An Overview of Service Organization Control (SOC) Reports

Recently there have been significant changes to reporting on service organizations. Due to the ever increasing compliance, regulatory and financial oversight in today’s business world, there are more requests for service organization control reports than ever before. This document provides a high level introduction to the recent changes as well as a high level description of the different options service control organizations have to provide their clients with these reports.

A brief history of the service organization control report illustrates its current evolution:

1992 – In response to the need for audit firms to gain an understanding of the controls over financial reporting at client’s service organizations, the AICPA issued SAS 70. This allowed the service organization to perform an audit over its financial reporting controls on its service lines. User entities and their auditors could now rely on this report and did not have to audit the service organization themselves. This made the user entity audits more efficient and reduced the amount of effort that a service organization would have to go through to meet its clients’ needs. Service organizations would now only be subject to one audit as opposed to having clients’ auditors requesting separate engagements.

1992-2011 – During this twenty year period, service organizations began to use more and more technology in their service lines. Their clients responded by wanting information about not only their internal controls over financial reporting but also their security and IT controls. Even though SAS 70 reports were designed only to report on financial reporting controls, they were being used to report on other IT controls. In response to the misuse of the SAS 70 report and the need for service organizations to be able to report on their IT control system the AICPA started working on a new service organization control reporting structure.

June 15, 2011 – The AICPA’s new service organization control reporting system went into effect. Service organizations could now choose between three options of service organization control reports; SOC 1, SOC 2 and SOC 3 reports. These reports are discussed below.

SOC 1 Reports (SSAE 16)
SOC 1 reports have taken the place of SAS 70 reports. SOC 1 reports are also referred to as SSAE 16 due to the fact that Statement on Standards for Attestation Engagements 16 is the new guidance that auditors use to conduct a SOC 1 engagement. SOC 1 reports specifically address service organization’s internal controls over information and processes used for financial reporting by their clients. SOC 1 reports are intended to be used only by the service organizations’ clients and clients’ auditors. Some examples of services and operational controls included in SOC 1 reports are:

- Operational transactions that are significant to the organization's financial statements
• Automated or manual systems that process these transactions from point-of-entry to inclusion in the financial statements
• Accounting records that report the user organization's transactions
• How the user organization's information systems capture information significant to their financial statements
• The reporting process used to prepare the organization's financial statements

SOC 2 Reports
SOC 2 reports were designed in order to accommodate service organizations clients’ need for information about the service organization’s IT controls. With the introduction of cloud services, Software as a Service, data centers, etc... it became necessary to introduce a specific reporting framework to report on IT controls around these services. The SOC 2 report specifically addresses one or more of the following five attributes; Security, Availability, Processing Integrity, Confidentiality, and Privacy. The report was designed by the AICPA in order to give service organizations a structured method in which to evaluate and report on the effectiveness of their IT controls. The SOC 2 report offers a detailed description of the service organization’s key controls over one or more of the above attributes. The report is restricted to specified parties and is commonly only used by a service organization’s clients and potential clients. Auditors perform SOC 2 engagements under Attestation Standards 101 (AT 101).

SOC 3 Reports
A SOC 3 report is used to report on the same IT control attributes that a SOC 2 report does. Whereas the SOC 2 report is a restricted report that provides a detailed description of the controls identified in the report, a SOC 3 report is a general use report (unrestricted as to who can use it) which gives the auditors’ opinion as to whether or not the service organization has achieved an effective control environment over one or more of the attributes. There are no descriptions of the internal controls in a SOC 3 report. Auditors perform SOC 3 engagements under AT 101.

TYPE 1 Reports vs. TYPE 2 Reports
In addition to having three different varieties of service organization control reports, SOC 1 and SOC 2 reports offer both Type 1 and Type 2 variations. A Type 1 report outlines the service organization’s internal control system as well as the suitability of the design of the control environment as of a specific date. In addition to the components of a Type 1 report, a Type 2 report includes an opinion on the operating effectiveness of the internal control system and a description of the tests of controls over a specified period of time. As a SOC 3 report does not provide any details of the internal control system, there are no variations of that report.

Benefits and Need of SOC Reporting
In a business environment where service organization clients need to have audits, and have an ever changing and increasing array of compliance requirements they are subject to, they often require their service organizations to have one or more of the SOC reports. SOC 1 reports allow their auditors to rely on the financial reporting controls of a service organization and save them the cost of having their auditors perform an independent assessment of the service organizations internal controls. A SOC 2 or
SOC 3 report gives users assurance that their information with the service organization is secure, confidential, and private, as well as that the system(s) they are using will be available, complete and accurate. Types of system(s) that a service organization offers as well as their clients’ needs usually determine what SOC reports a service organization obtains.

Figure 1 below provides an overview of the differences between the three types of SOC reports.

*Figure 1 – SOC Reporting Summary*

<table>
<thead>
<tr>
<th>Report</th>
<th>Controls Addressed</th>
<th>Content of Report</th>
<th>Use of Report</th>
<th>Report Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 1</td>
<td>Controls over financial reporting</td>
<td>Description of internal control system(s). Auditor opinion of fairness of presentation and suitability of design of internal control system. Type 2 report includes the auditor opinion of the operating effectiveness of the internal control structure as well as a description of the tests of controls performed.</td>
<td>Restricted to management, clients, and clients' auditors.</td>
<td>Type 1 and Type 2</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Controls over security, availability, processing integrity, confidentiality, and privacy</td>
<td>Description of internal control system(s). Auditor opinion of fairness of presentation and suitability of design of internal control system. Type 2 report includes the auditor opinion of the operating effectiveness of the internal control structure as well as a description of the tests of controls performed.</td>
<td>Restricted to specified parties; generally management, clients, and clients' auditors.</td>
<td>Type 1 and Type 2</td>
</tr>
<tr>
<td>SOC 3</td>
<td>Controls over security, availability, processing integrity, confidentiality, and privacy</td>
<td>Auditor opinion as to whether the service organization has achieved an effective internal control environment.</td>
<td>General use. No restrictions.</td>
<td>No options available.</td>
</tr>
</tbody>
</table>

About Kevin P. Martin & Associates

KPM is a CPA and consulting firm, offering a full spectrum of tax, audit, business, IT, risk and compliance services. We help organizations understand the increasing challenges they face, and create and implement plans and controls that enable them to manage their risk and comply with the myriad regulations to set them on a path for success and growth.

www.kpm-us.com
info@kpmonline.com
Call us: 781-380-3520