

WHITE PAPER:

LEVERAGE THE BENEFITS OF A CULTURE OF COMPLIANCE

To comply is to follow the rules or regulations. It's that simple and that complicated.

In today's difficult and challenging regulatory and business environment, compliance should represent more than a federal or state requirement. It should be harnessed as a business tool to foster more efficient operations that save time, money, and headaches.

When it comes to understanding and meeting Federal Energy Regulatory Commission (FERC) and NERC requirements, the energy and utility industry faces some unique challenges. Luckily, when it comes to creating a Culture of Compliance, this industry can learn quite a bit by looking at how other industries such as life sciences, manufacturing and finance have addressed similar challenges.

In this brief paper, we'll attempt to provide an overview of the most important challenges, the requirements and benefits of meeting them, and some ideas on how to make compliance easier.

Creating and maintaining a Culture of Compliance is not always easy, but it can be done with the right mix of strategy, strong leadership, programs and tools, and personnel training. This is critical to the success of today's energy and utility companies. At stake are huge fines, civil penalties, terrible publicity, and even threat to life if the power grid is interrupted for an extended period of time.

What is a Culture of Compliance?

The Culture of Compliance is by no means a new concept. However, the rationale behind it and the best approach for attaining a strong compliance culture have evolved over the last several years. In part that's because of experiences in the financial industry and elsewhere which too often demonstrated that a so-called Culture of Compliance designed only with regulations in mind was not a true Culture of Compliance.

"You know it's not enough to have Culture of Compliance policies," the SEC's then-Director, Office of Compliance Inspections and Examinations told an industry conference in 2003 in the wake of some turbulent times and corporate scandals. "It's not enough to have procedures. It's not enough to have good intentions. All of these can help. But to be successful, compliance must be an embedded part of your firm's culture."

The SEC outlined what it believes are the five key elements to a Culture of Compliance. With minor adaptation, those same elements can be applied to the energy and utility industry, and indeed most industries.

An effective Culture of Compliance should include:

A strategic vision: Compliance activities cannot simply be reactive or to 'stay out of trouble.' They must be related to some larger strategic goal.

Identification: Specific risks that could occur within each strategic area should be identified.

Controls: Control points for each of those specific risks should be established.

Documentation: Detailing provides transparency, both internally for senior management, and externally to auditors and other regulators as appropriate.

Accountability: It must include clear responsibilities and assignments of specific tasks and goals to named personnel.

“You can have the best policies and procedures in the world, but if no one is making them work, they will be useless,” the SEC’s Lori Richards noted.

Regulation on the Rise

The FERC and the Electric Reliability Organizations (ERO) have ramped up their inspection and enforcement efforts in recent years. As these regulators mature in their experience and share their lessons learned, the regulatory environment will increase in scrutiny.

According to FERC’s revised policy statement on penalty guidelines issued September 2010, “To have an effective compliance program...an organization shall: exercise due diligence to prevent and detect violations; and otherwise promote an organization culture that encourages a commitment to compliance with the law.”

Some utilities have already harnessed a Culture of Compliance to reduce risk and increase efficiency. These “early adopters” are prime case studies for the importance of achieving true compliance.

The Right Solution

Given the importance of a Culture of Compliance, it is also critically important to identify the areas where your organization may need to work with outside partners and/or software systems.

When considering such a partnership, make certain you consider how they can assist you in the following areas:

RELIABILITY NERC/FERC STANDARDS COMPLIANCE

Companies and their compliance organizations will need assistance tracking and assessing programs and procedures to maintain reliability and meet or exceed the ever-evolving tough NERC/ FERC standards and requirements. Insist on tools that display key business and compliance metrics for at-a-glance assessments of compliance programs. Those tools must also assist in performing gap-analysis of requirements for all functional requirements, self-reporting, standard balloting and documented evidence. Make certain they are easily configurable to comply with codes of conduct, changes in the organization or compliance landscape.

COMPLIANCE MAINTENANCE AND RECORD KEEPING

Any system should keep accurate records detailing compliance programs, ensure due dates are met and subject matter expert (SME) reviews are documented and stored, track program effectiveness and identify and remedy any compliance gaps. It should also allow for easy assignment of specific tasks (i.e., reviews, mitigation plans, etc.) to functional SMEs.

SELF CERTIFICATION MANAGEMENT / SELF-REPORTING

Automate all ERO and regional self-certification requirements for registered entities. Systems should schedule and manage single or multiple requirements, entities or regions across any desired reporting schedule and automatically assign and measure activities for compliance to keep track of certification reviews and regional filings for each standard/requirement. Companies should be able to monitor and see status details instantly with graphical management dashboards (live data).

A strong Culture of Compliance program must be able to self identify and issue internal reviews and investigations (root causes) that will be reviewed by senior management. An internal Corrective Action program with appropriate mitigation plans should be assigned to an accountable individual with due dates that can be addressed quickly. Individuals need to meet their deadlines and management must support these individuals with the resources and material they need.

BENCHMARKING AND LESSONS LEARNED

The nuclear industry has been benchmarking and sharing lessons learned for many years. These have improved run cycles of plants, shortened outage and maintenance times, and improved relationships with the regulator. Utilities required to implement electric reliability standards now understand that this is an important part of compliance and improving overall performance and many industry groups are now sharing these lessons learned. The proper tools and programs can improve a company's regulatory compliance programs. Benchmarking other companies that have a strong compliance program, or attending ERO or industry workshops are excellent places to discuss best practices.

SENIOR MANAGEMENT SUPPORT AND LEADERSHIP

Having senior management support for implementing a strong Culture of Compliance cannot be stressed enough in today's environment. Most programs fail to be properly implemented without the leadership and support of management. Companies with a strong Culture of Compliance have periodic management reviews and metrics in place to discuss new requirements, ensure internal mitigation plans are being addressed, as well as the proper resources to prepare for self-certification, reporting, spot-checks and audits. Management should also ensure that periodic self-assessments of the compliance program are performed and reviewed. The ERO assesses management support when they are reviewing potential violations and going through the enforcement process.

BES CYBER SECURITY MANAGEMENT

To stay on top of compliance with CIP cyber system security and reviews requirements, programs should map and track BES cyber systems, components, and matrix information for determining impact ratings. They should offer support for meeting the 36-month review requirements and provide detailed status of all activities and deadline alerts at-a-glance.

DOCUMENT MANAGEMENT/RECORD MANAGEMENT

Creating a central repository where key documents are revised, published, and archived is an essential part of a well run compliance program. Access should be controlled so that only those personnel who are allowed to view a given document can do so. Any system should be able to categorize CIP SCADA requirements and documents, and create and archive task and compliance checklists. Policies and procedures must also address compliance requirements within the organization. Any strategy must also maintain evidence that RSAWs (Reliability Standard Audit Worksheets) for audits have been successfully completed and be built on a foundation of excellent program tools.

A strong document management program includes:

- Identified subject matter experts (SMEs) for specific programs
- Detailed review and approval process
- Periodic document reviews (recommended once or twice a year)
- A responsive revision process so needed changes can be made quickly
- An internal organization review and approval chart
- Electronic routing and review process with electronic signatures and record retention
- Proper backup and retrieval programs for easy access to records. (This is essential for responding to regulators' spot checks, audits, and enforcement request.)

CHANGE MANAGEMENT

Managing the process of implementing and documenting changes in physical assets or processes is critical to maintaining compliance. Any Change Management system should be integrated with other compliance related systems and should control who has access to an organization's documents; address access to all physical, electronic and other critical assets; establish a central repository to keep strong controls on any change or revisions; and establish and monitor recurring training needs, reviews and sunset dates for regulations and other requirements. It should also help request, review, evaluate and manage approvals, categorize requirements, and create, require and archive checklists.

CORRECTIVE ACTION

The importance of a strong internal corrective action program cannot be overstated. Bluntly put, if you fail here, you most likely will fail in your compliance program.

Corrective Action systems should use Key Performance Indicator (KPI) dashboard metrics to see, at-a-glance, what current or potential compliance or operational issues may exist. It should provide for alerts that instantly notify the proper personnel when a current or potential problem is identified, have internal controls that assign corrective action tasks to specific personnel with deadlines, and automate follow-up reports directly to supervisors.

DASHBOARDS, KPIS & METRICS

Built-in analytics/reporting capabilities and graphical dashboards should automatically provide the company's leadership a detailed real-time view into all compliance activities, to make global oversight simple. This live data should not require internal resources to update.

NERC STANDARDS UPDATE SERVICE

A good compliance system should also provide an efficient means to stay current with the constantly changing NERC standards and requirements. Look for a service which monitors NERC for new or revised standards regularly, then parses the information, including PDFs and RSAWs, into user-ready forms so systems can be brought up to date very quickly. It should also provide regular e-notification and the ability automatically update/import everything needed to keep current.

Conclusion

In today's tough regulatory and economic climate, instilling a strong Culture of Compliance throughout an organization is more important than ever.

Success depends on identifying the right compliance issues, having strong management support, developing the right strategy, vetting and implementing the right tools and outside resources, and instilling a full compliance culture from the beginning to the end of all practices and procedures. Finally, this must all be fully and clearly documented and readily available to the subject matter experts and the compliance organization

Leveraging the benefits of a Culture of Compliance is not difficult if you have the proper program and support in place. It provides a competitive advantage in a very competitive environment.

To find out how AssurX can help with your compliance needs, please call 1-888-9-ASSURX.