



March 31, 2005

Jonathan G. Katz  
Secretary  
Securities and Exchange Commission  
Via email to: [rule-comments@sec.gov](mailto:rule-comments@sec.gov)  
RE: File No. 4-497

Dear Mr. Katz:

The Committee of Chief Risk Officers (CCRO) commends the Securities and Exchange Commission, Chairman William H. Donaldson and his staff, for recognizing the need for continuing evaluation of the Sarbanes-Oxley Act of 2002. I would like to take this opportunity to formally submit my comments for consideration at the roundtable on the Implementation of Sarbanes-Oxley Internal Control Provision on April 13, 2005.

The CCRO is a not-for-profit professional organization of over 30 representative energy and related companies, including major integrated oil companies, integrated electric and gas utilities, smaller power and gas marketers, and others. The CCRO is an independent, cross-industry group where member companies can identify and document best practices for measuring, managing and reporting the financial risks inherent in both regulated and unregulated for the benefit of the industry. You can see the current listing of our members on our web site at [www.ccro.org](http://www.ccro.org).

The CCRO has invested substantial time and resources working on the issue of governance of and compliance with Sarbanes-Oxley. In late 2002, we produced a 52-page white paper on "Best Practices for Governance and Controls" outlining the guidance on the control infrastructure for two primary areas: the business processes and the governance of them. The CCRO has a follow-up and updated white paper nearing public release.

While industry today is far from reaching a consensus on any single, integrated solution, CCRO members and many parties outside the CCRO concur that the governance and compliance environment within a company has significantly shifted in the past year. In light of the evolution of the issues surrounding Sarbanes-Oxley governance and compliance, the CCRO is drafting a comprehensive best practices guide that addresses the effects and structure of these issues within the energy industry.

## **Background**

The natural gas and electricity markets are characterized by market price fluctuations, financially unstable counterparties, doubtful regulatory cost recovery and detrimental rulemaking all of which create pressing disclosure considerations. Along with these complexities and risks comes a myriad of control problems rivaling those of large financial institutions.

Magnifying the effects of these risks are typical aspects of day-to-day (often minute-to-minute) operations in the energy industry. Common events and decisions may have much wider

consequences. For example, plant outage has proven, in many cases, to have massive financial impact on an organization while day-to-day operational volatility extends to the weather and economic-driven variability of load. Over the past few years, companies in the energy industry have spent considerable time and resources upgrading their control and reporting environment in order to adhere to the Sarbanes-Oxley Act. This experience has yielded many insights that may be of value for those companies new to the energy industry and/or just getting started in the Sarbanes-Oxley process.

Under Sarbanes-Oxley, all material event disclosures must be exceptionally rapid, thorough and accurate. The structure of the Act causes all information passing through the threshold of disclosure to become wholly and permanently bound to the disclosing officers. As such, the Act is expressly constructed to place responsibility and liability squarely on the shoulders of corporate executives. The way Sarbanes-Oxley achieves this aim is by eliminating what was previously an officer's most effective defense: the reasonable reliance defense.

The Exchange Act of 1934 allows that an officer can only be held civilly liable if he/she had the mental state to deceive<sup>1</sup>. The control framework contemplated by Sarbanes-Oxley is so comprehensive that it makes the possibility of an unintentionally false disclosure almost impossible. Moreover, it is the responsibility of the company to create a compliance-oriented culture to meet the subjective aspects of the Sarbanes-Oxley Act.

## **Lessons Learned**

Through its continued work surrounding Sarbanes-Oxley, governance, and compliance issues The CCRO has developed the following lessons learned from member companies' experience:

- Initial concentration on first phase of compliance (December 2004) – implemented quick fixes for initial planning, analysis and control design phase of Sarbanes-Oxley. These quick fixes do not support the significant financial and organizational commitment required for compliance over the long term.
- Need to focus more on institutionalizing the Sarbanes-Oxley compliance processes as part of daily business practices including creating a culture of compliance.
- More emphasis on a document management system that not only automates the large volumes of content, process maps, control test plans, etc. necessary for Sarbanes-Oxley compliance but also helps organize, analyze and document financial control objectives, business risks, and control design and testing.
- Recognize that Sarbanes-Oxley compliance was not just a one-time accounting exercise but rather an opportunity to develop value-added business processes that better manages and improves internal controls – a true business improvement initiative.
- Implementation and documentation of best practice energy risk policies and the associated specific process and procedures derived from these policies.

---

<sup>1</sup> see *Scienter* Ernst an Ernst v. Hochfelder, Ill., 425 U.S. 185, 96 S.Ct. 1375, 1381.

- Before deciding to install an enterprise system to manage Sarbanes-Oxley compliance – businesses need to take a more cautious approach and use industry auditor’s compliance reporting tool for the first year in order to understand the Sarbanes-Oxley process.
- There is a lot of work to do under Sarbanes-Oxley so the industry should choose key business processes and focus on those first.
- Move past the use of spreadsheets -- the risk of continuing to use these under Sarbanes-Oxley is just too high. Data management, version control and security are just a couple of areas where spreadsheets fail in the Sarbanes-Oxley process. This will likely involve creating a central corporate database at the individual transaction level.
- Don’t forget the minor control deficiencies – it’s easy to forget these until the next time. Following up on these deficiencies should be an ongoing activity within any organization.
- Upon completion of the initial phase of Sarbanes-Oxley compliance – take time to make sure this documentation is well organized – it will help in the next round of compliance.
- Pay more attention to the actual costs incurred for the entire compliance exercise – this will give financial management a better understanding of the costs going forward for compliance.
- There should be a more active internal ownership within the organization on the compliance process and its ongoing changes and requirements. This will lead to using less external expertise and allow for more consistency in the next round of the compliance process.

We at the CCRO look forward to answer any questions you may have.

Sincerely,

*Bob Anderson*

Robert M. Anderson  
Executive Director  
Committee of Chief Risk Officers