HOW TO FIND YOUR MATCHING "SOC" IN A BASKET OF WRINKLED GUIDANCE

By Mike Mellor, CPA DiSanto, Priest & Co.

DiSanto
Priest & Co.
Certified Public Accountants

Matching the right SOC report to your business can be like finding a matching sock in your laundry pile. Imagine you're holding in your left hand your favorite pair of socks, but not the whole pair, just one sock. The other sock that completes your favorite pair lies somewhere directly in front of you in a basket full of laundry that you took out of the dryer a couple days ago, but have since neglected to fold. Your laundry is wrinkled and tangled together and finding your matching sock is going to take some extra time from your morning routine: time you probably could have spent making your hair look just right. Now you could just grab a different pair of socks, a pair more easily accessible perhaps, but you don't want to wear just any pair of socks. You want the right pair. **Welcome to the world of SOC reporting.**

Now let's look at this story from another perspective. Let's say that the sock you're holding is actually your company, a service organization that has decided that it's time to start taking part in Service Organization Control (SOC) reporting. Maybe you want to show customers they can trust that the service your organization provides is reliable and will keep their information secure so that they choose to continue using your company rather than moving to a competitor. Or, maybe you have customers that are public companies, and their auditors have been requesting information on the controls you have in place over the service you provide. Whatever the reason, you have decided that getting a SOC report is the right solution.

BUT WHICH TYPE OF SOC REPORT DO YOU NEED?

As you may know, the AICPA has established three different types of SOC reports (appropriately named SOC 1, SOC 2, and SOC 3), each geared toward the purpose and user of that report, and figuring out the right one that meets your company's needs can be a lot like looking at basket full of your wrinkled, unmatched socks. So let's start folding some laundry to smooth out the wrinkles.

SOC 1 REPORT

We'll start with a SOC 1 report, often referred to as a SAS No. 70 or SSAE No. 16 report. Oftentimes when we think of SOC reporting, we inevitably jump right to a SOC 1 report. However, a SOC 1 is not necessarily the right match for your favorite blue and white, striped sock. A SOC 1 report specifically reports on controls at your service organization that relate to the user entity's financial reporting.

You will likely need a SOC 1 report if your customers and their auditors plan to use it as support for a financial statement audit, or if your customers plan to use it as support for their compliance with the Sarbanes-Oxley Act.

SOC 2 REPORT

But what if you're not communicating on controls over financial reporting? Perhaps a SOC 2 report could be the right match for that blue and white, striped sock. Instead of reporting on controls over financial reporting, a SOC 2 report relates to controls over five key factors: security, availability, processing integrity, confidentiality, and privacy. This report is more often used to establish trust in your organization and the service it provides. You would likely request a SOC 2 report if your customers need information and assurance about controls at your organization that affect the security, availability, and processing integrity of the systems your organization uses to process your customers' data, and the confidentiality and privacy of the information processed by these systems.

For example, companies in the financial services or health care industries will often require a SOC 2 report before working with, or continuing with, a service provider.

SOC 3 REPORT

Now maybe a SOC 2 report has too many stripes to match your favorite sock. Maybe your customers don't need all the details behind your processes and controls. That's when you would consider getting a SOC 3 report. A SOC 3 report is similar to a SOC 2 in that it relates to controls over security, availability, processing integrity, confidentiality, and privacy. However, a SOC 3 report is a general use report that provides a Certified Public Accountant's (CPA's) opinion on whether the organization maintained effective controls without going into the specific detail of each control or the CPA's tests of the controls.

A SOC 3 is generally beneficial if you want to make the report generally available, or if you plan to use the report as a marketing tool to attract potential customers.

Hopefully, now that we have folded through this laundry, you have found your matching "SOC." However, as any accountant has certainly figured out, accounting guidance can be a lot messier than your unfolded laundry. In fact, it's possible that your business needs more than one SOC report to fit its needs. You might need both a SOC 1 and a SOC 2 report, or maybe even all three reports, to fit the needs of all your report users. The table below, provided by the American Institute of Certified Public Accountants (AICPA), can help you ask the right questions in finding the appropriate SOC report for your organization:

HOW TO IDENTIFY THE SOC REPORT THAT IS RIGHT FOR YOU

Ask yourself the questions below to determine the best fit for your business.

Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customers' financial statements?	**Yes**	SOC 1 Report
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	**Yes**	SOC 1 Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	**Yes**	SOC 2 or 3 Report
Do you need to make the report generally available?	**Yes**	SOC 3 Report
Do your customers have the need for, and ability to understand, the details of the processing and controls at a service organization, the tests performed by the service auditor, and results of those tests?	**Yes**	SOC 2 Report
	No	SOC 3 Report

American Institute of CPAs. (July 1, 2015). Service Organization Controls (SOC) Reports for Service Organizations. Retrieved from **https://www.aicpa.org/InterestAreas/FRC/ AssuranceAdvisoryServices/Pages/ServiceOrganization%27sManagement.aspx**

About Disanto, Priest & Co.
Disanto, Priest & Co. is a full service public accounting firm headquartered in Warwick, Rhode Island with expertise in assisting companies in evaluating their current and planned third party assurance needs, like those described above. Give us a call if you need assistance as we would be glad to talk with you about your needs.

Headquarters
117 Metro Center Boulevard
Suite 3000
Warwick, Rhode Island 02886
Telephone 401.921.2000
Facsimile 401.921.2010
www.disantopriest.com