AICPA CITP Credential Examination Series

Topic: Service Organization Controls (SOC)

Presenter: Alex Thorne

Alex Thorne: Hello, and welcome to the AICPA CITP Credential Examination series. This podcast will assist you in preparing for the examination specific to the topic of Service Organization Controls.

By way of introductions, my name is Alex Thorne, and I am a AICPA CITP credential holder and a volunteer member of the CITP Credential Committee. I am pleased to share my insight around the topic of Service Organization Control reports, or SOC reports for short.

Specifically, the goal of this podcast will be to help you, the listener, understand when and what type of SOC report will be useful and also to clarify the differences between SOC 1, SOC 2, and SOC 3 reports, what they are used for, and just as important, what they are not used for.

Much of this material comes from a book titled *Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework* by Robert Moeller. Specifically, Chapter 19 of that book titled *Service Organization Control Reports and COSO Internal Controls*, which you can find on Safari Books.

You may be familiar with Safari Books if you are a member of the AICPA IMTA section. If you aren't familiar, I recommend you check it out. It's like an online library where you can check out books and read them for free, and the topics are relevant to the IMTA body of knowledge.

The SOC report chapter of the book also contains a great summary of the history behind the development of the SOC reports, from the early days of service organizations, to the old SAS 70 standard, and how it eventually evolved to the SOC 2 reports. I recommend checking that out also if you're interested in that history.

This podcast, however, will begin with considerations in determining the need for SOC reports, and then describe the three different types of SOC reports; SOC 1, SOC 2, and SOC 3, specifically the relevant users, the purpose and use, controls addressed, the standard under which the engagement is performed, and the report content.

When the AICPA in 2011 released a new service organization control reporting structure replacing the SAS 70, they defined three service auditor internal control reports called SOC 1, 2, and 3, with each designed to help service organizations meet specific user needs.

Broadly, all three of these reports are meant to assure the report's reader of the service organization's controls, and to help the reader obtain an objective evaluation of the effectiveness of those internal controls that address the compliance, operations, and financial reporting of a service organization.

Now, we will cover the differences between the three reports. First, SOC 1 reports, which are prepared in accordance with the Statement on Standards for Attestation Engagements No. 16, also known as SSAE 16, titled *Reporting on Controls at a Service Organization*. These SOC 1 reports retain the original purpose of SAS 70 reports and provide a vehicle for reporting on a service organization's system of internal controls that is relevant to a user organization's internal controls over financial reporting.

SOC 1 reports are intended to be auditor-to-auditor communications, just as the SAS 70 report had been. Their specific content will depend on the service auditor and the service organization's system. Their basic elements include the independent service auditor's opinion report, management's description of the service organization's system of internal controls, and the independent service auditor's tests of controls, as well as the results of these tests. Additional information provided by the service organization, but not covered by the service auditor's opinion may also be included within the SOC 1 report.

SOC 1 reports break down further into Type 1 and Type 2 reports. In a Type 1 report, the external auditor evaluates the efforts of a service organization at the time of audit to prevent accounting inconsistencies, errors, and misrepresentation. The auditor also evaluates the likelihood that those efforts will produce the desired future results.

A Type 2 report includes the same information as that contained in a Type 1 report. In addition, here, the auditor attempts to determine the effectiveness of agreed-on controls since their implementation. Type 2 reports also incorporate data compiled during a specific time period, usually a minimum of six months.

To illustrate the difference between a Type 1 and Type 2, you can relate Type 1 reports to performing walkthroughs of the controls only. In a walkthrough, you would understand the design of the controls and possibly examine evidence of one iteration of the control, also known as a test of one, to validate that it is suitably designed.

In a Type 2 report, you would have to go further than that, and evaluate the effectiveness of the control over time. There are many ways to do this. Testing a representative sample of the control's performance over the length of the audit period is one way, and also a way to visualize the difference between a Type 2 report, and the test of one for Type 1.

Before going on, it is important not to confuse SOC 1 with Type 1, or SOC 2 with Type 2. You can have a SOC 1 Type 1, or a SOC 1 Type 2. Same with SOC 2 reports; there are SOC 2 Type 1 reports and SOC 2 Type 2 reports.

So, let's discuss SOC 2 reporting. The purpose of a SOC 2 report is to offer service auditors and service organizations a reporting option when the subject matter is not relevant to controls over financial reporting. The SOC 2 report, prepared under AICPA Attest Standard AT 101, titled *Attest Engagements*, addresses controls at a service organization that are pertinent to security, availability, processing integrity, confidentiality, and/or privacy internal control issues.

In a SOC 2 report, management should identify one or more major internal control principles that it believes it has achieved and the criteria on which it will base its

assertion of achievement. This means that a SOC 2 report can address just security, or security and availability, or all five principles if management so chooses.

Now, a word on the five principles or the full name, the Trust Services Principles. Trust Services are a set of professional attestation and advisory services based on a core set of principles and criteria that address the risks and opportunities of IT-enabled systems and privacy programs. The following principles and related criteria are used by practitioners in the performance of Trust Services engagements.

Number one; security, which provides assurance that the system is protected against unauthorized access, use, or modification.

Number two; availability, which provides assurance that the system is available for operation and use.

Number three; processing integrity, which provides assurance that the system processing is complete, valid, accurate, timely, and authorized.

Number four; confidentiality, which provides assurance that information designated as confidential is protected.

And number five; privacy, which provides assurance that personal information is collected, used, retained, disclosed and disposed.

Further, SOC 2 reports are intended for user organization management and other stakeholders, such as business partners and customers, along with regulators who are knowledgeable about the subject matter and who may also benefit from the information contained within a SOC 2 report.

The report includes many of the same elements as a SOC 1 report, including the independent service auditor’s report, a description of the system, and a section containing the service auditor’s tests of the operating effectiveness of controls and the related test results.

To help understand why SOC 2 reports exist, in the past, confused readers would treat the SAS 70 report as assurance of their service provider’s quality, or possibly their cybersecurity processes, to evaluate them as a vendor. The SAS 70 was only meant to be read by auditors, so they could gain assurance over the controls relevant to their client’s financial reporting process only.

For example, if you obtained a SAS 70 from your vendor, it may have helped you understand if the reports you got from your vendor were accurate, but not if they protected your confidential data, or if they were vulnerable to malware, or something like that.

Now, the SOC 2 report is meant to do just that; provide the reader with assurance over the vendor’s security controls, or availability controls, etc., depending on the principles included in the report.

Also, as mentioned previously, a SOC 2 Type 1 would only provide the reader with an understanding of the suitability of the control's design. A SOC 2 Type 2 does that plus evaluates operational effectiveness over a period of time.

Finally, let’s discuss SOC 3 reports. SOC 3 reports, like SOC 2 reports, are also prepared under AT 101, and also allow service organizations to provide user organizations and other stakeholders with a report on controls that is relevant to security, availability, processing integrity, confidentiality, and/or privacy.

Unlike SOC 2 reports, however, SOC 3 reports do not include a description of the system or a detailed description of tests of controls and related test results. Instead, SOC 3 reports are short, maybe only a few pages, and publicly available, and they state whether the service organization’s system for providing its services to user entities is suitable. A SOC 3 report, you might find posted on the organization’s web page, while a SOC 2 report might be made available to a customer upon request.

When choosing between the three reports, a senior executive should meet with the user organization’s external auditors to assess which of these three types of SOC reports will best meet the varying needs of different audiences and cover different subject matter. A user organization should work with its external auditors, as well as directly with its service providers, to obtain reports giving it assessments of the internal controls provided by its service organizations.

On behalf of the AICPA Information Management & Technology Assurance Division, this is Alex Thorne and I’d like to thank you for tuning in to this CITP exam series podcast on the topic of Service Organization Controls.

This is one in a series of podcasts that the AICPA’s IMTA Division is pleased to offer around a variety of topics of importance for the CITP exam. Be sure to check out other podcasts in this series, on topics that include Data Analysis and Reporting Infrastructures, Data Backup and Recovery, Information Lifecycle Management, the COSO Model Framework, Internal Audit, PCI Compliance, and HIPAA Compliance.