scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.

Confirming Compliance – Do You Have Proper Oversight of Your Contractors?

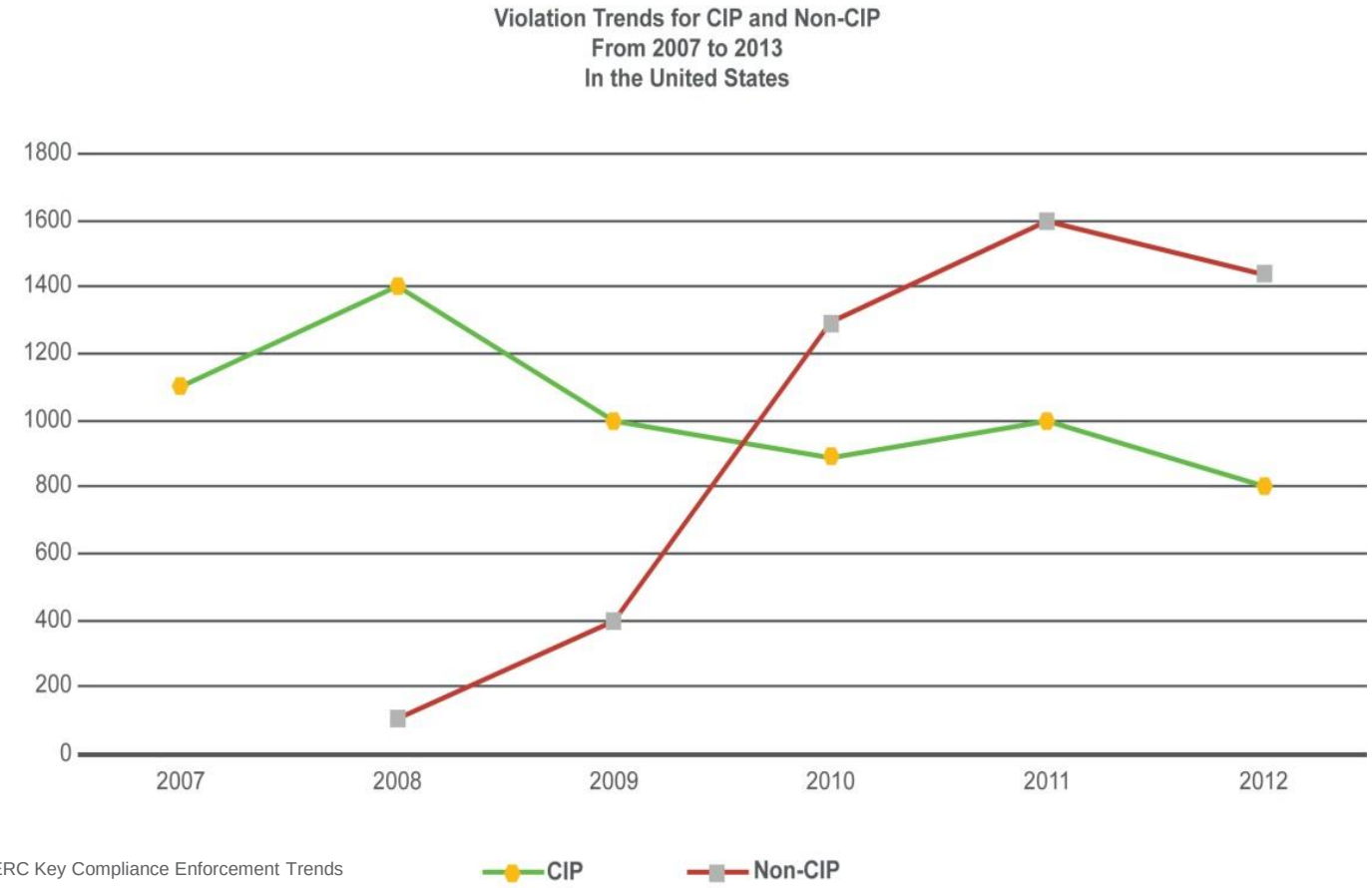
Establishing a NERC Compliance Governance Model

January 2014

The Current State of NERC Compliance

Situation

- Many utilities and merchant operators rely heavily on outsourced providers to operate and maintain transmission and generation assets; these contractors have varying degrees of familiarity with compliance standards and required documentation
- Even with the strategy to rely heavily on outsourced providers, transmission and generation asset owners are still accountable for many standards across the operator, service provider, and owner-registered functions
- As shown in the chart below, the total number of violations over a recent five-year period is beginning to stabilize; however, many entities continue to struggle with specific NERC standards



NERC Key Compliance Enforcement Trends

scottmadden
MANAGEMENT CONSULTANTS

Organizational Options

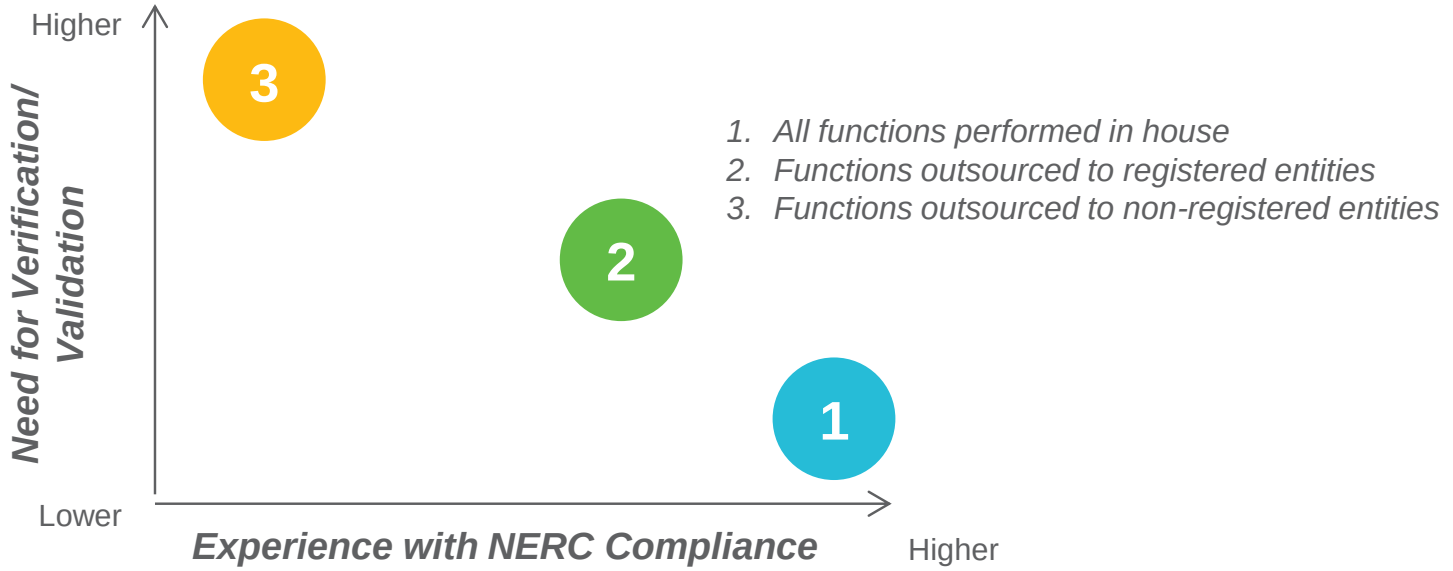
Most companies have chosen a hybrid option to organize NERC compliance activities

Centralized	**Hybrid**	Decentralized
• 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	• A central group performs oversight compliance for NERC compliance, but compliance work is done in the business units • Expertise on standards resides in the central group; expertise on operations resides in the business units • Standards-development work (participating in standards development, balloting) is centrally coordinated; priorities are set by central group • Participation on standards-development teams is managed by the business units • The hybrid approach leverages the expertise of the subject matter experts in the business units	• 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

- A NERC compliance governance model ensures that compliance documentation is correct and accurately reflects how the owner organization will operate. This is particularly important when key functions are outsourced

Need for Governance

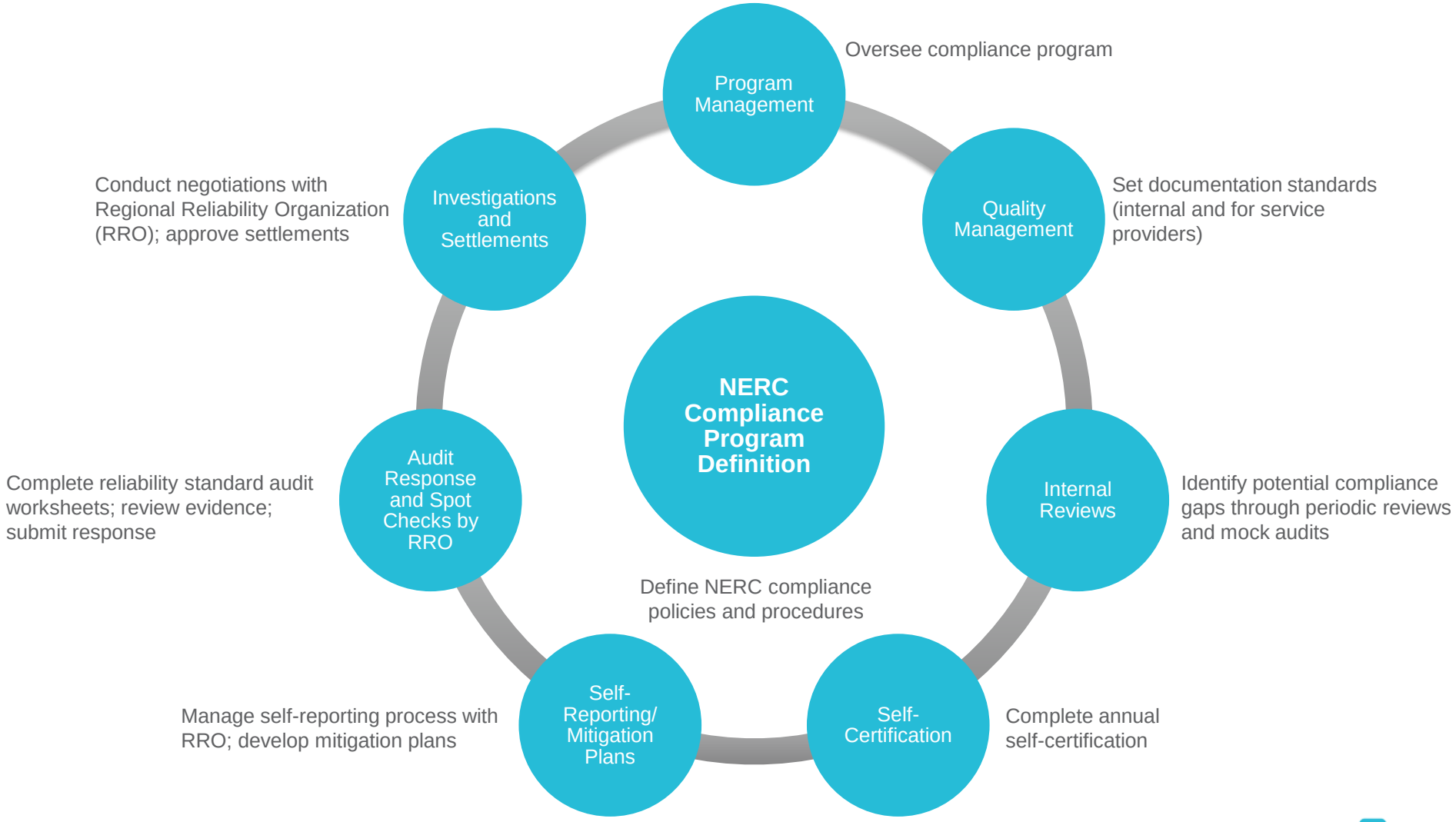
- It is our view that establishing a governance model for NERC compliance is key to mitigate violations found by auditors and avoid costly fines
- Clear governance and oversight are required to ensure that the work is performed in a compliant manner and that asset owners have the ability to confirm compliance
- Asset owners should establish an oversight process and independent verification mechanisms to validate that service-provider activity is performed to the prescribed standards and records are documented at a level sufficient to demonstrate compliance
- Ultimately, asset owners will be held accountable for complying with the NERC standards and as such need to put in place the appropriate governance over their outsourced providers



Electric transmission and NERC compliance subject matter expertise is required to validate evidence and successfully manage the compliance program with the reliability entity.

Governance Model Overview

The figure below illustrates ScottMadden's view of key NERC compliance processes and proposed roles for owner organizations by process area. The asset owner should consider how each is managed and performed.



It is expected that asset owners have governance and oversight over operations and maintenance performed on their assets.

scottmadden
MANAGEMENT CONSULTANTS

Our View

Asset owners must provide governance and oversight. We see well-defined compliance processes and open communication with outsourced providers as critical to success.

Owner	■ Build or source operational and compliance competencies to operate the assets ■ Establish requirements for outsourced providers	■ Define the NERC compliance program, including policies and procedures to set the foundation for on-going compliance ■ Validate contractor compliance evidence	■ Revise or amend contracts to ensure language is specific enough to hold outsourced providers accountable ■ Identify subject matter experts best able to address requirements
Outsourced Providers	■ Perform the work and provide evidence to demonstrate compliance ■ Provide evidence in the form required by the asset owner	■ Clarify expectations in line with the owners' culture of compliance	■ Be prepared to participate in joint mock audits with owners as requested

scottmadden
MANAGEMENT CONSULTANTS

How ScottMadden Can Help

- Establishing a governance model for NERC compliance
- 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 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
- Building a security management system to formalize governance and oversight of both physical and information security controls
- Creating a standard information risk assessment process and security risk management program
- Developing an enterprise security awareness program incorporating both regulatory and leading practice requirements

Contact Us

Cristin Lyons

Partner

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
cmlyons@scottmadden.com
O: 919-781-4191

Smart. Focused. Done Right.

Luke Martin

Manager

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
lukemartin@scottmadden.com
O: 919-781-4191

Smart. Focused. Done Right.