

Morgan Lewis

 **ERNST & YOUNG**
Quality In Everything We Do

webcast

Don't make the same mistake twice!
Avoiding repeat violations of Reliability Standards

17 November 2010

www.morganlewis.com

www.ey.com

Welcome to

Don't Make the Same Mistake Twice!

Avoiding Repeat Violations of Reliability Standards

- The audio will remain quiet until we begin. We will give periodic stand-by's until we are ready to begin at 1:00 p.m. (ET).
 - Audio is available via **Audio Broadcast**; you will hear the audio through your computer speakers. Please do **NOT** close the Audio Broadcast window.
 - **Make sure your speakers are ON and UNMUTED**
 - **Make sure your volume is turned up for the event**
- **ONLY** for attendees that are not able to hear audio through their computer speakers, you may join the teleconference. To do this, please:
 - Close the Audio Broadcast window.
 - Click on the REQUEST button on the Participants panel on the right-side of your screen to retrieve dial-in information.
 - Tech Support: If you are experiencing issues with your audio broadcasting, please call 866-779-3239.

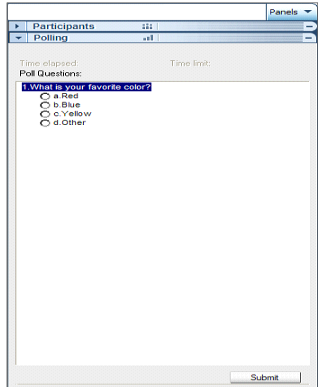
This event is listen only. Please use the Q&A tab to communicate with the presenters.

Responding to Polls

- During the Webcast will be asking *four* polling questions. For those interested in CPE credit, it will be necessary to answer the polling questions when they are asked.
- The polling panel appears on the right side, near the Q&A panel. Be sure to answer each question as it is asked.

Responding to polls

- ? Polling panel appears to the right of the slide area.
- ? Make your selection.
- ? Click **Submit**.
- ? If you are unable to complete a poll due to technology issues, send a Q & A message immediately.



Page 1

ERNST & YOUNG
Quality In Everything We Do

Reasons to avoid the repeat violation

- **Ongoing monitoring will assist in identifying and preventing violations of reliability standards.**
 - A compliance monitoring program can be adapted on an ongoing basis to identify potential violations so that the program can be used in the future to prevent repeat violations.
 - A thorough monitoring program can mitigate violation-related penalties.
- **FERC has directed Regional Entities and NERC to specifically consider repeat violations**
 - On August 27, 2010, FERC issued a Guidance Order discussing the role that repeat violations play in penalty assessments.
 - FERC considers repeat violations to be aggravating factors when assessing penalties.

FERC's guidance order

- **FERC addressed a Notice of Penalty filed by ReliabilityFirst.**
 - The Notice assessed a penalty for noncompliance with PRC-005 R2.
 - The Registered Entity was previously found noncompliant with the same requirement of the same standard only one year prior.
 - ReliabilityFirst failed to clearly explain why it did not deem the repeat violation to be an aggregating factor in assessing a penalty.

What are repeat violations?

- **The Commission considers a repeat violation to be:**
 - Repeated or continuing examples of conduct similar to that underlying the prior violation of the same or a closely-related Reliability Standard Requirement;
 - Conduct addressed in a registered entity's previously submitted mitigation plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or
 - Multiple violations of the same Standard and Requirement.

Considering repeat violations

- **The Commission now requires all Notices of Penalty to:**
 - Provide adequate information about all prior violations by a Registered Entity and by explaining how NERC and the Regional Entities assessed those prior violations in their penalty determinations.
- **Regional Entities and NERC still possess discretion to determine whether a repeat violation should aggregate a penalty assessment.**

Impact of FERC's guidance order

- FERC's guidance demonstrates that repeat violations will be closely considered by Regional Entities and NERC in future compliance proceedings.
- Entities subject to reliability standards must take steps to prevent against the occurrence of repeat violations.
 - A thorough and strong compliance enforcement monitoring program can provide such a service.

Avoiding the repeat violation

Four keys to avoiding the repeat violation

- The quality and performance of the compliance program in place
- The policies, processes and procedures for dealing with noncompliances
- The risk management program and how repeat issues factor into the risk mitigation plans
- How the monitoring options are designed, applied and funded

Compliance program leading practices that mitigate the risk of repeat violations

Most power and utility companies now have a compliance program with a framework and standards. The issue is the effectiveness and sustainability of the program – keeping the program current and vital. Representative compliance program practices that mitigate repeat violation risk include:

- Enterprise-wide standard compliance practices
- Embedded culture of ethics and compliance: tone at the top rolls through organization
- Comprehensive requirements inventory and robust maintenance process
- Comprehensive compliance risk assessment integrated with ERM
- User friendly and understandable tools for employees
- Processes mapped and documented, including mitigation processes
- Procedures identified and documented, including investigation procedures
- Usable metrics
- Targeted training
- Surveillance and audit processes
- Use of a maturity model, with emphasis on continuous improvement

Compliance program leading practices that mitigate the risk of repeat violations (cont.)

For each of the leading practices, certain sub-practices will further mitigate the risk of repeat violations. For example:

- Comprehensive requirements inventory and robust maintenance process

Leading sub-practices:

- Requirements are broken down into functional areas with process maps to help identify closely related requirements and all affected functions
- Requirements owners have input to and approve controls
- Requirements owners periodically certify operation of controls
- Standardized controls are applied across requirements to the extent possible to improve quality, consistency and project management
- Controls written to provide direction on how to manage and monitor compliance with the requirement

Compliance policies for responding to violations can reduce repeat violation risk

Leading companies reduce repeat violation risk with defined policies for responding to violations.

Key elements include:

- What is the protocol for escalating the reporting and review of noncompliances?
- How are remediation plans developed?
- How are remediation plans incorporated into current policies and procedures?
- What are the policies concerning when and how root cause and lessons learned analyses are performed?
- What are the policies for communicating root cause and lessons learned findings?

Risk assessment drives the remediation, mitigation and monitoring programs

The risk assessment drives the sustained response to noncompliances.

- Use of a risk based triage approach — the risk assessment drives the resources committed to the compliance program and program elements based on the likelihood and impact of compliance violations.
- The FERC's attention to repeat violations essentially increases the impact of repeat compliance violations.
- Some leading companies use supplemental questionnaires that highlight changes in compliance activity (including noncompliances, changes in enforcement, changes in regulations, changes in internal organization, etc.) to focus the risk assessment.

Monitoring options and considerations

- Depending on the risk assessment, monitoring options can include:
 - Monitoring and control within the function through work practices
 - Self assessments by the compliance area organization
 - Certification of the operation of the controls by the requirements owner
 - Internal audit department
 - External assessment
- At this point in time, many power and utility companies struggle with who and how to do a NERC readiness assessment.

Monitoring options and considerations (cont.)

- Additional key monitoring considerations include:
 - What information to measure
 - The repository for information collected
 - The documentation maintained
 - The reporting and communicating for management oversight and executive visibility and direction
 - Inherently the most significant factor influencing the likelihood of repeat violations is the quality and performance of the compliance program in place
- Measurement and monitoring can be periodic, real time documentation, and/or continuous controls. But in every case, for long term sustainability people need IT/system enabled tools to be compliant in a way that is both timely and not overly burdensome.

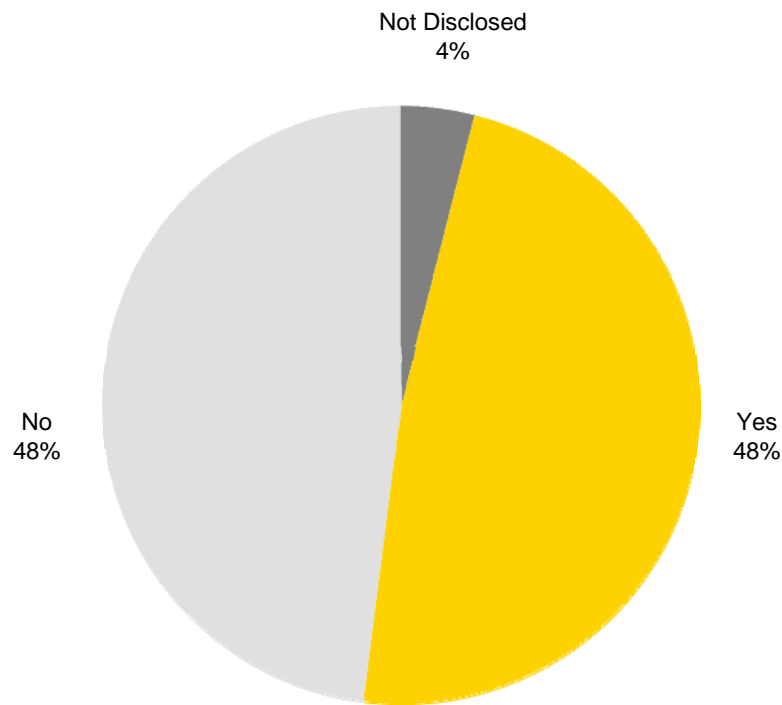
Field observations

Following are field observations from:

- Survey results
- Case study

Does your company have a continuous control monitoring program? Who is responsible?

Use of continuous control monitoring program



(n=25)

Who is responsible?

IT Audit Director

SOX Director /Internal Control Director

SOX Manager

SOX PMO

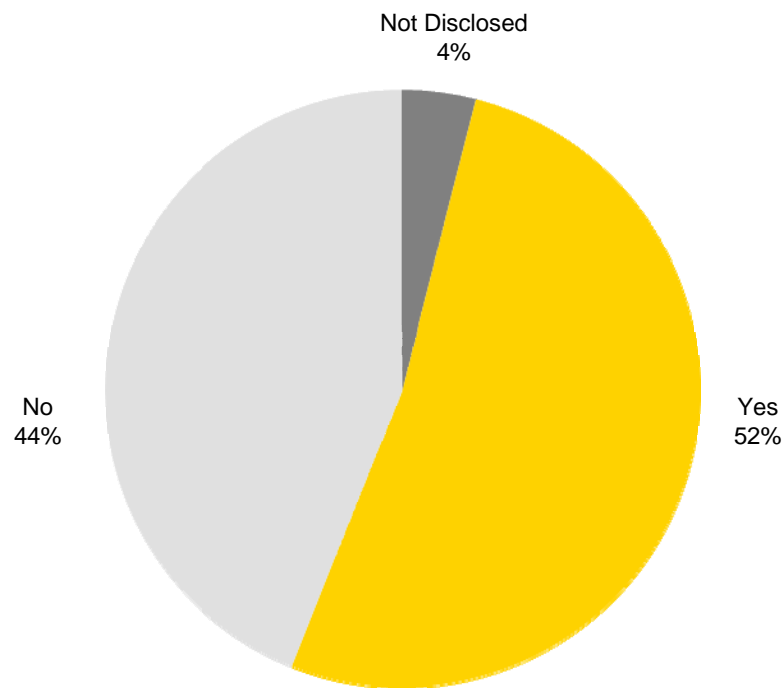
SOX Coordinators in Business Units and Shared Services Areas

Audit Services Director

Director, Compliance & Special Projects

Does your company require selected controls owners to provide real-time documentation related to the performance of the control?

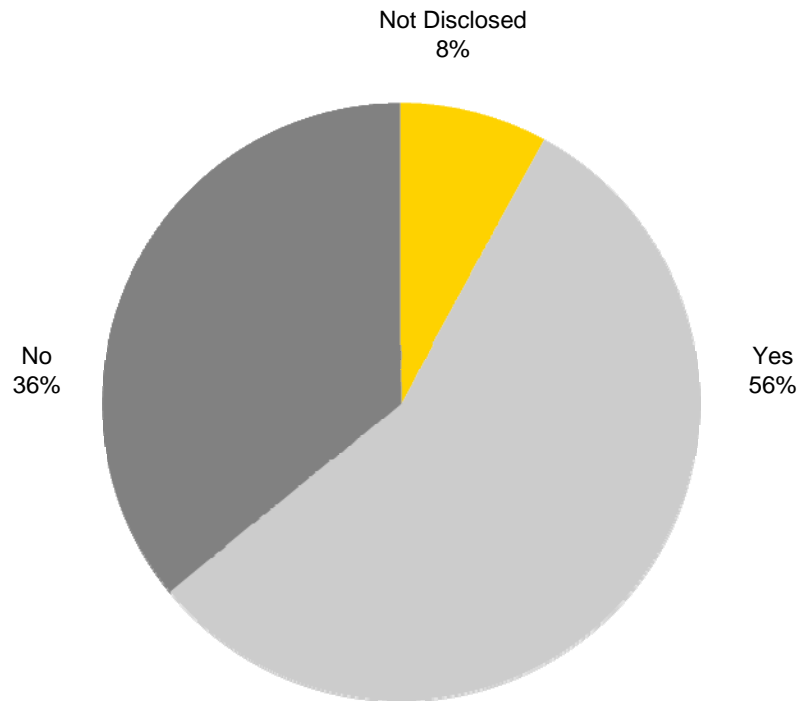
Use of real-time documentation of control performance



(n=25)

Does your company have an enterprise risk management (ERM) program?

Existence of ERM program



(n=25)

50% of respondents that affirmed having an ERM program said that the CRO – either stand alone title or in combination with another title – was responsible for the program

Other respondents note the following titles:

Director, ERM

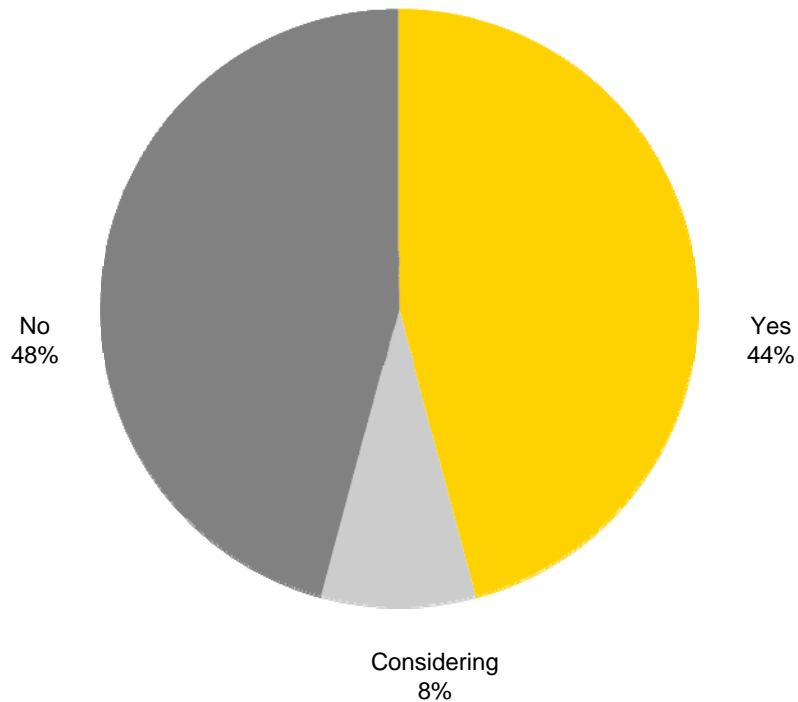
EVP, Risk

Director, Internal Audit

Director of Strategy & Communications

Does your company use a governance, risk, and compliance (GRC) tool?

Use of GRC tool



What GRC tool is your company using?

- Metric Stream
- SAP's GRC product
- TrinTech
- Oracle GRC
- AssurEx
- Combination of OpenPages FCM, Enviance, environmental and NERC databases

What GRC tool is your company considering?

- Oracle
- Archer
- Movaris
- SAP

Case study – how to better respond to NERC (and mitigate the risk of repeat violations)

Concerns

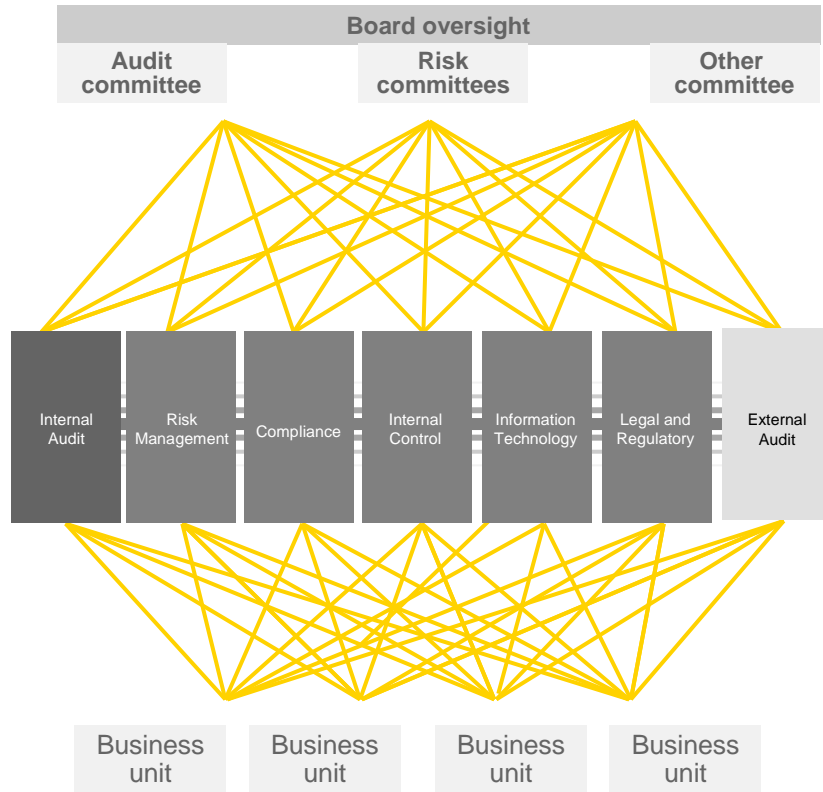
- Ability to respond completely and timely to audit was in question
- Management had no way of knowing controls were in place and operating
- Various levels of documentation of compliance existed

Future state

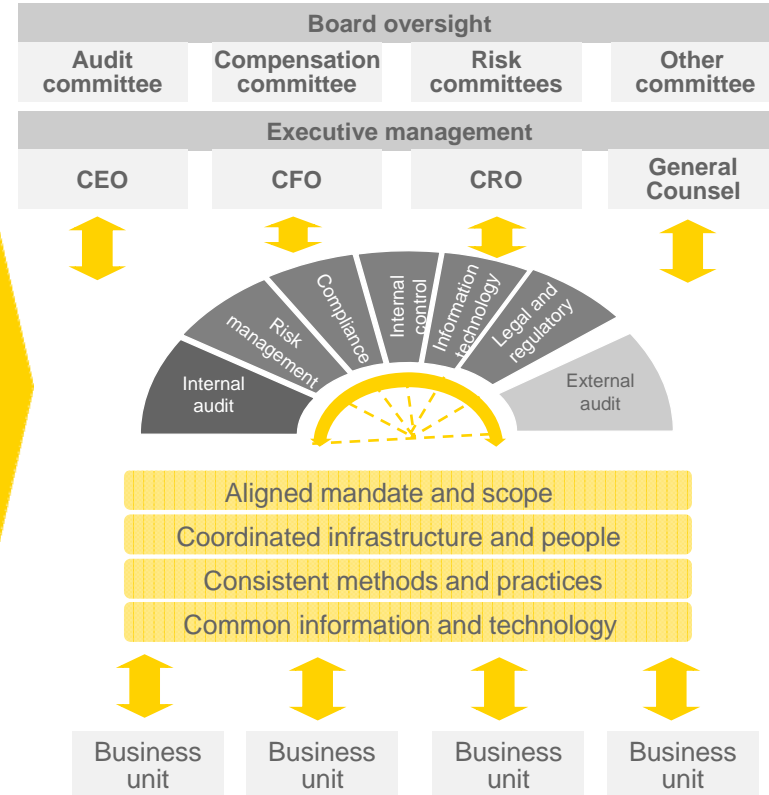
- Provide mechanism to give management a view into state of compliance
- Provide central repository for documentation of requirements, controls and monitoring
- Establish a process to report to regulators in a timely, accurate, and complete fashion, with adequate coordination and review across the Company

Future state – a transformation

Current state



Future state



Risk transformation

Siloed risk functions reduce value, increase costs and impact business performance

Compliance program activities

Compliance program governance

- *Develop the compliance strategy and framework*
- *Provide executive management with a mechanism to feel comfortable with the state of compliance throughout the organization*
- *Provide effective communication about changes in compliance obligations for managers and employees with compliance responsibilities.*
- *Educate management and employees regarding the implications of a changing regulatory environment and how to respond to it.*

Compliance/ Tactical and operational controls

- *Identify and document current and new compliance requirements*
- *Create and document controls across all requirements with input/signoff from the organizational owner of the requirement*
- *Create supporting policies and procedures (including specific policies on dealing with noncompliances)*
- *Create measurement and monitoring framework*
- *Review controls for legal implications to the Company*

Risk management

- *Assess the risk profile in an integrated fashion and provide a risk based approach to compliance activity based on a maturity model*
- *Provide a common set of systems for integrating and managing the variety of compliance programs*
- *Reduce the complexity and cost of managing compliance across a multi-regulatory environment and improve the consistency in polices, controls and reporting requirements*
- *Prioritize and optimize the labor needed to collect and access individual compliance programs*

Monitoring processes

- *Identify all parts of Company or Business unit(s) impacts by a particular compliance requirement and share a common understanding of the applicable interpretation*
- *Provide direction on how to manage and monitor the controls*
- *Develop functional requirements for a compliance management system (GRC)*
- *Design and implement the compliance management system*
- *Provide IT enabled monitoring tools*
- *Provide reasonable assurance of timely, accurate and complete external reporting with adequate coordination and review across the Company or business unit(s)*

Effect of a Compliance Program

- **The Compliance Program, Risk Management Program, and Monitoring options described herein directly address FERC's concerns regarding effective internal compliance initiatives.**
 - In October 2008, FERC provided guidance to industry participants with regard to effective compliance with FERC's governing statutes, regulations and orders.
 - In its Policy Statement on Compliance, FERC identified several factors that it considers when determining whether an industry participant maintains and employs an effective and robust compliance program.
 - The factors that FERC considers, among others, include:
 - Actions of senior management;
 - Effective prevention measures; and
 - Prompt detection, cessation, and reporting

Effect of a Compliance Program (con't.)

- **Actions of senior management**
 - FERC considers senior management to be directly responsible to ensuring that a culture of compliance exists within a company.
 - Senior management should devote sufficient time and resources to ensuring compliance.
 - Senior management should encourage company personnel to raise and/or identify compliance issues within a company.
 - Senior management should ensure that compliance officials within a company are part of a “dotted line” reporting structure that enables the personnel to report directly to a company’s Board of Directors or committee of the Board.
 - A thorough assessment of a company’s existing compliance program and the personnel responsible for the program, as described today, ensures that FERC’s concern regarding the role of senior management is addressed.

Effect of a Compliance Program (con't.)

- **Effective prevention measures**
 - This factor includes careful hiring, training, accountability, and supervision.
 - Effective prevention also includes periodic review and evaluation regarding the effectiveness of a compliance program
- **A variety of monitoring options and procedure assessments can ensure that a company's internal compliance program is robust, effective, and responsive to newly identified compliance issues.**

Effect of a Compliance Program (con't.)

- **Prompt detection, cessation, and reporting of the offense**
 - FERC acknowledges that prompt detection may result from a high quality and comprehensive internal monitoring system.
 - In considering potential penalties for noncompliance, FERC also supports providing substantial credit for violations discovered as a result of systematic internal auditing and supervision programs.
 - A company's behavior following the identification of a violation is also indicative of the degree to which the company maintains a strong culture of compliance.
 - Immediate cessation of the behavior giving rise to noncompliance and self-reporting an identified violation is indicative of a culture of compliance within a company.

Questions?

- **Contact information for speakers:**
 - [Morgan, Lewis & Bockius LLP](#)
 - Floyd L. Norton IV – fnorton@morganlewis.com
 - Stephen M. Spina – sspina@morganlewis.com
 - [Ernst & Young LLP](#)
 - Michael Marsico – michael.marsico@ey.com
 - Kenneth Novak – kenneth.novak@ey.com
- **New York CLE – C1290.61**