of efforts as multiple business units track relevant standards
- May require additional business unit staff to meet both operational and compliance requirements
- Makes a direct line of sight to CEO, BOD difficult

scottmadden
MANAGEMENT CONSULTANTS

5

Organization Design

- ScottMadden believes the hybrid model is the most appropriate for managing NERC compliance activities
    - Minimizes duplication of work; a central group provides oversight while the business units ensure the work is compliant
    - Provides a central point of coordination and accountability
    - Facilitates executive involvement and oversight
    - Enables a corporate view of compliance risk
- Based on recent discussions with industry leaders and client work, it appears that this model is being implemented widely across the industry. It requires:
    - Executive commitment
        - The stakeholders involved are the heads of various business units. Senior leadership is needed to ensure all are on board
    - Well-defined processes
        - These processes cut across various organizations and must have clearly defined handoffs
    - Clearly articulated roles and responsibilities
        - All parties must understand what they contribute to these cross-functional processes

> *While the hybrid model is the most appropriate for managing NERC compliance, it is the most difficult to implement and requires ongoing executive commitment*

scottmadden
MANAGEMENT CONSULTANTS

Key Processes

The table below suggests a possible delineation of functions across the oversight group and business units. These responsibilities should be clear and flexible enough to adapt to evolving NERC/FERC priorities

Compliance Process	Oversight Group	Business Units
Setting Standards for NERC Compliance	■ Establishes the standards that documentation must meet ■ Creates formats and templates that the business units use for documenting compliance	■ Ensures that the work being done meets the standards ■ Creates the documentation needed to demonstrate compliance
Self-Certification	■ Ensures that the company self-certifies on the required dates ■ Reviews evidence with the certifying officer	■ Provides evidence to the certifying officer that the organization is in compliance
Audit Preparation	■ Manages preparation for an audit ■ Educates business units on the standards and their requirements ■ Educates business units on the audit process ■ Reviews evidence	■ Ensures that standards are assigned to specific SMEs ■ Works with the oversight group to ensure that SMEs are prepared and have all the necessary supporting evidence ■ Completes RSAWs
Standards Development	■ Coordinates standards development efforts ■ Ensures corporate priorities are addressed	■ Provides SMEs to contribute to select drafting teams

scottmadden
MANAGEMENT CONSULTANTS

Key Processes (cont'd)

Compliance Process	Oversight Group	Business Units
Internal Audit	■ Identifies deficiencies in documentation and evidence through internal spot checks or mock audits	■ Provides SMEs to amend documentation and evidence to meet the standard set by the oversight organization
Self-Reporting	■ Manages the process to identify violations and self-report to the RRO as appropriate ■ Serves as the primary point of contact with the RRO	■ Identifies incidences of non-compliance and provides them to the oversight group ■ Provides subject matter expertise during any investigation
Investigation and Settlements	■ Manages the negotiations with the RRO, NERC, and FERC ■ Works with senior management to determine negotiating position; approve settlement	■ Provides evidence and support for negotiations ■ Provides engineering or other expertise on company compliance with standard

> *Roles and responsibilities for each of these processes should be clear.*
> *In the hybrid model, management must ensure that both the compliance organization and the business units fulfill their obligations*

How ScottMadden Can Help

- Designing the NERC compliance organization and associated processes; ensuring that stakeholder needs are addressed
- Assessing the existing NERC compliance organization and processes; providing actionable recommendations
- Developing and documenting a plan for audit documentation
  - Ongoing compliance tracking and reporting plan
  - Self-reporting process
  - Audit documentation templates
- Auditing specific standards
- Assisting with the assembly/compilation of compliance documentation
- Identifying and resolving reporting gaps between new requirements and existing documentation
- Ensuring consistent reporting across operating companies
- Identifying a compliance documentation repository, knowledge-sharing approach, and methodology to respond to regulatory inquiries and for self-reporting
- Preparing a long-range plan for documentation review and refresh