Call for Papers from *Current Issues in Auditing*: System and Organization Controls (SOC) Services

The AICPA has a suite of System and Organization Controls (SOC) services that CPAs can perform for outsource service providers (service providers). The purpose of SOC services is to provide a service provider's clients (users) assurance about specified processes and controls of the service provider. SOC services typically result in the issuance of a report that is shared with users. Examples include SOC 1 services which can provide users assurance that the service provider's internal controls over defined control objectives and related financial reporting processes are suitably designed and are operating effectively; SOC 2 services which can provide users a report on controls relevant to security, availability, processing integrity, confidentiality and privacy; SOC for Cybersecurity which is intended to help organizations communicate information about the effectiveness of their cybersecurity risk management programs; and SOC for Supply Chain which is intended to provide assurance concerning an entity's controls for producing, manufacturing, or distributing goods to better understand the cybersecurity risks in their supply chains.

Despite the proliferation of outsourcing, the increasing exposure to cybersecurity risks, and an abundance of related auditing rules and initiatives (e.g., PCAOB AS 2601: *Consideration of an Entity's Use of a Service Organization*; AICPA tools to help assess cybersecurity risks; expanded testing of SOC services on the CPA Exam; and the CAQ's promotion of the role of auditors in company-prepared cybersecurity information), little is known about how auditors perform or rely on SOC services.

To address this knowledge gap, we are seeking submissions of short, well-written papers that investigate SOC services. Questions that might be investigated include, but are not limited to:

- How familiar are auditors with SOC services? How frequently are SOC services performed? Are special skills required to perform SOC services?
- How has the increase in outsourced processes impacted the work of auditors of users' financial statements? How do auditors determine if SOC 1 reports are required for their financial statement audits? What is the extent of reliance on SOC 1 reports? Do auditors play a role in determining the controls to be tested or the level of assurance to be obtained when they rely on SOC 1 services?
- How has the increase in the use of information technology and cybersecurity risks impacted the work of auditors? How do auditors determine if SOC 2, SOC for Cybersecurity, and SOC for Supply Chain reports are required? When are SOC 2 engagements preferred over alternative types of assurance (e.g., HITRUST)? What is the extent of reliance placed by auditors on SOC 2, SOC for Cybersecurity, and SOC for Supply Chain reports in connection with their financial statement audits?
- Does performing SOC services for a financial statement audit client enhance audit quality? Are there independence issues that should be considered when performing SOC Services?

Paper submissions

Paper submissions should follow the *CIIA* editorial policy and be submitted using the AAA's manuscript management system (https://aaahq.org/Research/Journals/Section-Journal-Home-Pages/Current-Issues-in-Auditing). If you have questions, please contact Co-editor Nicole Staats Wright at: wrightns@jmu.edu. **All manuscripts must be submitted by December 31, 2023.**