American
Petroleum
Institute

Lisa A. Soda
Corporate Affairs Ass
1220 L Street, Northw
Washington, DC 20005-4070
Tel 202-682-8590
Fax 202-682-8207
E-mail sodal@api.org

Jonathan G. Katz, Secretary
Securities and Exchange Commission
450 Fifth Street, NW
Washington, DC 20549-0609

Dear Mr. Katz,

Thank you for the opportunity to respond to your request for comments on the implementation of Sarbanes-Oxley Internal Control Provisions. The comments below are a compilation of industry response generated and supported by the American Petroleum Institutive (API) Information Technology Security Forum (ITSF). The ITSF is made up of the Corporate Chief Information Officers at API member companies. Please feel free to contact me with additional questions and/ or feedback to the oil and natural gas industry.

API Information Technology Security Forum (ITSF) Response to SEC Request for Input on Sarbanes-Oxley

- Guidelines are needed as to what general computer controls should be included for SOX. In the absence of such guidance, organizations are defining their own control sets which vary widely in content, and different auditing firms are emphasizing and testing different controls. This raises the likelihood that some organizations may be required to do more to comply with SOX than others.

  General computer control guidelines should not be completely prescriptive. Threats to computerized information are constantly evolving, requiring corresponding alteration of computer security countermeasures. A prescribed set of general computer controls would be counterproductive as there would be little incentive for companies to do more than the SOX requirements. This could actually lead to an erosion of security and a greater likelihood that a newer computer attack could compromise financial data.

  Rather than dictating all of the controls, we believe a model similar to that used in the HIPAA Security Rule should be considered. The HIPAA Security Rule classifies controls as "required" or "addressable". Required controls must be implemented. Addressable controls should be examined by the entity to determine the applicability of the control, and then either implement it, implement compensating controls, or document why the control is not necessary. A concept of addressable controls would provide flexibility in SOX compliance and allow for new technologies or countermeasures to be introduced while ensuring that all companies address the same needed computer general controls.

- As the primary purpose of SOX is to prevent inaccurate data within the financial report, the SOX IT control sets should focus on the integrity of financial information rather than on the availability and/or confidentiality of the information.

- There should be some benefit or efficiency to having adequate general computer controls. Reliance should be placed on ensuring adequate general controls so that application controls testing can be reduced. For example, if an application control, such as a SAP system configuration control around three way match of PO/Receipt/Invoice has been tested in year one, and configuration change management controls have been tested and are adequate in year two, there should be no need to retest the configuration control around the three way match in year two.

- The following controls should be considered "required" (mandatory) for SOX compliance within all companies:

    - Access security to view, add, change or delete data is based on the individual's demonstrated need, which is in line with the organization’s security policy.
    - Management has a control process in place to periodically review and confirm access rights. Periodic comparison of resources with recorded accountability must be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration.
    - A strategy for back-up and restoration is in place that includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures are in place to ensure that back-ups satisfy the above-mentioned requirements.
    - The logical access to and use of IT computing resources is restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. These mechanisms prevent unauthorized personnel from accessing computer resources.
    - User accounts are managed to ensure timely action related to requesting, establishing, issuing, suspending and closing user accounts. This includes formal approval by data or system owners granting access privileges.
    - Procedures are in place to provide a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function. The tests cover all components of the information system (e.g., application software, facilities, technology, user procedures).
    - Changes (emergency and scheduled) are recorded and authorized.
    - Appropriate segregation of duties exists between the personnel recording financial transactions and programmers and implementers.
    - Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.

- The SOX controls need to be considered in their entirety. For example, some IT issues (administrator access for example) are better mitigated by financial controls and vice versa. Focusing on controls in a silo may result in companies spending abhorrent time and resources fixing IT items which may already be mitigated elsewhere.