Operational Integrity Enhancement
Energy Industry Analysis
**Operational Integrity Enhancement**

**Energy Industry Analysis**

Operational integrity in the energy industry is a broad and complex issue that includes key physical infrastructure components—such as power plants, oil rigs, power lines, and underground pipes—not just information and control systems. The complexity is amplified by the fact that some parts of the energy industry are highly regulated and subject to explicit regulatory requirements about all aspects of their business, while other parts are much less regulated and most of their regulatory requirements focus only on safety. Also, while some energy industry sectors are regulated nationally or globally, many others are regulated at the state or local level. For example, utility companies typically fall under the purview of state regulators and are often subject to detailed requirements about everything from maintenance, inspection, and reliability to how much they can charge and how much profit they can make. In contrast, oil pipelines are much less regulated, although some attention is given to safety and environmental impacts.

Because of this breadth and complexity, the industry's drive to improve operational integrity is scattered across countless rules and regulations that vary by sector and jurisdiction—and thus cannot be fully captured simply by describing a handful of key emerging regulations. However, generally speaking, it would be fair to say that the energy industry recognizes the importance of operational integrity and that various regulatory bodies in the industry are actively working to address the issue.

Regulatory requirements and guidance related operational integrity in energy generally fall into four major categories:

**Physical infrastructure**

Much of our nation's underlying energy infrastructure has exceeded its useful life and needs to be replaced. For example, in some places, the underground pipes that carry natural gas have deteriorated to a point where the gas is essentially traveling through tunnels of dirt—creating a significant risk of leaks and explosions. To address this issue, many regulators are responding by requiring utilities to implement long-term infrastructure replacement programs.

The business of a utility is to provide safe, reliable, and cost-effective service to customers, while also generating sufficient revenue to ensure a reasonable rate of return. Since the services being provided are "necessary," regulators (generally in the form of commissions) are designated at the state and federal levels to manage and protect these interests. "Keeping the lights on" or "keeping the gas and water flowing" is the number one objective, and capital investment in infrastructure is vital to meeting this objective.

While infrastructure planning and management has always been an area of scrutiny in any rate case or utility management audit, commissions have begun imposing more sophisticated financial and risk assessment requirements as part of the associated justifications in order to clear the approval processes. This is likely attributable to a few key factors: (a) aging infrastructure and the lack of sufficient longterm plans to address the rapidly increasing risk of major failures, particularly in gas and water infrastructure; (b) market conditions that have driven prices down, creating a "do more with less" environment; and (c) the transition of customers from deregulation, which froze rates and for many years insulated consumers from natural market driven rate increases that would have occurred in smaller increments.

The need to fix big-dollar problems in aging infrastructure—combined with an inability to generate sufficient revenue due to market conditions, as well as increased pressure on regulators to mitigate the "sticker shock" to consumers in deregulated territories—increases the burden of proof for utilities when proposing rate recovery for day-to-day and long-term operations. All of this leads to numerous levels and forms of risk in both operations and financial planning. The increased burden of proof is being enforced in a variety of ways, including: more specific regulation; the use of more sophisticated analysis tools and resources by commissions in rate cases; government initiatives with a focus on infrastructure management; and imposition of "recommendations" (guidance that is labeled as voluntary but in reality is mandatory).

All utilities are vulnerable to change. However, some types of utilities are more likely to be targets for change. For example, the gas utility sector is likely the highest priority for regulators looking to drive widespread infrastructure improvement because reliability failures in the sector pose the greatest safety risks. Other sectors may be vulnerable to more targeted enforcement of regulatory change. This includes, for example, utilities that for a variety of reasons—relationships, bad actor reputation, poor filings—have historically not been very successful in rate recovery or other regulatory proceedings.
Cybersecurity

The energy sector is seeing a rise in cyber threats—particularly against critical infrastructure—and regulators are working hard to increase and improve cybersecurity and compliance controls to address those threats. Publicized threats, such as Dragonfly and Black Energy, target industrial control systems (ICS) and other energy assets, while quieter threats and the expanded use of cyber assets in day-to-day operations add to the need to transform cybersecurity programs.

Complicating all of this is the use of different frameworks (i.e., Critical Infrastructure Protection (CIP), NIST) by many entities, as well as inconsistent implementation of processes and controls depending on the nature of the assets to be protected. Finally, lack of focus on assurance activities to verify the proper execution and effectiveness of existing controls—and to identify areas for improvement or remediation—increases the risk of a major failure.

As the Smart Grid grows and evolves and energy companies increase their use of ICS, there will likely be a mounting need to protect those systems from abuse. Headlines and perceived major failures, risks, and threats will drive increased legislative focus. This will likely spur support from regulators for the development and implementation of rules that allow for better monitoring, tracking, and enforcement of specific cybersecurity controls and compliance obligations similar to the NERC CIP requirements.

Recent versions of NERC’s CIP framework expanded the scope of cyber assets that power and utility companies must monitor—an increase for some utilities of more than 1,000 percent. The effect of these changes applies unevenly. For example, a challenge for small and mid-sized companies is that the expected vigilance and compliance infrastructure of the expanded CIP regulations is not scalable. They face the need to implement the same changes as larger companies, but with smaller budgets and staffs. Larger companies, however, may face significant expansion of the number of assets requiring protection and the challenge of managing compliance programs and resources that are spread across a much larger organization (or even separate entities). This could trigger other regulatory concerns, such as cost allocation regulations for shared assets and services.

Additional complexity exists for entities that are regulated for some cyber assets and not for others. Many organizations think they already have robust processes and are in compliance. But assessments of controls for unregulated assets often reveal that the controls are not being implemented as intended. Utilization of different processes, controls, and frameworks while leveraging the same resources, assets, and controls can create confusion and cause many of the gaps or implementation failures.

Cybersecurity efforts in energy are focusing on non-ICS cyber assets as well. The CFTC recently approved the NFA’s cybersecurity guidance that will require members to adopt—and enforce—policies and procedures to secure customer data and protect their electronic systems. The CFTC is also considering some proposals to ensure that the major exchanges, clearinghouses, and swap data repositories are doing adequate evaluation and testing of their own cybersecurity and operational risk protections.
Operational integrity related to energy trading

Regulatory scrutiny and guidance related to energy trading have increased significantly in the wake of the financial downturn and other headline-grabbing problems. This is an area where specific regulations have been introduced, and where enforcement actions are increasingly common. Here are some of the key focus areas and trends:

• Regulation automated trading (Reg AT). This regulation includes a series of risk controls, transparency measures, and other safeguards to improve transparency and reduce the potential risks associated with automated trading on DCMS. Reg AT requires the implementation of risk controls—such as maximum order message and maximum order size parameters—as well as the establishment of standards for the development, testing, and monitoring of algorithmic trading systems. It also requires high volume traders that use algorithmic trading for key futures products to register with the CFTC. Other requirements include the use of self-trade prevention tools by market participants on DCMS, and the disclosure of rules and attributes of DCM electronic trade matching platforms that materially affect factors such as: the time, price, or quantity of execution of market participant orders; the ability to cancel or modify orders; and the transmission of market data and order or trade confirmations to market participants.²

• Counter-party credit assessment. The supply chain for energy involves numerous steps and numerous counterparties. Real-time credit assessment and scoring enables traders to assess the financial viability of counterparties before deciding to execute a trade.

• Swap data repositories. Tracking swap transactions and resolving problems before the transactions are reported to regulators.

• Price data reporting. Updating FERC’s price data reporting guidelines (which were originally issued in 2003/2004) to capitalize on the latest technologies.

• Real-time trade surveillance. Increased scrutiny from regulators and the market emergence of new surveillance platforms are getting the attention of corporate boards. In response, many companies are considering focusing more resources on trade surveillance and monitoring and on the creation of comprehensive compliance policies that include financial and physical trade surveillance. Firms have traditionally monitored trades at the end of each day, looking for prohibited activities—often using basic tools such as spreadsheets. Now leading firms are moving to real-time monitoring that looks at trades as they are being entered and executed. This helps internal compliance groups proactively identify and investigate problems before regulators initiate an action or inquiry.

Because some of these areas of increased regulatory focus are not strictly mandated by the government (for example, some industry groups such as Deloitte’s Risk Council, are developing leading practices to help address surveillance responsibilities), companies should consider putting in an effort to seek senior management support to obtain budget and/or resources to address them.

Quantitative risk management for major projects

In the oil and gas sector, Deloitte is working on a five-year project to help the Bureau of Safety and Environmental Enforcement (BSEE) develop and adopt a probability-based approach to risk management. The idea is to shift the focus from subjective/quantitative risk factors to objective/quantitative risk factors (i.e., setting standards based on probability percentages—for example, requiring a project to achieve expected reliability of 99.9 percent based on quantitative probability estimates).

The emphasis is on identifying and addressing operational risks early (i.e., in the planning and design phase), rather than reacting to problems after the fact. Risks that are not identified and addressed early can lead to problems that are extremely expensive to resolve—and that potentially threaten the ultimate success of the project. This is especially relevant in the oil and gas sector, where projects can cost tens of billions of dollars—and where problems can have catastrophic impacts on the environment. Also, this issue is especially relevant today because (1) in the past, high oil prices made it easy to throw money at problems, but now that oil prices are low companies cannot afford expensive snafus and (2) numerous headline-grabbing environmental disasters have put the industry under the microscope from regulators, the public, and the media. For example, oil spills have increased the pressure for tighter regulations on operational reliability and safety and for a better methodology to manage risk and reduce the probability of accidents.
Contacts
Mike Prokop
Managing Director
Deloitte Advisory
Deloitte & Touche LLP
Mprokop@deloitte.com

Endnotes
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

© 2016 Deloitte Development LLC. All rights reserved.