INTERNATIONAL JOURNAL OF COMPUTER AUDITING
Editorial

Third Party Assurance: Need More Attention on SOC Reports

Ju-Chun Yen [1] | Tawei (David) Wang[2]

1. Graduate Institute of Accounting and Department of Finance, National Central University, Taiwan
2. School of Accountancy & MIS, College of Business, DePaul University, United States

Reference Format: Yen, J. & Wang, T. (2023). Third Party Assurance: Need More Attention on SOC Reports. International Journal of Computer Auditing, 5(1), 1-3. https://doi.org/10.53106/256299802023120501001

According to a Deloitte survey in 2022[1] , 76 percent of respondents had their IT services delivered through third-party models, and more than 90 percent of the respondents will rely on third-party service providers for data analytics and robotic process automation deployment arrangements. However, as these organizations (called user entities) cannot directly monitor the service providers' controls over the outsourced systems that may influence user entities' business operations and financial reports, whether these service providers establish suitable and effective controls to ensure the data confidentiality and privacy, system integrity, availability becomes an important issue for user entities.

Echoing the need for more reliable assurance of the controls of the service providers' systems, the Association of International Certified Professional Accountants (AICPA) introduced in 2011 the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) as the backbone framework for the SOC reporting[2]. The main SOC for service providers has three types[3]:

1. *SOC 1 addresses the controls of a service organization related to internal controls over user entities' financial statements (ICFR). There are two levels of SOC 1: Type 1 reports include the service organization auditor's[4] opinions about whether the service organization management's description of the system is fairly presented and whether the design of controls is suitable as of a certain date. For a Type 2 report, the service organization auditor needs to provide the same two opinions about the controls over a period of time and an additional opinion about the operating effectiveness of the controls. Also, in a Type 2 report, the service organization auditor needs to list the tests they performed and the test results.*
2. *SOC 2: SOC 2 addresses controls over a service organization that affect the following five criteria: security, availability, processing integrity, confidentiality, and personal data privacy, which has a broader scope than SOC 1. SOC 2 also has two levels of reports, Type 1 and Type 2, the same as SOC 1. While both SOC 1 and SOC 2 have restricted use for the service organizations and the management, clients, and financial statement auditors of the user entities,*

AICPA also provides another type of SOC report for service organizations for public use:

3. *SOC 3: The scope of SOC 3 is similar to SOC 2. However, for public use, SOC 3 report includes fewer details of controls and tests. In addition, the service organization auditor only provides one opinion about the operating effectiveness of controls.*

While SOC 1 is prepared according to AT-C section 320, "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting,"[5] the control criteria of SOC 2 and SOC 3 are based on TSP Section 100, "Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy." [6] The trust services criteria are aligned with common criteria in the COSO framework, categorized into control environment, communication and information, risk assessment, monitoring of controls, and control activities. In addition, the trust services criteria include category-specific criteria related to availability, processing integrity, confidentiality, and personal data privacy.

Despite its importance, our understanding of SOC reporting remains very limited. In this editorial, we encourage more research in the following three areas as a starting point for us to understand more about the role played by SOC reports.

1. *The effect of SOC reporting on service organizations: As SOC reporting is not mandatory, researchers may be interested in what factors motivate a service organization to obtain SOC assurance and how it chooses over different types (SOC 1, SOC 2, and SOC 3) and levels (Type 1 and Type 2) for their system controls.*
2. *The effect of SOC reporting on user entities: As service providers' control will affect the security risk of user entities and further influence the business risk, whether user entities are aware of the importance of obtaining SOC reports from service providers and select those with SOC assurance becomes a substantial issue to their shareholders. In addition, it is still unclear whether obtaining SOC reports from service providers is an important factor for user entities' financial statement auditors to assess control risks and how the reports are used.*
3. *The quality of SOC reporting: While PCAOB monitors and evaluates the quality of financial statement audits, there are no existing institutes or mechanisms to assess the quality of SOC reporting and the service auditor's auditing process and opinions. Several factors may affect the quality of SOC assurance, including the competence or experience of the service auditor. Especially, while the use of SOC 1 and SOC 2 is limited and cannot be obtained by outsiders, it is more difficult to evaluate the quality of SOC assurance.*

As more organizations outsource their business information processes or functions, such as cloud computing and storage, third-party data centers, and digital asset guardians, to third-party service providers, the reliance on third-party assurance over the system controls will also increase. This editorial briefly introduces SOC reporting to our readers and points out several possible research directions that may enhance our understanding of SOC reports.

References

1. Deloitte.Us-global-outsourcing-survey (2022)
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-global-outsourcing-

survey-2022.pdf

2. *The AICPA Auditing Standards Board (ASB) completed its attestation clarity project with the issuance of SSAE No. 18, Attestation Standards: Clarification and Recodification.(2023) https://www.aicpa-cima.com/resources/download/aicpa-statement-on-standards-for-attestation-engagements-no-18*
3. The Meaning of SOC from the AICPA (2022) https://www.truvantis.com/blog/the-meaning-of-soc-from-the-aicpa
4. Here the service organization auditor indicates the auditor who provides assurance service for SOC, not the service organization's financial statement auditor.
5. Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting(2021) https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/at-c-00320.pdf
6. 2017 Trust Services Criteria (With Revised Points of Focus – 2022) (2023) https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022