



What you need to know about NERC reliability compliance.



Proactively Addressing Mandatory Reliability Standards in the Electric Power Industry.

Introduction

A sea change is sweeping through the North American bulk electricity system in the wake of the U.S. Energy Policy Act of 2005 (EPAAct). Previously voluntary reliability programs under the aegis of the North American Electric Reliability Council (NERC) are transitioning to mandatory standards under the Federal Energy Regulatory Commission (FERC), with substantial financial penalties for non-compliance. The enforcement time line commenced on January 1, 2007, while financial penalties may be imposed as early as July 1, 2007 (pending final FERC and Canadian provincial approvals).

Reliability Standards Emerge

Reliability standards had their genesis following the major North American power outage experienced in November 1965 throughout the Northeast, with the implementation of voluntary operating policies and planning standards. These were designed to ensure the reliability of the bulk power system in the United States and Canada. Subsequent outage events, such as the summer 1996 Western grid blackouts, and the August 2003 Northeast blackout, led to further emphasis on these standards. As a result of EPAAct, FERC certified NERC in 2006 as the Electric Reliability Organization (ERO) with full oversight for enforcing reliability standards compliance. An additional result of EPAAct is that FERC now has full authority to approve all reliability standards. To date, NERC has submitted 107 standards to FERC for approval; 83 have been approved while 24 are awaiting approval pending further refinement. Many of the approved standards received conditional approval and will require updating—a process that may require up to two, and in some cases three years to complete. Furthermore, some of the standards in their initial form do not specify measures or compliance criteria, which complicates enforcement.

Scope of Mandatory Reliability Standards

Any entity that owns, operates, or uses any portion of the Bulk Power System must comply with these new mandatory reliability standards. The compliance process itself involves periodic, formal NERC audits by the Regional Reliability Councils (RRC) every three years. The process also involves active self certification, periodic reporting of compliance data and statistics, exception reporting of disturbances, and self reporting of any non-compliance with NERC policies, procedures, or standards.

To illustrate the complexity of the compliance process, consider a utility that owns and operates transmission. As such, it must adhere to the NERC reliability standards and participate fully in the compliance

process. For instance, the company must demonstrate compliance with a host of standards, some of which are: 1) transmission operations (TOP); 2) personnel performance, training, and qualifications (PER); 3) critical infrastructure protection (CIP); 4) emergency preparedness and operations (EOP). To comply with personnel performance standards, for instance, the company must file written job descriptions of each operating position in the control room, as well as written operating procedures. In addition, the company must implement initial and ongoing training programs for all operating personnel. Complying with CIP standards requires the company to establish, maintain, and document cyber security awareness programs as well as personnel risk assessments, and physical security programs for each identified physical asset. To comply with TOP standards, the company must develop, implement and maintain formal policies and procedures for a range of reliability activities as well as maintain specified data records for a range of time frames. In the EOP area, the standards mandate a host of procedures and contingency plans to address potential emergencies, including specific personnel contingency plan training and demonstration of actual contingency plans. As company executives recognize, the compliance requirements illustrated just by the examples cited in these four reliability categories encompass multiple major areas of company operations.

This paper explores the scope of the issues involved as an entity prepares for a NERC reliability standards compliance audit. It also examines the pre-audit steps that bulk power entities can take now to clearly demonstrate self compliance when audited by their Regional Reliability Council. Central to these tasks is how an entity can best approach developing and implementing internal processes that will fully support an effective self-reporting and audit program compliant with the NERC reliability standards. While this paper emphasizes the pre-audit phase of the compliance process, due to the ongoing nature of the self reporting requirements, it is equally relevant to establishing a continuous compliance process.

Audit Readiness: Pre-Audit Considerations

Entities subject to the NERC reliability standards face multiple decision points on how best to approach establishing a compliance program and on the types of processes, tools, and technology that best support their approach. Making the right decisions, tailored specifically to the needs and challenges of a given entity, before the initial NERC compliance audit can help an entity become “audit ready.”

An entity boosts its audit readiness by establishing a compliance process and identifying possible compliance gaps early in the process.

Identifying and addressing potential risks to compliance is key. An entity boosts its audit readiness by establishing a compliance process that coordinates the monitoring, analysis, and reporting of the appropriate data; identifying possible compliance gaps early in the process; and implementing the processes

necessary to close any identified gaps. Such a proactive, integrated, and transparent process will help entities better manage potential non-compliant audit findings and minimize negative impacts.

How an entity approaches the pre-audit process determines its readiness for the audit itself and post-audit activities. An effective road to the most positive outcome includes:

- Identifying the NERC functional model applicable responsibilities
- Identifying the applicable reliability standards based on the entity's functional responsibility
- Identifying who within the entity's organization is responsible for each applicable standard
- Collecting the necessary data to demonstrate standards compliance and to identify any compliance gaps

Identifying Applicable Reliability Responsibilities and Standards

Because bulk power entities have long been subject to voluntary compliance with NERC operating policies and planning standards (both of which have transitioned into the current mandatory reliability standards), most are already very knowledgeable about the reliability responsibilities and standards categories relevant to their functions. However, a brief review of these issues helps to illuminate the process, tools and technology decisions needed to build an audit ready entity.

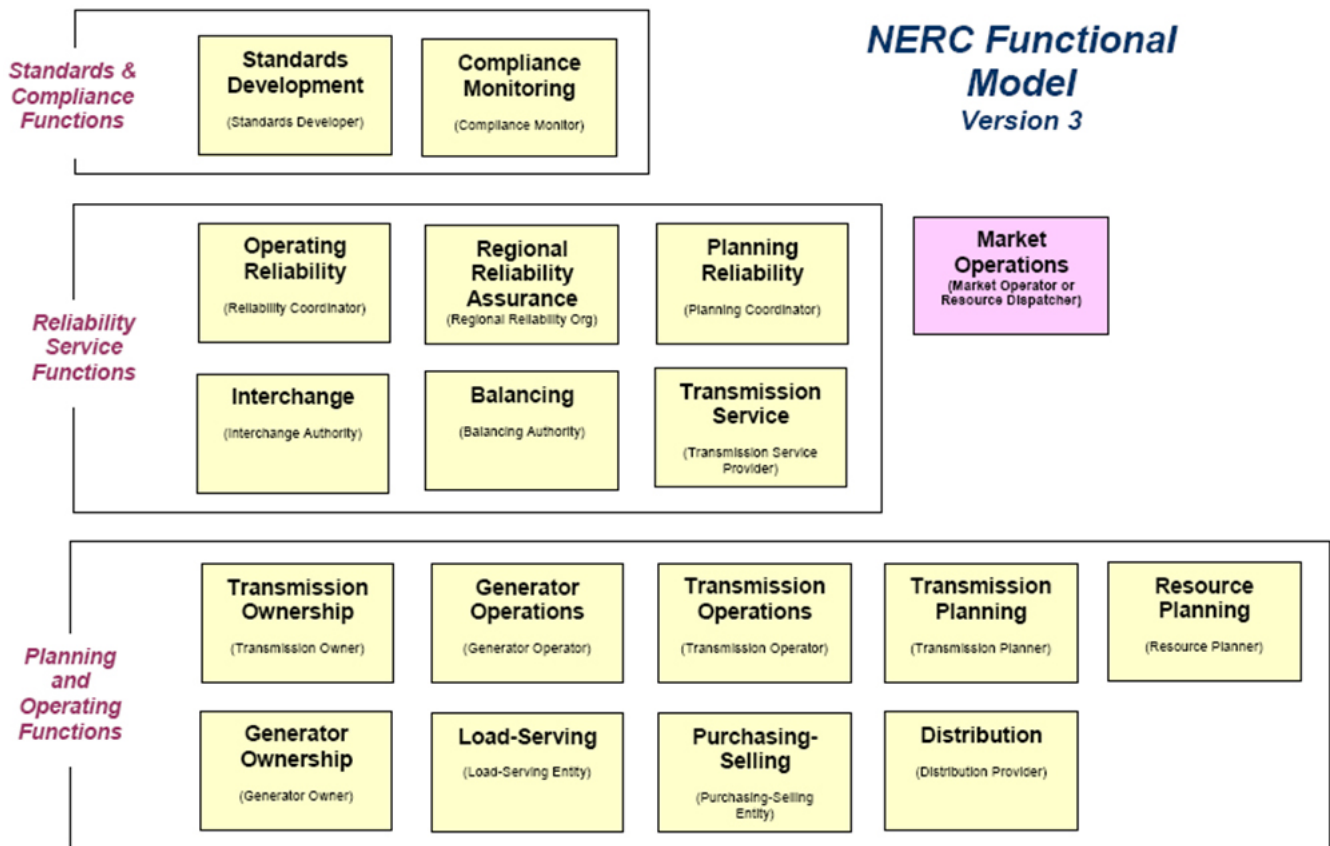
An objective team of assessors, specially trained to collect pertinent data and identify areas of non-compliance, can perform without the constraints that might hamper an internal team

Responsibility functional model

A thorough understanding of an entity's NERC reliability responsibilities helps to ensure that appropriate decisions on the compliance processes and needed technologies are made. At the outset, any entity responsible for any part of the bulk power system reliability must comply with NERC reliability standards. Beyond that, the type of entity and its functions in the bulk power system define an entity's specific compliance responsibilities. Figure 1 illustrates the NERC functional model, which defines three main categories of functions: 1) standards and compliance; 2) reliability service; and 3) planning and operation. Various types of entities fit within these broad functional categories.

Figure 1. Reliability Functional Model

Each entity must comply with the particular reliability standards relevant to their function's specific areas of responsibilities. These particular standards are found within a framework of categories that NERC developed.



Reliability standards categories

The NERC reliability standards are classified within 14 specific categories (see Table 1). Mapping the NERC function-based entity designations described above with these 14 reliability categories provides a matrix, which illustrates the relationship between the functional entity and the reliability standards (see Table 2). Each category contains multiple standards and each standard consists of multiple requirements. Table 2 shows the relationship between standard categories and functional responsibilities if at least one requirement within a category is applicable.

Table 1. Reliability standard categories

BAL	Resource and Demand Balancing	MOD	Modeling, Data, and Analysis
CIP	Critical Infrastructure Protection	ORG	Organization Certification
COM	Communications	PER	Personnel Performance, Training, and Qualifications
EOP	Emergency Preparedness and Operations	PRC	Protection and Control
FAC	Facilities Design, Connections and Maintenance	TOP	Transmission Operations
INT	Interchange Scheduling and Coordination	TPL	Transmission Planning
IRO	Interconnection Reliability Operations and Coordination	VAR	Voltage and Reactive

Table 2. Functional entity/reliability standard relation

		Reliability Standards Categories													
		BAL	CIP	COM	EOP	FAC	INT	IRO	MOD	ORG	PER	PRC	TOP	TPL	VAR
Functional Reliability Entities	Standards Developer														
	Compliance Monitor														
	Reliability Coordinator	X	X	X	X	X	X	X			X		X		
	Regional Reliability Org	X	X		X	X	X		X			X		X	
	Planning Coordinator					X			X					X	
	Interchange Authority		X				X								
	Balancing Authority	X	X	X	X		X	X			X	X			
	Transmission Service Provider		X				X	X	X					X	
	Transmission Operator	X	X	X	X		X	X			X	X	X		X
	Generator Operator	X	X	X	X			X				X	X		X
	Transmission Owner		X			X		X	X			X			
	Generator Owner		X		X	X		X	X			X			X
	Transmission Planner					X			X					X	
	Resource Provider								X						
	Load Serving Entity	X	X		X	X		X	X			X	X		
	Purchasing-Selling Entity						X						X		X
Distribution Provider					X						X	X			

Because these reliability standards continue to evolve, uncertainty remains about the pending and additional future standards. Some of the approved standards require revision, and NERC plans to adopt additional standards by the end of this decade. To stay abreast of changing standards and compliance requirements, bulk power entities need to carefully monitor this continuous standards development process, which is likely to persist at least for the next several years. This inherent uncertainty drives an entity’s need for a flexible and responsive compliance process, nimble supporting tools, and robust technology platforms, as discussed in the next section.

Identifying People, Processes and Data

People, processes and data are the building blocks of a strong compliance program. Following three core readiness steps can provide a strong foundation in this regard:

- 1) assessment,
- 2) remedial action plan, and
- 3) implementation.

Taken together, these activities serve to gather and record findings of non-compliance, as well as to conduct a risk assessment. With this information, entities can prioritize allocation of time, budget and resources to address any areas of non-compliance. By following these steps, an entity can better establish or enhance an easily accessible data collection method that supports the self-compliance process. Secondly, the process generates an audit-readiness report to help ensure that the actual NERC audit proceeds smoothly.

The inherent uncertainty of pending and additional future standards drives an entity's need for a flexible and responsive compliance process, nimble supporting tools, and robust technology platforms.

1) Assessment

Essentially a gap analysis, the pre-audit assessment compares the desired, compliant state of operations with the current state of operations. Any gaps are the deficiencies that must be rectified to satisfy the specific standard and achieve compliance. A pre-audit assessment helps entities improve performance during a NERC audit by providing an opportunity to correct or begin to correct deficiencies before NERC identifies them.

Effective gap analysis relies on accessing the right data. This, in turn, requires identifying who within the entity is primarily responsible for adhering to any specific NERC standard. Different individuals deal with different data areas within an entity. By matching a “face” with a requirement, an entity can more easily assemble all the pieces of information needed for a pre-audit assessment as well as improve performance during an actual NERC audit.

2) Remedial action plan

A pre-audit assessment might demonstrate deficiencies in certain compliance areas. By identifying such deficiencies early in the process, the entity can develop short-, medium-, and long-term action plans to address the deficiency as well as to prioritize the activities needed to carry out remedial action. For instance, a pre-audit assessment might identify the lack of formal policies and procedures for responding to Interconnection Reliability Operating Limit violations, a point of non-compliance with TOP standards. In this case, the remedial action plan may include developing and maintaining such policies and procedures.

3) Implementation

With the process and tools in place to capture, review and interpret key data points from across the enterprise, an entity can implement and document the remedial action plans needed to close the gaps between current and desired operational states. For example, a pre-audit assessment may identify a deficiency in data that NERC auditors need to assess compliance for a particular standard. The implementation stage would implement the remedial plan to ensure that data compilation occurs as needed for ongoing compliance.

Resources for establishing an ongoing compliance process

From an oversight and management perspective, the pre-audit process is a highly time-consuming endeavor. Many entities benefit by teaming with an external partner who can assume day-to-day process management. An objective team of assessors, specially trained to collect pertinent data and identify areas of non-compliance, can perform without the constraints that might hamper an internal team. This resource can streamline the process, allowing internal personnel to focus on their primary job responsibilities. Other entities may already have an ongoing, full time compliance process and need only external support for data analysis and to pinpoint areas where the process can be improved. Certification professionals can be a valuable resource, since they already have extensive expertise in auditing methodologies.

People, processes and data are the building blocks of a strong compliance program.

Because effective compliance efforts hinge on efficient, thorough data collection and analysis, automated software tools offer the capability to harvest data at points throughout an entity, reducing the time investment of executives. Due to the continued evolution of the reliability standards, software tools must also be able to closely monitor changing requirements and align data collection efforts accordingly. Using a software tool that can deliver updates to standards tailored to the needs of the entity is a crucial capability.

Conclusion

Any new regulatory requirements pose risks and the implementation of NERC reliability standards compliance is no exception. Entities that act early and proactively to be certified compliant will benefit in several ways. First they will establish a positive relationship with NERC auditors and rule setting committees that will enhance their influence in setting further reliability compliance standards. Shareholders and investors are likely to view compliant entities with more confidence. Most obviously, compliance minimizes the possibility of financial penalties as well as other financial, legal and personal risks that can damage an entity's reputation.

Key Areas of Consideration

- Identify which standards you must comply with. Keep in mind that some standards are not yet final and even those that have been approved are subject to change.
- Identify data needed to demonstrate compliance and what tools and processes will be needed to manage the compliance process.
- Identify key individuals responsible for each standard.
- Assess current vs. . compliant state and identify gaps.
- Prepare a plan to remedy each deficiency.
- Prioritize deficiency remedies.
- Implement remedies.
- Ensure ongoing data compilation for compliance.

About the Authors

Sam Brattini is an Executive Consultant with KEMA, Inc. responsible for managing projects that provide planning, procurement, and implementation consulting services to electric utility operations. Prior to joining KEMA, he was a senior design engineer at the GE Switchgear Department in Philadelphia. He was also an Adjunct Professor of Electrical Engineering at Villanova University while employed by GE. Sam has had engineering consulting assignments with utilities Internationally. Sam is a registered professional engineer in the Commonwealth of Pennsylvania, the Commonwealth of Virginia, and the State of Michigan. He is the chairman of the Backup Facilities NERC Reliability Standard SAR Drafting Team.

William Cassel is a Senior Principal Consultant with KEMA, Inc., and has over 40 years of experience with control center operations and the design and implementation of large energy management and distribution management systems, including 15 years of experience with an electric utility. Mr. Cassel has provided a full range of services including program management, organizational studies, operations procedures and training development, system requirements definitions, system procurement, and project implementation and acceptance support. His in-depth knowledge has been especially pivotal in ISO/RTO projects, in national control center projects with two- and three-level hierarchical system configurations, and in large-scale distribution management projects around the world. Mr. Cassel is a Registered Professional Engineer in the State of Delaware.

Joe Moran is Vice President of Operational Systems Consulting at KEMA. He has nearly 20 years of experience in all aspects of power operations and market operation system projects including procurement specification development, evaluation of suppliers' capabilities, statement of work development, and testing. Mr. Moran has worked with ISOs, market participants, investor owned utilities, G&Ts, and municipals providing various services.

For more information:

Sam Brattini
(215) 997-4500 x 270
sam.brattini@kema.com

William Cassel
(215) 997-4500 x 262
william.cassel@kema.com

Joe Moran
(215) 997-4500 x 264
joseph.moran@kema.com

www.kema.com