CIOs now come under Sarbanes-Oxley

Description

Dec 15 2014 : This was the deadline for a new Sarbanes-Oxley framework regarding management of Technology Assets. Read the article below to get details of what needs to be done in the control, governance and reporting of technology assets and its management.

Article by Craig Calle, SHI.

(link to original article at the end of this post, published here through WordPress share)

Today (Dec 15 2014) marks a turning point for anyone responsible for managing technology assets. As of today, accounting professionals are obliged to put technology in the **Sarbanes-Oxley** (SOX) spotlight.

Just about everyone has heard of SOX, the legislation passed in 2002 in response to notorious accounting scandals at Enron, WorldCom, and other public companies. The premise was that if we could ensure the quality of corporate financial reporting based on secure internal controls, we could enhance the integrity of our financial system. SOX ushered in a number of new requirements for company management and boards, as well as for the accounting profession. Among the more noteworthy aspects, per Section 404 of the Act, CEOs and CFOs have to personally affirm their responsibility for maintaining an adequate internal control structure and procedures for financial reporting, and (per Title III) can be individually liable for shortcomings in the accuracy and completeness of corporate financial reports.

Less well known is just how corporate management and the auditing community design and evaluate internal controls. The answer is that they rely on the Committee of Sponsoring Organizations of the Treadway Commission, or COSO, an organization that provides thought leadership and guidance on internal control, enterprise risk management, and fraud deterrence. COSO promulgated foundational guidelines in its Framework as far back as 1992 and updated its guidelines in May 2013. Generally speaking, the updated guidelines accommodate a business landscape that has changed considerably over the past two decades. Of interest to those who are naturally drawn to this blog is that the new Framework draws special attention to technology assets. The updated guidelines set a deadline of **today** for companies to adopt their new Framework for internal controls.

The **new Framework** is comprised of five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. These components embody 17 principles representing the fundamental concepts of internal control. The principle of interest to Finance/Accounting and IT executives is a control activity: “The organization selects and develops general **control activities over technology** to support the achievement of objectives.**”**

What does this mean for corporate executives? The new Framework has implications for IT asset management (ITAM), IT service management (ITSM), and data security — a set of disciplines we call technology asset management.

Internal auditors will be obliged to scrutinize their IT and procurement departments much more carefully than ever before. The quality and degree of housekeeping around ITAM will have to escalate dramatically. Organizations will need to persistently know whether software entitlements match actual usage — no small feat. Organizations also will have to know where devices are located, so they're not just asset tagged and forgotten. At a time when it is more likely that companies would record furniture rather than software on their balance sheet, the accounting profession is finally addressing the assets that generate significantly more return — and risk — to shareholders.

A company that has outsourced IT to a third party should be especially interested in the updated COSO Framework. Outsource service providers can give companies the false comfort that the ITAM box is checked, but often fall short of comprehensive control.

Organizations increasingly are evaluating and implementing new ways to help them deliver services to their employees. This revolution in service management, popularized by ServiceNow, but also offered by BMC, CA, IBM, and HP, among others, will no doubt cause precipitate scrutiny around the associated internal controls.

Considering how vulnerable companies have been to security threats, and how increasingly public security failures have become, we predict that these new SOX guidelines will be an important catalyst for improvement.

Technology asset management is hard to do right. It is a practice that cannot be executed simply by purchasing a software tool, although there are many available, from Flexera, HP, LanDesk, ServiceNow, and even SHI. Tools play their part, but success in ITAM almost always comes from a rigorous review of an organization's behavior to understand how business needs are satisfied by technology, and how that technology is procured and managed. People and process far outweigh the importance of the tools in the world of technology asset management.

SHI's **Asset Management Team** is uniquely positioned to help your company get its arms around the technology assets that generate considerable risk and return to your shareholders. Contact myself or your account team today to learn more about how these newly effective SOX regulations affect your organization.

https://rythium.com/sarbanes-oxley-deadline-new-chapter-technology-asset-management-shi-blog/

https://rythium.com/

You might want to read more about our CEO Sheshagiri Anegondi (Sheshu). He is amongst the foremost Oracle License Experts globally.

Author
adminlicens