

# Role Based Access Governance and FERC/NERC Compliance: A Pragmatic Approach

FEBRUARY 2009

*User access governance is a core component of much of the regulations within the energy and utility industry.*

## Executive Summary

With the passage and recent audit deadlines of FERC and NERC guidelines, regulatory compliance has become a major focus for energy and utilities corporations. IT Security and business unit stakeholders in particular, are challenged in a variety of ways. Compliance with the letter of the guideline can be a challenge for organizations without strong access governance processes and policies. Complicating matters, demonstrating compliance through an annual review and certification process can be even more complex and time consuming, which results in less time available for organizations to focus on core business activities. The net result is higher operational and regulatory risk exposure.

Energy and utility organizations that build FERC and NERC compliance into a set of automated processes for access governance will benefit by reducing access related business risks, lowering the overhead associated with demonstrating compliance, increasing operational efficiency while streamlining access delivery and change management.

## Background

Regulatory oversight and audit standards in the energy and utility space focus largely around reliability. Reliable service for consumers, who rely on power for daily life and even survival in extreme climates, is tantamount. Much of the current guidelines were written in response to high profile incidents, such as the 2003 Northeast Power Blackout and the event at Ohio's Davis-Besse nuclear power plant (also 2003), where safety systems were brought offline for nearly five and a half hours due to an IT access issue. Fortunately, the plant was offline for other reasons at the time, so disaster was averted. These types of events provide a sobering reminder for the need for proper access risk management.

The Davis-Besse incident was particularly interesting: though the culprit was the Slammer worm, it was largely an access governance issue that was responsible for the vulnerability. A contractor partner with inappropriate access to the corporate network acted as the entry point for the worm. The corporate network, which was not appropriately segregated from the safety systems allowed the worm access.

Access governance is a core component of much of the regulations within the energy and utility industry. Segregation of Duties (SoD) is a primary component to ensure that access is appropriate for a particular job function or role so that transmission information can't be leveraged to manipulate market pricing. As an example, a major utility in the mid-west violated regulatory SoD standards through inappropriate access to transmission data. Certain shared employees of the corporation's risk analysis group compiled forward electricity price forecasts using price data collected separately by the wholesale merchant and the affiliated power marketer. Audit staff found that by providing each group with access to the other group's price data, the shared risk analysis group acted as an improper conduit of market information.

The corporation's marketing team had direct and indirect access to transmission data through the Energy Management System on several occasions. Such access, while perhaps not malicious and seeming inappropriate, can represent a significant regulatory risk exposure for organizations with ad hoc access control and governance processes. To mitigate such exposure, organizations need to implement automated access governance procedures and controls.

*In 2010, organizations must be auditably compliant, meaning organizations must be able to produce all documentation for the previous twelve months to auditors.*

## Regulatory Oversight

FERC has also directed NERC to monitor the work that the National Institute of Standards and Technology (NIST) is doing on potentially complementary technical standards. As a result, the NERC CIP, while created initially by NERC, may be a work in progress, and requirements may evolve to incorporate NIST requirements in the future.

NERC's CIP has become a de facto cyber-security standard for virtually all energy and utility organizations in the North America. The CIP became required in 2006, with external auditing beginning in June of 2007. The CIP spells out a fairly prescriptive set of access controls to which energy and utilities firms must adhere. At a high level, to comply, organizations must:

- Create and maintain a security policy
- Identify and implement electronic access controls for access to critical assets, maintain documentation of the access controls, and update it at least annually
- Continuously monitor electronic access to critical assets
- Protect information associated with critical assets, plus policies and practices used to keep them secure

In addition, NERC requires a multi-faced and comprehensive compliance program, which involves:

- Periodic reporting
- Self-certification
- Exception reporting
- Investigations
- Random spot checking and audits
- Compliance audits (separate from Readiness Evaluations)
- Self reporting

The NERC CIP standard requires compliance with the full scope and intent of all requirements in the second quarter of 2009. Organizations must at that point begin to maintain documentation, logs and audit records that can demonstrate compliance. In addition, one year later in 2010, organizations must be auditably compliant, meaning organizations must be able to produce all documentation for the previous twelve months to auditors and external stakeholders on demand.

*Implementing a control framework for access governance will pay dividends both in terms of operational and compliance risk reduction as well as in a reduction of the operational overhead with compliance*

## Getting Compliant

For most organizations, becoming compliant with the CIP standard will actually be a smaller task than being able to demonstrate compliance. Nevertheless, it is the most critical step of the process. For the most part, the majority of CIP cyber security requirements are covered in other common control standards such as ISO 27001/2 (formerly 17799), COBIT, NIST or ITIL or in other regulatory obligations such as Sarbanes Oxley. Overlap between the standards is detailed below:

- **Create and maintain a security policy:** documented in CIP 003-R1 and also covered in ISO domains 5 and 11 and COBIT control objectives DS5 and ME4. Also implicitly required under SOX section 404.
- **Identify and implement electronic access** documented in CIP 004-R4 is covered in ISO domains 11 and 12, and COBIT control objectives DS 4 and 5 and also implicitly required under SOX section 404.
- **Continuously monitor electronic access to critical assets** documented in CIP 004-R4 is covered in ISO domains 11 and 12 and COBIT control objectives DS5 and ME2 and also implicitly required under SOX section 404.
- **Protect information associated with critical assets** is documented in CIP 002, and is covered in ISO domain 11 and COBIT control objective DS5.
- **Establish system management policies and procedures for configuring and securing critical assets** is documented in CIP 004 and CIP 007 and is covered in ISO domains 11 and 12 and COBIT control objectives DS5, DS9 and DS11.
- **Define and document electronic incident response actions** is documented in CIP 008 and is covered in ISO domain 13 and COBIT control objective DS8.

Entities who manage information security and regulatory compliance to the letter of these control frameworks certainly need to perform due diligence to account for subtleties present in the CIP standard, but the groundwork for the majority of requirements should exist in such entities.

An initial NERC CIP compliance program should start with a readiness assessment and gap analysis, followed by a mapping exercise to the existing control framework. Organizations with a comprehensive control framework in place will have a leg up on the process, but for other entities this can represent an opportunity to build such a framework. As we will discuss later in this paper, implementing such a control framework for access governance will pay dividends both in terms of operational and compliance risk reduction as well as in a reduction of the operational overhead required with ongoing compliance processes. Regulatory compliance management is an ongoing process, and should not be treated as a one-time project.

## Access Governance Requirements

To become compliant with specific CIP requirements, organizations require enterprise-wide visibility to user access. Under CIP requirements 004-1 R4 and 007-1 R5, a holistic view of all user access entitlements is required. To get a unified view of user access is almost impossible from most organizations without a centralized access governance framework in place, as they tend to manage access at the information resource level. Having such a framework in place provides a comprehensive view of enterprise access reality: i.e., understanding who has access to what at a fine grained entitlement level. Since most organizations manage access in an ad hoc and siloed manner, there is no easy way to aggregate user access data to get a consolidated view. And managing access at an application or technical level only provides a coarse grained view, which will not provide the visibility into specific user entitlements (to validate SoD requirements) which is required to instantiate effective controls.

*A strong access governance program should contain the ability to stop segregation of duties violations from being granted in the first place.*

Organizations are also required to perform regular access reviews under CIP 003-1 R5 and CIP 004-1 R4. For many entities, access reviews are performed in an ad hoc and manual fashion, and can be a painful and labor intensive process. Typically, this involves exporting user access data into spreadsheets. Controls are then applied in a manual fashion. The resultant data is quite error prone. Poor access change management can allow problems to fester and multiply. For instance, entitlement drag can occur when a person changes roles. Under a manual process, administrators will frequently grant new privileges and entitlements without removing old access. Under a manual approach to change management, this can be quite a prolific problem that is difficult to detect. Any analysis performed in such an ad hoc manner on suspect data by humans is subject to error. While such errors can be explained to and negotiated with auditors, such tasks take time away from day to day operations, and as such time is taken away from risk management and risk exposure suffers.

A manual, ad hoc approach to access certification typically stems from a “check the box” approach to compliance management; it reflects an effort to do the minimum to become compliant. Organizations pursue this approach typically because they are constantly under-resourced, and make certification and compliance less of a priority. A roles construct, while requiring an initial investment, will pay dividends down the line, both in terms of increased operational efficiency and reduced access-related risk. Using a role-based approach for access delivery or changing management provides preventative control points that can automatically head these problems off, making reviews far more accurate.

Formalizing an access risk management program is also a core requirement of the CIP standard, covered in requirements CIP 004-1 R4 and CIP 007-1 R5. Additionally, the FERC Standard of Conduct requires automated controls to ensure segregation of duties controls are enforced, for instance to ensure that the marketing department does not have access to risk analysis and price forecast data. Most organizations rely on manual, detective controls in this area, catching potential violations through periodic audit and review processes. Automated preventative controls are far superior, and a strong access governance program should contain the ability to stop segregation of duties violations from being granted in the first place.

*Every day that a control gap waits to be remedied costs organizations in terms of opportunity cost around staff utilization and increases risk exposure.*

This process is known as continuous role lifecycle management, and it reduces the administrative burden involved with access delivery and change management. As a result, fewer control violations go unnoticed, and access reviews and risk management efforts become much less labor intensive. Continuous Role Lifecycle Management provides a preventative point of control. When access requests – initial or change – are made, policies are checked through controls in real time.

Closed loop remediation is also a critical requirement, spelled out in CIP 004-1 R4. When control violations occur and access incidents materialize, the time to remediation must be minimized. For example, upon employee termination, the CIP mandates that access be terminated within a set time period depending on the nature of the termination. If the termination was involuntary and for cause, access must be revoked within 24 hours, otherwise it must be revoked within a week. And there are operational costs to be considered. Every day that a control gap waits to be remedied costs organizations in terms of opportunity cost around staff utilization and increases risk exposure. Additionally, closed loop remediation in an automated fashion gives executives, stakeholders and auditors assurance that issues have been remedied, and provides the audit trail (as a system of record) to prove it.

## Demonstrating Compliance

Being compliant is of little value to organizations if demonstrating evidence of compliance to auditors and regulators is difficult or impossible to produce. For entities with ad hoc and manual compliance processes in place, the costs are high.

“Rubber stamping” is a common occurrence in organizations with poor access governance. It occurs due to a language gap between business stakeholders who are required to certify compliance and IT Security who describe asset entitlements in technical terms which are then used for certification. Because entitlements are represented by the application, system and information resource, rather than by business process, it is difficult for a business stakeholder to understand access reality. User access data that is not in a context that the business can understand (for example, if it is expressed in cryptic security syntax) can lead to “rubber stamping” of compliance attestation reports. Not only do regulatory auditors look for this occurrence, it can lead to a serious regulatory fine or penalty.

In addition, compliance fatigue is a common problem for organizations. The average large organization is subjected to numerous regulatory disclosure mandates, and utilities are no exception. System administrators and business owners alike frequently complain about being required to respond to redundant and independent requests for access certification from numerous sources.

*Change management through continuous, dynamic access lifecycle management simplifies compliance.*

A roles-based approach to access governance can help scope reviews down considerably. For example, roles provide the opportunity to certify by role rather than individual. A department of 300 people might be represented by four or five roles. By certifying the role structure – entitlements that make up the role – a great deal of efficiency is gained. If no member of the role has entitlements outside of the role, and the entitlements within the role structure are in compliance, then everyone that is a member of the role automatically inherits the compliance. Additionally, role-based access governance can automate a set of processes for event driven reviews that requires a review of access only when it changes. Both steps are proactive measures that lead to significant reduction in overhead.

Business certifiers and external auditors need to make sense of siloed data from disparate sources in disparate formats. The data then needs to be collated, and the findings presented in a logical format. Manual generation of such reports can be a long and expensive process. Worse yet, a static audit report is out of date shortly after it's produced. Asking the business to do manual certifications in spreadsheets is inefficient, and asking external auditors to do the same is expensive.

An automated roles construct also introduces a preventative approach to managing operational and compliance risk. A manual, ad hoc approach is also by its nature reactive. Executives concerned about access risk exposure and concerned about their NERC compliance posture do not have access to such information ahead of an external audit. Internal audit groups can provide periodic updates, but the information is not dynamic, and becomes stale soon after the audit is performed. As a result, organizations are frequently unaware of their compliance posture and regulatory risk exposure. Change management through continuous, dynamic access lifecycle management simplifies compliance by introducing controls automation with a full audit trail, providing that proactive visibility that organizations require.

## ABOUT AVEKSA

Aveksa provides the only comprehensive, enterprise-class solution for access governance, risk management and compliance.

Aveksa automates the monitoring, reporting, certification and remediation of user entitlements and roles; enables role discovery and lifecycle management; and delivers unmatched visibility into the true state of user access rights. With Aveksa, business, security and compliance teams can effectively collaborate and enforce accountability.

Our growing customer base includes leading organizations in financial services, healthcare and manufacturing.

## Automation is the Solution

To meet the objective of being auditably compliant in a cost effective and streamlined fashion, organizations should invest in an automated access governance program, with regulatory compliance as a core component. The automated access governance framework should provide:

- Enterprise-wide visibility to user access aggregated and normalized to present a unified view and business friendly context
- A regular automated access reviews and certification processes
- Automated access risk management controls
- Continuous role lifecycle change management
- Closed-loop access rights remediation
- An auditable system of record
- Analytics metrics and reporting for access decision support

CIP 003-1 RS	CIP 004-1 R4	CIP 007-1 RS	FERC Standard of Conduct	Specific Regulatory Requirement	Access Governance Control Description
	X	X		Discover user entitlements across all information resources	Continuous enterprise-wide visibility to user access
X	X			Review & certification of user entitlements	Automated & regular reviews of user access
	X	X	X	Controls automation	Access risk management
		X		Privileged user governance	
X				Access delivery administration	Continuous role lifecycle management including automated preventive controls for SoD enforcement
	X			Access change management	
			X	Access policy management	
	X			Access rights risk remediation to critical systems	Closed-loop access remediation system
X	X			Up to date list of users & entitlements	Auditable system or record

Such a program should leverage the overlap between NERC CIP and other IT control frameworks and external regulations, reducing compliance fatigue, providing on demand access to access governance and compliance posture. This approach will ease both the initial setup of a NERC CIP compliance program as well as streamline the ongoing maintenance, reducing organizational costs and mitigating access risk exposure.

For additional information about Aveksa solutions visit us online at [www.Aveksa.com](http://www.Aveksa.com).



### Aveksa Inc.

265 Winter Street  
Waltham, MA 02451

[www.aveksa.com](http://www.aveksa.com)

© 2009 Aveksa Inc. All rights reserved. Aveksa and the Aveksa logo are registered trademarks of Aveksa Inc. All other company and product names may be the subject of intellectual property rights reserved by third parties. 02/09