# SYSTEM AND ORGANIZATION CONTROLS (SOC) REPORTS – How to Use Them and Who May Need Them

**Presented by: Mike Shamblin**

**PYA Audit & Assurance Principal**

**January 23, 2020**

# Overview

- History of the SOC report
- SOC 1
- SOC 2
- Type I vs Type II
- Anatomy of a SOC Report
- SOC 3
- Cybersecurity SOC

# History of the SOC Report

- Original Statement on Auditing Standard (SAS) 70 was issued in 1992
- SAS 70 report was designed as a way for organizations to demonstrate testing of their internal controls over financial reporting
- While not the intended purpose, organizations began using the SAS 70 report as a way to demonstrate, as a vendor, they were safe and secure to work with
- Statement on Standards for Attestation Engagements (SSAE) 16 (issued in 2010) replaced SAS 70
- SSAE 18 superseded SSAE 16 in 2017

# SOC 1

- The SOC 1 was created to reflect the purpose of the original SAS 70, which was a report for an organization to demonstrate testing of internal controls over financial reporting (ICFR)
- If Organization A serves Organization B and the ICFR of Organization A will impact the financial reporting of Organization B, then Organization B will likely want to obtain a SOC1 for Organization A
- A SOC 1 report is less common than a SOC 2 report

# SOC 2

- Created so that Organizations could demonstrate that, as a vendor, they are safe and secure to work with (i.e. data hosting organizations, payroll processors, investment trustees/custodians, etc.)
- There are five “Trust Services Principles” in a SOC 2 audit, which include:
  - Security – the system is protected against unauthorized access
  - Availability – the system is available for operation and use as committed or agreed
  - Processing Integrity – system processing is complete, valid, accurate, timely, and authorized
  - Confidentiality – information designated as confidential is protected as committed or agreed
  - Privacy – personal information is collected, used, retained, disclosed and destroyed in accordance with the privacy notice commitments

# Type I vs Type II

- Do not confuse a Type I and Type II with the SOC 1 and SOC 2
- Both the SOC 1 and SOC 2 have options of a Type I and Type II report
- A Type I report is focused on the design of controls and does not consider the operating effectiveness of controls
- A Type I is as of a specific date in time
- A Type II considers the design of controls (like a Type I) but also considers the operating effectiveness of controls
- A Type II covers a period of time – for example six or 12 months

# Anatomy of a SOC Report

- Service auditor opinion report – clean?
- Written assertion from management
- Description of the service organization's system of controls
- Complementary user entity controls – rely on the user entity (you) to implement to achieve the vendor control objectives
- Results of tests of controls

# SOC 3

- Very similar to a SOC 2 but with a couple of distinct differences:
  - A SOC 3 is designed to be more widely distributed and is not limited to user organizations
  - A SOC 3 report does not include a description of the service organization's system of controls

# Cybersecurity SOC

- Organizations are under increasing pressure to demonstrate that they are managing cybersecurity threats, and that they have effective processes and controls in place to detect, respond to, mitigate and recover from breaches and other security events
- To address this market need, the AICPA has developed a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs.  The framework is a key component of a new SOC for Cybersecurity engagement, through which a CPA reports on an organization's enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of an organization's efforts.

# SOC Reports

- Frequently Asked Questions

# QUESTIONS?

Mike Shamblin
mshamblin@pyapc.com

PYA, P.C.

800.270.9629 | www.pyapc.com