Achieving
Higher
Expectations

**COSO Framework for Service Organizations and SOC Reporting (Part 1 of 3)**

One of the most important reference tools that companies use to establish and evaluate their internal controls is the Committee of Sponsoring Organizations' (COSO) *Internal Control - Integrated Framework.* Initially published in 1992 (the 1992 Framework), the COSO framework has been the most widely used model for internal control for the past 20 years. Auditing standards followed by CPAs who delivered SAS 70 reports historically and now deliver Service Organization Control (SOC) 1, 2 and 3 reports require that elements of the COSO framework be considered and addressed in all SOC reports. This generally appears in section 3 of SOC reports. The 1992 Framework received additional recognition and prominence with the passage of the Sarbanes-Oxley Act of 2002. Section 404 of the Act required publicly traded companies to evaluate their internal control over financial reporting relevant to a "recognized framework". The 1992 Framework was selected by nearly every public company as the benchmark for evaluating controls and was also endorsed by the Securities and Exchange Commission.

In order to address the significant changes that have occurred in the past 20 years in technology and the business environment, COSO updated the 1992 Framework in 2013 (the 2013 Framework). When the 2013 Framework was released, COSO provided guidance and recommendations about transitioning to the new framework by or before December 15, 2014. After that date, the 1992 Framework is considered superseded by the 2013 Framework.

Just as public companies have had to transition to the 2013 Framework for their SOX 404 compliance efforts over the past year, service organizations who receive SOC 1, 2 or 3 reports also must make this transition. Public companies have been required by their external auditors during the past year to map their historical control systems to the 2013 Framework. Service Organizations have not been required to go to the same lengths and produce the same documentation as public companies, but CPAs who deliver SOC reports are also heavily focused on this when evaluating the design of controls and the description of service organizations' systems.

Three differences between the 1992 and 2013 Framework that impact service organizations will be evaluated in this post and 2 future posts:

1. Emphasis on understanding and evaluating controls of outsourced service providers (OSPs).
2. Emphasis on risk assessment and fraud risk assessment.
3. Emphasis on IT controls.

The first item above is likely the most relevant to service organizations who receive SOC reports and has the most over-arching impact. COSO recognized that over the past 20 years there has been a massive shift in outsourcing and the use of OSPs. As such, the 2013 Framework includes requirements for evaluating the controls of significant OSPs. Companies that use OSPs (user entities) are now paying much more attention to the SOC reports of their significant OSPs. And these user entities are expecting their OSPs to adopt the 2013 Framework and provide relevant information about it in the SOC report. SOC auditors can guide their clients through this process and help them make the relevant updates to SOC reports and control components.

Another result of the increased emphasis on controls of OSPs in the 2013 Framework is that more and more service organizations are being required by their customers to provide annual

K Financial, Inc.

The State
Mercantile Building
801 Main Street, Suite 225
Louisville, CO 80027
Phone: 303.665.8060
Fax: 303.665.0813
www.kfinancial.com

SOC reports. In the past, particularly when SAS 70 was still the de facto standard for service organization control reporting, audit reports were generally only required of the largest service organizations. Now, the requirements are trickling down to smaller service organizations as their customers develop a greater appreciation of the importance of controls at OSPs.

In upcoming blog posts, we will evaluate how other changes in the 2013 Framework impact service organizations that receive SOC reports.

Thanks for reading!