INSIGHT. INTEGRITY. INTEGRATION.

ComplyTec
ENTERPRISE COMPLIANCE

NERC Compliance for the Power Generation and Bulk Transmission Industry

Security and reliability concerns for the North American bulk power system

The United States Department of Homeland Security identifies the Energy Sector as one of 16 Critical Infrastructure Sectors whose assets, systems, and networks (physical or virtual) are so vital that their incapacitation or destruction would have debilitating effects.[1] As such, the energy sector is divided into three (3) interrelated segments, including electricity, oil, and natural gas, which are overseen by the Federal Energy Regulatory Commission.

The security and reliability of the North American power grid is threatened daily by multiple sources, including physical and cyber threats.[2] Physical threats include natural hazards, technological/accidental hazards, and adversarial/human-caused threats, while cyber threats include such activities as hacking, malicious code, loss of intellectual property, phishing, denial of service, and insider damage.

To detect, monitor, limit, and mitigate activities that threaten the security, stability, and integrity of the power grid, the U.S. Federal Government has enacted legislation that appoints the North American Electric Reliability Corporation (NERC) to monitor the bulk power system, and develop and enforce a series of reliability standards

What is NERC and how does it ensure the integrity of the bulk power system?

NERC is an international regulatory authority tasked with ensuring the North American Bulk Power system remains secure and reliable. To this end, NERC develops—and legally enforces—reliability standards to which all qualified power-generating and bulk transmission companies must adhere.

The Energy Policy Act of 2005 outlined federal regulations governing the development and enforcement of Reliability Standards for the planning and operation of the Bulk Power System in the United States. The legislation charged the Federal Energy Regulatory Commission (FERC) with the task of establishing an independent electric reliability organization (ERO) to develop mandatory Reliability Standards subject to FERC approval and to monitor industry participants' compliance with those standards. NERC was designated as the ERO by FERC in 2006.

NERC Reliability Standards are grouped into 14 categories relating to bulk-power system operations and planning. Each standard describes what measures are to be completed, who must complete them, and in many cases, how compliance will be measured. Thus, each standard may include several requirements that will impose duties on multiple parties.

Failure to comply with NERC regulations can result in fines of up to $1 million per day per violation.[3] Thus, it is prudent for power generation and bulk transmission companies to implement regulatory compliance solutions to ensure that all aspects of the organization adhere to NERC standards.

[1] U.S. Department of Homeland Security Critical Infrastructure Sectors. https://www.dhs.gov/critical-infrastructure-sectors.

[2] Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats. ICF International, Inc. (June 2016).

[3] Appendix 4B: Sanction Guidelines of the North American Electric Reliability Corporation (Effective July 1, 2014). In: NERC Rules of Procedure (Effective March 19, 2015).

How can companies remain compliant with NERC standards?

Utilities and organizations required to comply with NERC regulations and laws have multiple options, including:

- Manual processes (spreadsheets, word processing documents and email);
- Generic Governance, Risk, and Compliance (GRC) tools;
- Isolated point solutions.

While manual processes provide an adequate starting point for organizations to track, monitor, and remain compliant, such solutions quickly become inefficient as complexity increases, thereby creating additional challenges. Generic GRC tools are costly, complex, and time-consuming for organizations to modify due to the nature of open GRC platforms. Few point solutions are available in the market, and are generally rigid, resulting in costly customizations to be performed at the expense of the organization. Thus, all such solutions fail to adequately address organizations' needs of providing a customizable, fully-functional, scalable, and dynamic NERC compliance solution—this is where ComplyTec derives its competitive advantage and offers value-added solutions.

Why ComplyTec is your best solution for NERC compliance

ComplyTec is a world-class provider of custom enterprise compliance solutions. For their custom NERC compliance solutions, ComplyTec aligned with leading NERC Compliance Subject Matter experts who have spent their careers in the power generation and bulk transmission sector. Leveraging such partnerships, ComplyTec has developed a customizable, end-to-end NERC compliance solution that provides clients with a comprehensive framework to meet, track, monitor, and remain compliant with all NERC regulations and laws. The ComplyTec solution allows organizations to:

- Meet NERC regulatory and compliance obligations. ComplyTec's NERC framework minimizes the risk of costly, public compliance failures and reputational damage by confidently managing the overall NERC compliance posture, and reducing the costly time burden on critical resources. It does this by automating task assignments, report creation, and controls assurance testing using a custom centralized portal.
- Create exception requests, remediation plans, and findings to correct all issues uncovered during the controls testing process.
- Eliminate manual, non-scalable NERC compliance activities by implementing a consistent and repeatable process for managing the everchanging NERC regulatory landscape.
- Expand the overall understanding and visibility to better manage NERC requirements. Improve assessments of relationships between organizational information assets and business processes and/or processing activities that are in the scope of the NERC regulatory requirements.
- Improve understanding, visibility and status tracking of NERC related incidents.

Thus, with ComplyTec's full-service, end-to-end NERC Compliance Solution, companies eliminate the risk of compliance failures and costly punitive actions by leveraging an efficient and automated framework for updating, tracking, reporting and alerting on all aspects surrounding an organization's NERC regulatory landscape.

ComplyTec offers a full suite of enterprise compliance resources

ComplyTec has a successful 20-year track record of providing North American companies with a comprehensive set of enterprise compliance solutions.

ComplyTec is a leading provider of business-driven security and risk management solutions to critical sectors including banking, government, healthcare, retail and utilities. ComplyTec recognizes that it is crucial for business and security leaders to understand how security incidents impact the overall business, in terms of continuity, intellectual property, data and reputational damage.

ComplyTec provides software solutions and consulting services to assist organizations to quantify business and IT risk. We provide identity management solutions to protect against today's most consequential attack vector, identities. Ensuring user accounts aren't compromised using identity management tools is analogous to locking the front door. ComplyTec also offers advanced threat detection and response solutions to protect against cyber-attacks. Realizing all breaches cannot be prevented all the time, we also must detect them to respond to them, isolate them, mitigate the damage, and recover from them, preferably automatically and with minimal damage or no damage at all.

Thus, ComplyTec's full suite of enterprise compliance solutions guarantees that your organization is fully covered in all aspects of Governance, Risk Management, and Compliance.

Risk Management
Cyber Security
DOC
Compliance