TASK FORCE: SARBANES-OXLEY COMPLIANCE
Plan of Action

Situation Analysis

Sarbanes-Oxley compliance remains a daunting challenge, with murky requirements and perplexity over what constitutes reasonable and effective compliance. The ambiguity has led to a state of general alarm over potential noncompliance consequences, with internal and external auditors, consultants and lawyers engaged in a feeding frenzy. CFOs and auditors run roughshod through the IT organization, sapping IT productivity in the short term and wresting control over business processes away from the CIO (perhaps permanently). Regulators, auditors and primary IT vendors threaten to exert unwelcome influence on how compliance should be achieved, potentially to the detriment of the business.

Beyond the immediate challenges of compliance, the Sarbanes-Oxley process is significantly transforming audit practices, which may have repercussions for business and IT far beyond the Sarbanes-Oxley deadline.

Mission Statement

The CIO Executive Council seeks to help CIOs effectively manage the ongoing process of achieving Sarbanes-Oxley compliance by crafting broadly accepted guidelines for reasonable and effective compliance with what are deemed the most critical and IT-relevant requirements. The Council will assist CIOs in jointly leading (with Finance) compliance efforts by sharing compliance intelligence and best practices, and collectively influencing and partnering with regulatory agencies, audit firms and primary IT vendors on what constitutes reasonable and effective compliance.

In addition, the Council will work on behalf of its members to proactively understand changes to audit practices and help guide legislation relating to audit practices.

Assumptions

- Legal council will be involved in the creation, review and approval of all deliverables

Constraints

None identified

Leadership Team

- Chair, Marc West (CIO, Electronic Arts)
- Standing Committee Chair, Randy Krotowski (CIO, ChevronTexaco)

Key Audiences

- The CIO Executive Council (CIOs)
- Audit firms and associations
- Appropriate regulatory agencies and legislators
- Executive peers (CEOs, CFOs)
- Primary IT vendors
- Business and mainstream media
- Legal council

Goals

- Bring clarity to Sarbanes-Oxley compliance
- Assist CIOs with achieving compliance reasonably and effectively
- Advance the CIO agenda on compliance priorities and methods for effective and reasonable compliance to Sarbanes-Oxley requirements
- Understand and influence the changing nature of audit practices and their ramifications

Objectives

- Focus attention on the most critical and IT-relevant compliance requirements
- Define, document and promote guidelines
- Leverage Council experience and intelligence with compliance best practices, tools and audits
- Create a dialogue with select audiences to discuss Sarbanes-Oxley compliance
- Create a knowledge-exchange channel with select audiences to discuss audit practices

Major Deliverable(s)

- Develop and promote a CIO Sarbanes-Oxley playbook that will help guide CIOs in what they must do to achieve effective and reasonable compliance. Elements may include:
  - Clarification and enumeration of the most critical requirements of the legislation that fall in the CIO's purview—what the CIO should focus on. These may include the following:
    - System development and implementation
    - Management of changes
    - Computer operations
    - Security
    - Company-level controls
    - Monitoring and evaluation
  - Leadership models for managing compliance campaign and projects. This could include education for the CFO and CIO on the rationale for a CIO leadership role.
  - Compliance campaign and best practices, tips and techniques gleaned from practitioners
  - Sample project plans
  - Confidential compliance case studies
  - Annotated list of effective compliance tools
  - Resource listings
  - Discussion of the playbook in live, dedicated forums for Council members and potentially select non-members.

- Establish formal and ongoing dialogue opportunities with identified audiences relating to Sarbanes-Oxley issues. Specific goals of the dialogue may include:
  - Seek input for, and ultimately approval of, the CIO Sarbanes-Oxley playbook, thereby heading off influence from other parties that may be detrimental to CIOs' businesses.
  - Influence legal, auditing and consulting practices and behavior as they relate to compliance consulting and auditing.
  - Establish dialogues and partnerships with primary software vendors on orchestrated ways to facilitate compliance in their product development and deployment. It may include a live-event "summit" with major vendors.

- Establish formal and ongoing knowledge-sharing channels with identified audiences on the changing nature of audit practices and the ramifications for IT and business.

Founded by

The Resource for
Information Executives