Top Dozen FAQs about FERC SOC

Compliance Audits and Monitoring

1. What has FERC indicated about their plans to conduct SOC Audits?

A. FERC is continuing to implement their SOC Audit Program after announcing the commencement of Phase II at the January 19th Commission hearing. During February, over one dozen energy firms, representing a mix of gas and electric companies, were served with Data Requests, some of which are quite wide-ranging.

2. Do FERC's Audits cover extensive issues or are they more cursory examinations?

A. FERC completed their cursory examinations of the website and OASIS posting requirements in December (Phase I). The new round of audits comprise a full range of performance issues covering past, present and future compliance with the SOC. Initial reports from the first group of Phase II auditees indicate that some of the data requests have over 70 items that could result in terabytes of information transfers and thousands of pages of printed materials over a four-to-six month audit period.

3. Will FERC audit every jurisdictional energy company?

A. FERC has the responsibility to ensure that all jurisdictional facilities are in compliance with the rules and regulations of the SOC. By auditing companies in the initial stages of Phase II, FERC hopes that other companies learn from the experiences of the early auditees. Eventually though FERC will have to assure themselves that all companies are complying with the SOC.

4. What standards or practices will FERC use for their audit basis?

A. There are few standards or practices that FERC has indicated is an acceptable compliance threshold for the many elements of the SOC. Besides the specific indications contained in the rules, other standards and practices will become better known as FERC's audit program progresses. FERC wants prompt compliance and they are fostering an audit environment that is flexible and workable for each company. Not every compliance technique will work equally effective at any given company.

5. If there are no standards or practices how can a company ensure that the measures they take will be compliant with the rules?

A. Depending upon your interpretation, the rules may be ambiguous **or** FERC may be granting wide latitude to companies that are engaged in compliance activities. FERC's expectation is that companies will be ***consistent*** in their application of the rules. Concepts such as good-faith-effort and Best Practices are applied as FERC looks at company's compliance responses.

6. What help is there to assist us in our compliance efforts?

A. Your internal regulatory staff has already developed many of your compliance activities. Industry associations can also provide some guidance. FERC staff has been helpful with meeting requests, telephone conferencing and disseminating information. Private firms, such as outside law firms and Regulatory Service Providers (like ProComply) have also developed some tools and information kits.

7. How can I best prepare for a FERC audit?

A. In an ideal environment, each company should satisfy themselves that they have exercised the highest level of diligence, control and governance as they would with any other regulatory regime. The keys to ensuring that the company is making its best efforts are preparation, implementation and monitoring of each element of the SOC. A core team of across-the-board company personnel, empowered with executive sponsorship, should regularly commit to ensuring that the company is executing at the maximum effectiveness.

8. Is there any value to self-auditing and internal compliance monitoring?

A. Contrary to the views of some companies that continue to resist compliance with the SOC, FERC has strongly encouraged companies to pursue compliance with the SOC by engaging in the typical policy-and-control formulae that are applied to other regulatory regimes, like Sarbanes-Oxley for example. While FERC cannot grant any dispensation to companies that self-audit and self-report, they might narrow the scope of their own audits as they deploy resources to uncovering more urgent non-compliance practices elsewhere.

9. How can self-auditing be implemented at the company level?

A. A typical self-audit program involves several steps of development:

i. breakdown the SOC rules into its constituent elements;
ii. ascertain the range of compliance responses (current industry practices);
iii. determine the relevancy and impact of each of the elements;
iv. ascertain your current level of compliance with each element;
v. accumulate documentary and other evidence of that compliance;
vi. develop audit objectives and findings criteria for each element;
vii. coordinate, produce and conduct the audit event; or
viii. hire an outside SOC auditing firm (like ProComply).

10. How can effective internal monitoring be implemented?

A. An internal monitoring program is more comprehensive than a self-audit which gauges only current compliance. Internal monitoring can be developed only after an initial assessment or audit of current compliance has produced the body of information from which to begin programmed monitoring. An Internal Monitoring Program, which ***gauges continuous-compliance***, should, at a minimum, consist of:

i. a thorough understanding of all existing company operating procedures at the administrative, operational, technical and financial levels;
ii. a thorough understanding of all existing internal governance controls and mechanisms to monitor compliance with other regulatory regimes;
iii. an acceptable cost-benefit analysis of specific consequential monitoring processes;
iv. repeatable metrics and tests to regularly ascertain compliance status;
v. an effective corrective control process for managing and implementing corrective change; or
vi. hiring an outside SOC Monitoring Program developer (like ProComply).

11. This looks like a lot of upfront labor just to comply with some vague rules. Why should we spend our resources on this much work?

A. Besides the possible penalties for non-compliance (fines are typically in the millions, with highest to-date at over $20 million), there are other considerations as well. Companies are obligated to inform their shareholders of any risks they may be facing. Being at the minimally-compliant level with the SOC is certainly much riskier than being continuously-compliant. Not spending the resources to obtain compliance validation would be viewed very unfavorably in this current environment.

An important benefit of the upfront work is that it avoids the mess, confusion and huge costs associated with the fallout from a failed audit or non-compliance exposure. The costs to a company for handling a FERC audit are many times more expensive than to conduct good compliance practices from the outset- and its just good corporate governance.

The rules are not vague. They *<u>are</u>* complex and they seem to be a moving target, but FERC intends that companies have the option of complying with various SOC elements in the manner that best fits the company's business and operating procedures, as long as their measures result in compliance.

12. How can our Company have the best compliance program and avoid FERC as best we can?

A. ProComply offers products and services exclusively for FERC Standards of Conduct. Our expert training programs are highly customized and used by nearly three dozen varied gas and power transmission providers. Our SOC Audit Program is an independent evaluation of all of your current compliance efforts, a sort of gap analysis. Our Compliance Monitoring Services provide thorough and independent ongoing corroboration of the status of key compliance metrics. Together this package of offerings is the leading-edge approach to minimizing the risks of violations and the multi-million dollar fines that are being assessed.