Third Party Risks:

Governance and Controls Assurance through SOC 1 and SOC 2 Reporting

Demands for Assurance

Third party processing organizations (a.k.a., service organizations) spanning a variety of business sectors including healthcare, financial services, life science, technology, services and distribution are being requested by their customers (otherwise known as "user organizations") to obtain an assurance report on control activities related to the integrity of certain processes and security over sensitive information being processed by those third parties.

Many user organizations realize that while they have outsourced certain aspects of their business, they continue to be responsible for the activities conducted by the third party processing organization. The customers of these user organizations are looking for enhanced assurance over how its information is used and protected. A good deal of this concern has been driven by well publicized hacking events such as Target, HomeDepot, Sony, and Yahoo. However, regulations and standards have also driven the demand such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), the Graham Leach Bliley Act (GLB), the Meaningful Use standards of the Centers of Medicare and Medicaid Services (CMS), and others including various state and International privacy laws. As the number of data breaches continues to increase, cybersecurity and the protection of data are of increasing importance to many organizations – and the list is growing.

Evolution from SAS 70 to SOC 1 Reports

Statements on Standards for Attestation Engagements No. 18 (SSAE 18) is an update to a previous standard known as SSAE 16, which itself was an update to another standard known as Statement on Auditing Standards No. 70 (a.k.a., SAS 70) that was created in the early '90's by the American Institute of Certified Public Accountants (AICPA) in which an auditor would provide assurance regarding specific control objectives over transactions and processes related to financial reporting. Service Organization Control No. 1 (SOC 1) reports are conducted using this standard and are based upon the achievement of Control Objectives established by management of an organization. For instance, a Control Objective may be stated like this, "All new customer contract pricing data is entered into the XYZ system accurately, completely and timely."

Depending upon the nature of the services provided, control objectives often include a combination of IT General Control objectives as well as financial processing control objectives. For instance, the Control Objective stated previously regarding customer contract pricing ultimately relates to financial reporting and is therefore a financial control objective. However, the statement, "All application and network program changes are reviewed and tested by a supervisory authority prior to being placed into the production environment," relates to an information technology processing control and is therefore an IT General Control objective.

SOC 2 Reporting

A separate set of standards were created by the AICPA in the early 2000's to establish requirements by the public accounting profession when examining and issuing reports on controls over matters not related to financial reporting. For instance, while payroll processing relates to financial reporting as it directly impacts the accuracy of payroll expense, the integrity of a background screening process does not directly relate to financial transaction processing and financial reporting. These requirements are codified within TSP section 100 of the AICPA's Trust Services Criteria (formerly known as the Trust

Services Principles). Reports issued under TSP section 100 utilize the five Trust Services Categories including Security, Confidentiality, Availability, Processing Integrity, and Privacy. Service Organization No. 2 (SOC 2) reports are conducted using TSP section 100.

Each of the Trust Services Criteria are supported by dozens of Points of Focus which provide greater definition of each Criteria. In addition, management of service organizations can choose to comply with all, some, or just one of the five Categories. Often, the choice of Category will depend upon the needs and wants of the service organization's customers.

TRUST SERVICES CATEGORIES OVERVIEW
Security – the system is protected, both logically and physically, against unauthorized access.
Availability – The system is available for operation and use as committed or agreed to.
Confidentiality – Information that is designed "confidential" is protected as committed or agreed.
Processing Integrity – The system processing is complete, accurate, timely, and authorized.
Privacy – Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with the privacy criteria put forth by the AICPA and the Canadian Institute of Chartered Accountants (CICA).

Type 1 and Type 2 Reports

Both within SOC 1 and SOC 2 engagements, the auditor may issue two types of reports, namely a Type 1 or Type 2 report. Specifically, a Type 1 report addresses management's description of the system and the suitability of the design of controls as of a specific date. Whereas a Type 2 report addresses management's description of the system, the suitability of the design, and the operating effectiveness of the controls over a period of time (e.g., six months). The demand for Type 2 reports far outpaces the demand for Type 1 reports as customers of 3rd party service organizations are seeking a greater level of assurance that controls have been in place and working for a sustained period of time – typically 12 months. However, Type 1 reports can fulfill a short term benefit, particularly when a service organization is given an ultimatum from an important customer or prospect that they must obtain a SOC report in order to continue to provide services. In these instances, Type 1 reports can be created in a much shorter period of time.

Revisions to the SOC Standards

The Trust Services Criteria were developed almost 20 years ago and they have undergone a few changes, particularly during the past five years, as the demands for greater clarity and simplicity have grown in the headwind of cybersecurity threats. Nearly every business that relies upon a 3rd party processor is seeking a greater level of assurance over some combination of security, confidentiality, system availability, processing integrity, and privacy. Also driving the demand for greater assurance is the rapid change and influence of technology in business and the ubiquitous exchange of sensitive financial and operational information like credit card and bank account data, Personally Identifiable Information (PII), and Protected Health Information (PHI).

The most recent revisions to TSP section 100 / SOC 2 reporting are intended to do several things:

- Provide a greater deal of flexibility in application across a variety of different subject matters including an entire entity, division, function, or a particular type of information used by an entity;
- More fully align the Trust Services Criteria to the 2013 COSO Internal Control Framework including the use of all 17 Principles and their underlying 88 Points of Focus;

- Streamline the underlying Criteria within the Privacy Category;
- Enhance the service organization's description of its Risk Assessment activities; and
- Expand the service organization's obligations to manage and monitor its own use of 3rd parties.

Obtaining a SOC 1 or SOC 2 report just a few years ago was an onerous task, as it was considered a painful and costly exercised for many organizations – especially smaller companies who lacked capital and capacity, as well as discipline to undergo an examination.

Unfortunately, the process may not get any easier or less expensive for the foreseeable future. Obtaining an unqualified opinion from a competent accounting firm will become more burdensome for several reasons including: 1) the increased disclosure required by service organization management; 2) increased risk of data breaches and related disruptions to business; and 3) related exposure to risk by the independent accounting firm providing the opinion. Perhaps adding to this dilemma is the shortage of professionals in public accounting who are willing and able to perform SOC reports.

SOC 3 Reports

SOC 3 reports are designed to meet the needs of 3rd parties who want some level of assurance regarding the controls at a service organization. SOC 3 reports are prepared using the AICPA's and the CICA's Trust Services Criteria, yet contain much less detail than what is contained within a SOC 2 report.

For example, a service organization may need to provide a prospective customer with some comfort that the service organization has obtained a satisfactory opinion from a public accounting firm in the form of a SOC 2 report. However, a service organization may be apprehensive to share the sensitive details contained within a SOC 2 report to a prospective customer including the description of proprietary processes and systems, as well as the results of controls testing, for fear that such information may be disclosed to the general public, or fall into the hands of a competitor. In this instance, a SOC 3 report will be made available.

In Summary

Cybersecurity insurance coverage alone will not protect most organization. In fact, many cybersecurity policies will begin to require some level of independent assurance such as a SOC report as a prerequisite for coverage. And even if a service organization maintains coverage as well as a SOC report, one might assume that the actual amount of insurance protection maintained in a cybersecurity policy is contained in the fine print.

SOC 1, SOC 2, SOC 3, SSAE 16, SSAE 18, SAS 70, TSP 100, COSO, Type 1 and Type 2 may sound like a game of alphabet soup. However, service organizations and users of those service organizations should be certain that assurance over systems security, confidentiality, privacy, processing integrity, and system availability is very serious business. In fact, it is likely to get even more serious as organizations experience the fallout of security breaches, denial of service attacks, and other serious disruptions to their business. Perhaps it may be time for those service organizations without a SOC report to begin exploring options.

About the Author

John McLaughlin, CPA is the Executive Director of The Audit Exchange and has performed SOC readiness work and signed over 100 SOC 1, SOC 2 and SOC 3 opinions across a variety of businesses. He can be reached at jmclaughlin@theauditexchange.com