

# Compliance Auditing for NERC



## Ease your NERC Compliance Efforts While Reducing Overall Costs

*Energy providers face increasing pressure to secure their operations from cyber security threats. Several high profile breaches, constant virus and worm threats, as well as the summer 2003 electrical blackout, have resulted in increased scrutiny. Further, in response to Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection, the federal government has demanded that the energy industry develop standards of practice to ensure the security of the nation's energy infrastructure. The collection, retention and analysis of event and log data is a key requirement for compliance. SenSage helps organizations quickly implement Compliance Auditing for NERC solutions that uniquely deliver actionable results.*

In August 2003, the North American Electric Reliability Council (NERC) approved the Cyber Security Standards for electric power providers. Like other security regulations such as HIPAA, Sarbanes-Oxley, and GLBA, NERC mandates the goals for information security, but not how to achieve them.

In July 2005 the Standards Drafting Team released the updated Cyber Security Standards. At the heart of these controls is an infrastructure with extensive logging and auditing mechanisms capable of storing and protecting massive volumes of log data throughout an entire enterprise network.

### **Protecting Energy Companies – Identifying and Preventing Cyber Threats**

Given the criticality of the nation's energy infrastructure, NERC calls on energy companies to develop comprehensive security strategies. These strategies must cover protection of critical cyber assets, ongoing monitoring to detect security threats, and comprehensive incident response to contain security breaches. However, most organizations focus their security efforts at the perimeter – preventing outsiders from getting inside. The IT research firm, Gartner Group, reports that “over 70% of unauthorized accesses to information systems are committed by employees.”

Cyber threats, especially insider threats, are difficult to detect when existing security infrastructure focuses on protecting the perimeter. Insiders are not denied access by firewalls, they have valid user-names and passwords and their activity does not trigger IDS alerts. The key to detecting abuse early is instituting a comprehensive, consistent and frequent review of information system activity – quite simply, the data contained in log files. These log files contain the records of all IT activity. By analyzing this data, organizations can identify, investigate and respond to security incidents. The NERC Cyber Security Standards specifically recognizes the threat from insiders, and mandates energy companies to review internal log records to identify suspicious behavior. (See the attached table for more detail.)

Every workstation, email system, database, router, firewall, and server can produce thousands (even millions) of records daily. In aggregate, an Agency can easily accumulate 100s of millions of log records to review every day. Given the sheer volume of data, and the breadth of different sources, log analysis presents a daunting challenge.

### **The SenSage Solution – Your Answer to NERC**

SenSage provides energy companies with enterprise log management capabilities needed to secure their information systems and comply with NERC regulations. SenSage is a

purpose-built solution for collecting, retaining and reviewing massive volumes of event logs. These logs are the legal record required by IT Security and government regulatory compliance. By automating the collection, archival, and analysis of log records from all systems – SenSage gives organizations much better visibility into IT activity, helping to identify and respond to security threats (including insider abuse) and comply with the NERC regulations.

SenSage was developed specifically to solve the challenges of enterprise-wide log management. SenSage solutions scale to support virtually unlimited volumes of event logs, storing months or even years of records in an efficient and compressed format. The product’s unique compression

technology facilitates queries under compression, producing rapid search results. SenSage’s web-based Analyzer provides an easy-to-use interface for viewing, creating and running reports, and performing comprehensive investigations. SenSage works seamlessly with all common platforms and legacy systems to produce the exhaustive and unified audit trails recommended by NERC.

### IT Auditing and Logging Controls

The following table summarizes the auditing and logging requirements in the NERC Cyber Security Standards:

For more information see: <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

NERC Requirement	Requirements Addressed by SenSage
<p><b>Key Definitions</b></p>	<p><b>Critical Assets:</b> Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.</p> <p><b>Cyber Assets:</b> Those programmable electronic devices and communication networks including hardware, software, and data.</p> <p><b>Critical Cyber Assets:</b> Those Cyber Assets essential to the reliable operation of Critical Assets.</p> <p><b>Electronic Security Perimeter:</b> The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.</p>
<p><b>CIP-005-1 Electronic Security</b></p> <p>This standard requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.</p>	<p><b>R3. Monitoring Electronic Access Control</b> – The Responsible Entity shall implement and document the controls for <i>logging authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.</i></p> <p><b>R3.3.</b> At least every ninety calendar days, the Responsible Entity shall review access logs for unauthorized access or attempts.</p> <p><b>M3. Documentation of Controls</b> implemented to log and monitor access to the Electronic Security Perimeter(s), as well as <i>logs and business records</i> verifying that these controls have been implemented.</p> <p><b>M3.3</b> Business records documenting the <i>review of access logs to determine unauthorized access or attempts.</i></p> <p><b>1.3. Data Retention</b></p> <p><b>1.3.1</b> The Responsible Entity shall keep records (for example, <i>access logs, firewall logs, intrusion detection logs</i>) for a <i>minimum of ninety calendar days.</i></p> <p><b>1.3.2</b> The Responsible Entity shall keep other documents and records required by this standard from the <i>previous full calendar year.</i></p> <p><b>1.3.3</b> The compliance monitor shall <i>keep audit records for three years.</i></p>

SenSage, Inc. offers patented event data warehouse solutions that provide actionable results from massive amounts of log and event data. Hundreds of customers have deployed SenSage solutions to reduce security, fraud and compliance risks at a fraction of the cost of traditional data warehouses and log management solutions. Based in San Francisco, the company markets its solutions directly and through partners, including Cerner, EMC, HP, Hitachi Data Systems, McAfee, Tokyo Electron Device and many others. Visit [www.SenSage.com](http://www.SenSage.com) for more information.