Achieving
Higher
Expectations

COSO Framework for Service Organizations and SOC Reporting (Part 2 of 3)

In part 1 of this series, we discussed the recent changes to the COSO framework and the overall impact that the updated framework has on service organizations that receive Service Organization Controls (SOC) reports. Three of the differences that were identified between the 1992 and 2013 Framework that impact service organizations are as follows:

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.

In the last post, we discussed item #1 above. The objective of this post is to discuss the increased emphasis on risk assessment and fraud risk assessment.

Every SOC report (whether it is a SOC 1, SOC 2 or SOC 3) should include information about the service organization's risk assessment process. Risk assessment can take many forms and there is no "one size fits all" format. Risk assessment is intended to be an evolutionary process, designed to meet the specific needs of individual companies. Many of our SOC clients struggle with risk assessment and ask the following questions:

- Who should be involved in the risk assessment process?
- What topics should be covered in our risk assessment?
- How should we document our risk assessment?

The COSO framework includes valuable guidance to help answer these questions, including practical examples of how the risk assessment process can / should be performed. Generally, we recommend that C-level executives participate in the risk assessment process, as well as each department head. The risk assessment should cover questions such as the following:

- What events could occur that could prevent us from achieving our strategic objectives?
- What could happen that could bring our company to its knees?
- What keeps each member of the C-suite up at night?
- What has gone wrong in the past and what are we doing to address it?

We recommend that our SOC clients formally document the risk assessment in a memorandum and update it at least annually. The significance of impact and likelihood of occurrence should be assessed for each risk that is identified and controls should be identified and linked to the risks.

As a result of the increased emphasis on fraud risk assessment in the updated COSO framework, many companies are beginning to produce stand alone fraud risk assessments. Another approach is to include very specific consideration of fraud in the overall risk assessment. The fraud risk assessment should include the matters identified above, but with an emphasis on fraud. It should also include specific brainstorming regarding how the company is susceptible to fraud and how fraud could be perpetrated both internally and from outside parties.

Two of the controls that appear in almost every SOC report relative to fraud are background checks and reference checks. Both are valuable, but we often see an increased emphasis on background checks and less documentation and rigor around reference checks. Keep this in mind – 86% of fraudsters that are caught and prosecuted have no felonies on their records.

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

But many of them are not “first time offenders”. Studies show that companies will often fire fraudsters and not take the time to prosecute them so there is no record of their prior offenses. For this population of individuals, background checks do not provide much value. We recommend that reference checks be performed consistently for new hires, in conjunction with background checks, and that they always include the following question: “Is this person eligible for re-hire?” For legal reasons, references do not generally provide much information. However, the re-hire eligibility question is often considered safe and is answered. A “no” response to this question is valuable information that can be used to prevent a future fraudster from working for your company.

Thanks for reading!