AuditLiaison

Preparation Steps for SAS 70-SSAE 16 Audit
January 2011

SAS 70 has been around since 1992. However, due to a number of storied events and data privacy and business trends, it has become something that more and more companies are becoming familiar with in recent years.

SAS 70 stands for "Statement of Auditing Standards No. 70: Service Organizations" issued by the AICPA. SSAE 16 stands for "Statement on Standards for Attestation Engagements No.16, Reporting on Controls at a Service Organization" which supersedes the SAS 70 requirements for periods ending on or after June 15, 2011. Historically, SAS 70 audit/attestation reports were most relevant to auditors.

However, with the introduction of the Sarbanes-Oxley Act in 2002, internal controls over financial reporting stepped into the spotlight. It seemed suddenly that every publicly-traded company was requesting SAS 70 audit reports because nearly every company utilized at least one service organization. In addition, due to the widespread cases of data theft over the last decade, user organizations (the companies utilizing service organizations) became more and more concerned about data privacy .

The AICPA has substantially enhanced the information available to both service organizations and their customers with the newly developed "Service Organization Control (SOC) Reports Section". Information as to what type of SOC report is required by service organizations and what each service organization should consider is provided here.

Is a first time SAS 70 certification on the radar for your organization? If so, you'll need to carefully set expectations with your customers who are likely the most interested in your SAS 70 progress. In doing so, you'll need to determine the scope of the project, get comfortable with a possible lengthy timeline, assess potential complexities of implementation, and factor in an appropriate amount of time to run with the new and improved controls before commencing the actual audit.

During the preparation for the audit, it may be helpful to frequently remind yourselves that this is not an exercise designed simply to pass an audit. The objective of the SAS 70 / SSAE 16 audit and preparation process is to ensure that your company remains focused on delivering high quality products and information to your customers in an efficient and effective manner. This understanding will help to avoid taking an otherwise minimalist approach while implementing the key controls that impact customer financial reporting, and related, data and assets.

Setting Customer Expectations: Timeline

The timeline required in preparing for and undergoing an audit of controls as a service organization is surprisingly lengthy. You will need to assess existing controls and remediate control deficiencies before operating new controls for an acceptable period prior to beginning the audit [See Countdown to Audit article.docx for illustrative timeline details]. An acceptable duration to operate with effective controls before the audit is 6 month. The relevant timeframe from an accounting industry standard is important because although your customers have asked for your SAS 70 audit report, the awareness was driven by their audit firm. However, the six month operating effectiveness requirement is not the only factor in causing the lengthiness of the SAS 70/SSAE 16 preparedness timeline.

Project Leadership

As a service organization, it is critical that you understand how to manage an effective and efficient internal controls audit. Management must first identify and assign a leader to monitor preparedness progress and provide updates to the executive team. The criticality of committing to the chosen project lead cannot be overstated. The importance of Management's commitment to a favorable SAS 70/SSAE 16 preparedness project outcome must be communicated throughout the organization. And, the project lead must understand that no other demands take precedence over the execution of the preparedness plan.

Risk-driven Scope

The next step is to clearly define the significant processes that impact your customers' financial statements. Once the significant processes have been identified, an operational and financial risk assessment must be performed. What services are you providing? What are the risks to the customer from operational and financial perspectives? Simplify the risk assessment process by asking "What could go wrong?" during processing. Every service provider has two primary concerns: 1. Protection of customer assets (**including** their data), and 2. The accuracy of customer transactional information. Involve the management team, but most importantly, involve your process owners. The process owners understand how the transactional information flows and have often experienced what has gone wrong during processing in the past. Analyzing past mistakes provides valuable insight. Management teams, across industries and even country borders, tend to appropriate a false sense of security once an error has been corrected. Process breakdowns and errors tend to recur at vulnerable points during processing. The vulnerable points are identified by analyzing past errors as well as performing a thorough risk assessment.

Assess Control Gaps and Remediate

Once the risks have been identified, management and the project team can begin the control design and implementation process to address the vulnerabilities. First, define and test the existing controls that the company relies on to ensure accurate customer processing. Do the existing controls work? Is there evidence that they were performed? What additional controls are needed? The control solutions to implement depend on the type and nature of risks identified. Automated controls almost always function more effectively than manual controls, however, they can be more complicated to design and take longer to implement. With that said, once implemented, they are highly effective and easier to maintain. The other control "type" consideration is whether to focus on prevent versus detect controls. Ideally, you want a good mix of prevent and detect controls.

Implement / Monitor / Call your audit firm

The point to understand during the risk assessment and control identification process is that an internal control environment over transactional processing and financial reporting cannot be built on the assumption that no mistakes will be made. In spite of all that we know, companies continue to take a minimalist approach in implementing the key controls that impact customer financial reporting, and related, data and assets. Don't be fooled into thinking that the project you are undertaking is to pass an audit. Utilize the SAS 70-SSAE 16 audit preparation process to ensure that your company remains focused on delivering high quality products and information to your customers in an efficient and effective manner.

At this point, the risks to accurately and securely process customer transactions have been defined. Likewise, prevent controls have been identified at the key inflection points throughout processing. Detect controls have been identified to provide sanity checks for completeness, accuracy, valuation, occurrence, and presentation and disclosure. The Company then develops a project plan to remediate the controls gaps identified.

As you can note in the timeline, the risk and control identification process should take no longer than 2 or 3 months if it is done efficiently. The remaining time spent in preparing for a SAS 70-SSAE 16 audit will be remediating the "gaps" between the risks and existing controls. At this point, ensure that the project lead has a firm grasp of the company's operations, as well as, project management. The lead must clearly understand and be able to communicate what will be required to enhance the existing control environment. In addition, the lead, or a professional project manager in most cases, must be able to keep the process owners on schedule and facilitate the implementation of the new controls. With an appropriate timeframe and strong leadership, the SAS 70-SSAE 16 audit preparedness process can transform the entire operating environment into being completely customer-focused.

Author: **Jay P. Anthony, Certified Public Accountant, Certified Information Systems Auditor, & Certified Forensic Accountant** has nearly 20 years of audit experience and has been involved in performing or managing numerous SAS 70 audits, Sarbanes-Oxley internal control audits, and financial statement audits. For questions or comments on the article, please email jay.anthony@auditliaison.com.