scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.®

Why Embed NERC Compliance into Operations?

Revised November 2021

Common Symptoms May Indicate More Significant Problems

Our clients experience the following common symptoms related to their NERC program:

- Excessive time spent preparing for an audit
- Employees unaware of compliance requirements
  Limited compliance oversight
- Lack of line accountability for compliance activities
- Mitigation actions which are not targeted to the issue
- Workers are unclear on their roles and responsibilities

Which are often discovered through events such as:

- Difficulty locating evidence
- Access controls for CIP information not properly restricted
- Missed patch evaluations
- Overdue or incomplete mitigation actions
- Repeat violations (e.g., GOP fails to notify TOP)
- Evidence is not stored properly for maintenance and testing

And can be an indicator of underlying problems:

- Lack of compliance infrastructure
- Gaps between internal operational processes and NERC standards
- No defined roles or responsibilities
- Ineffective issue resolution

scottmadden
MANAGEMENT CONSULTANTS

Why Embed NERC Compliance into Operations?

Problems that Lead to Violations

Lack of a Culture of Compliance 1
Employees are generally not aware of what NERC compliance is or why it is important. As a result, execution of compliance activities varies widely.

NERC Compliance is not close enough to the work being performed 2
Corporate compliance groups do not understand the day-to-day operations well enough leading to internal standards, documentation and guidance that is not actionable

No defined roles or responsibilities 3
Accountability model for compliance-related activities are not clearly defined or understood. Roles and responsibilities are not documented, often causing issues when key individuals retire or transition to new roles

Lack of compliance infrastructure 4
Evidence is not stored in a common repository. NERC Compliance activities (routine work and mitigation actions) are not visible to line management making it difficult to monitor regulatory-required tasks.

Gaps between internal processes/procedures and NERC standards 5
Internal compliance procedures are unnecessarily complex, or confusing, and do not meet the requirements of the NERC Standards

Ineffective issue resolution 6
NERC-related resolution processes do not address fundamental problems which can lead to recurring violations and are often not aligned with established corrective action programs

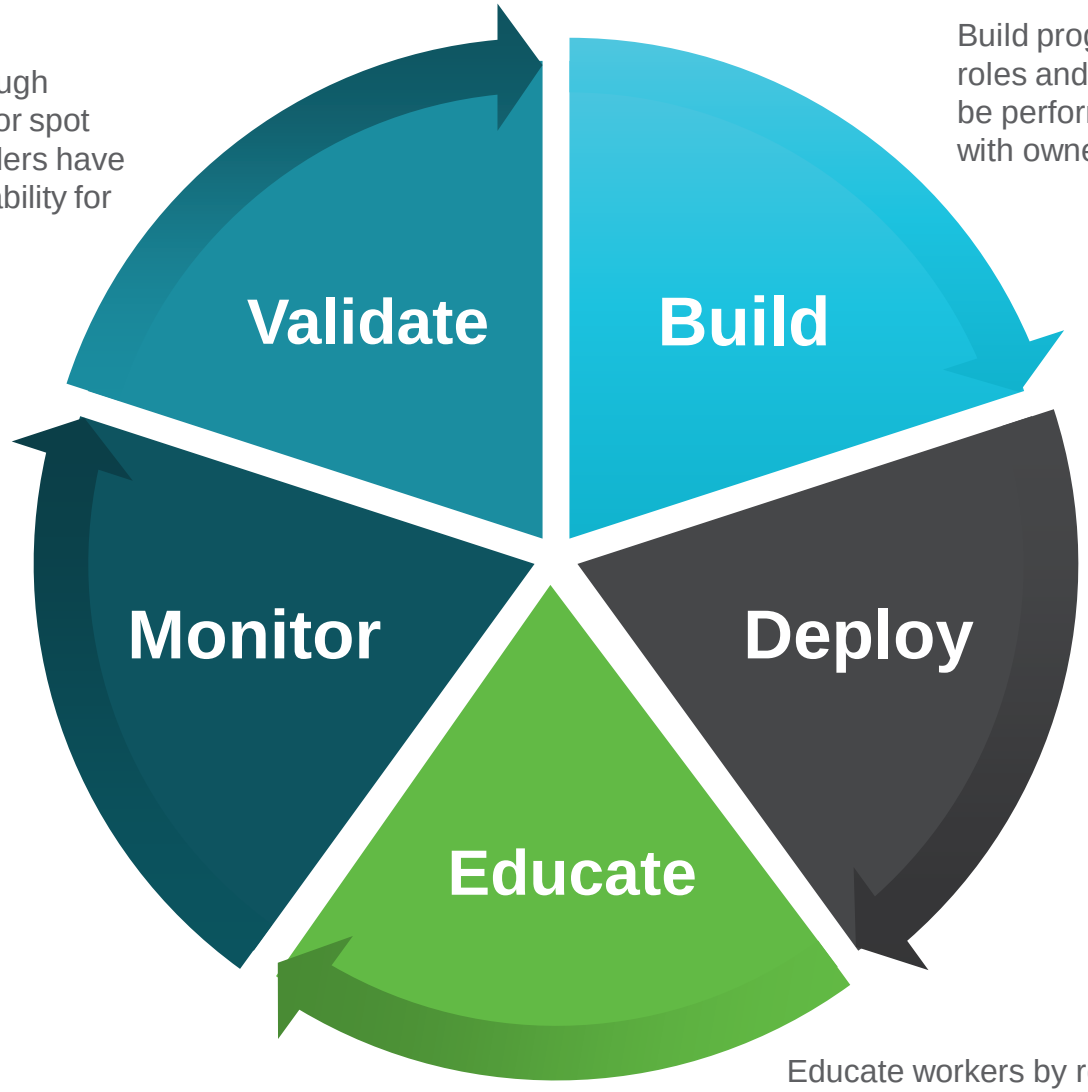
Lack of coordination between IT and CIP Compliance 7
Lack of communication and coordination between IT and CIP Compliance leading to inefficiencies and potential compliance gaps. Confusion or overlap on who performs CIP compliance and cybersecurity work

scottmadden
MANAGEMENT CONSULTANTS

How to Operationalize a NERC Compliance Program

Validate compliance through internal self-certification or spot checks. Ensure line leaders have awareness and accountability for NERC Compliance

Build programs and procedures which specify roles and responsibilities and how work should be performed. Define an accountability model with ownership for each standard



Monitor completion of work and store evidence in approved locations. Use line managers to ensure work is performed on time, and compliance analysts to ensure evidence meets standards

Deploy job plans with work instruction details and embed this within the work management or ticketing system

Educate workers by role for awareness and technical performance of NERC compliance work

scottmadden
MANAGEMENT CONSULTANTS

ScottMadden's NERC Compliance Service Overview

With our NERC compliance services, our energy experts have the capabilities and experience to:

- Assess gaps in programs, procedures, and processes, compare them to industry leading practices, and develop mitigations measures to address gaps and improve the compliance program
- Address findings by improving or implementing NERC compliance program elements such as training, work management processes, procedures, and program documents
- Develop and conduct role-based training rather than positional based
- Conduct field validation of the program activities to ensure the people executing the work are able to practically apply the training, procedures, and processes that have been developed
- Develop detailed programs, procedures, and processes that comply with the regulations without adding significant burden or time to your daily tasks

We bring more than 35 years of experience working with utilities across North America to help you address the challenges of NERC compliance and create a successful and cost-effective compliance program.

scottmadden
MANAGEMENT CONSULTANTS

Cybersecurity, CIP and Operational Technology (OT) Capabilities

Capabilities

Cybersecurity		NERC CIP	Operational Technology (OT)
Corporate – Security / IT	Energy	IT, Generation, Transmission	Energy
■ Security Operating Model Services • Governance • Security risk assessment • Business planning • Metrics and performance management • Security functional support	■ Governance and accountability model ■ Work scope delineation ■ Sourcing evaluation for Cybersecurity and OT tools ■ Cyber hygiene – risk-based application of security controls to specific assets	■ NERC CIP Compliance Implementation • Program development • Program recovery • Process improvement • Education and NextGen Training® • Change management • Field visits to validate controls and procedure execution ■ NERC CIP audit support and technical advisory	■ Organizational design and staffing ■ Technical advisory support ■ Work management ■ Program development ■ OT/IT integration or separation ■ Architecture and system design review ■ Owner's engineer / functional advisor ■ Transformation

■ Cybersecurity program development
■ Cybersecurity program implementation

scottmadden
MANAGEMENT CONSULTANTS

CONTACT INFORMATION

Sean Lawrie
Partner

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
slawrie@scottmadden.com
O: 919.781.4191
M: 404.731.6338

Luke Martin
Partner

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
lukemartin@scottmadden.com
O: 919.714.7615
M: 919.349.3922

Todd Ponto
Director

ScottMadden, Inc.
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
tponto@scottmadden.com
O: 919.781.4191
M: 802.342.3837

scottmadden
MANAGEMENT CONSULTANTS