American Journal of Industrial and Business Management, 2026, 16(8), 922-931
https://www.scirp.org/journal/ajibm
ISSN Online: 2164-5175
ISSN Print: 2164-5167

System and Organization Controls

Cameron Fisher

New York, USA
Email: cafisher@mit.edu

How to cite this paper: Fisher, C. (2026). System and Organization Controls. *American Journal of Industrial and Business Management, 16,* 922-931.
https://doi.org/10.4236/ajibm.2026.168048

Received: July 29, 2026
Accepted: August 25, 2026
Published: August 28, 2026

Abstract

Critical digital services from third party providers increase firms' operational, security, and financial risks. The System and Organization Controls (SOC) framework is a standardized assurance approach intended to reduce information asymmetry between service providers and stakeholders. This paper brings together archival and experimental research on SOC and connects those findings to broader ideas in monitoring and governance. The goal is to show how SOC practices fit into firms' efforts to build operational resilience and stakeholder assurance. It also outlines several research designs, including event-studies, regulatory shock settings, and matched difference-in-differences approaches that future work could use to study the causal effects of SOC adoption. These contributions position the paper as a conceptual and practical roadmap for guiding subsequent research and applied investigations.

Keywords

Digital Service Provider, Information Technology, System and Organization Controls

1. Introduction

Modern firms increasingly place mission critical systems and data with third party providers, which raises their exposure to operational, security and financial risks. These relationships shift operational control outside the firm and create third- and nth-party risks that increasingly concern auditors and stakeholders.

Regulators have emphasized cyber risk as a systemic concern. As Chair Powell (2021) observed, "The risk that we keep our eyes on the most now is cyber risk." This paper examines SOC assurance as one governance mechanism firms use to manage third-party exposures.

This concern motivates standardized assurance mechanisms such as SOC re-

porting using AICPA standards, to provide objective evidence about provider controls over availability, confidentiality, processing integrity, privacy and security.

This article (1) defines SOC reporting and its variants, (2) synthesizes archival and experimental evidence on adoption, and (3) proposes identification strategies to estimate causal effects and practical guidance for auditors, customers, regulators and service providers.

2. Background on SOC and Risk Management

SOC reports are a standardized assurance used by critical service providers such as AWS, Microsoft, Oracle, etc. These attestations are produced by AICPA qualified practitioners and vary by scope and audience.

SOC reports are heterogeneous. SOC 1 focuses on controls relevant to financial reporting; SOC 2 addresses operational trust services; SOC 3 is a public, summary version of SOC 2 for non-expert audiences. Type I reports attest to controls at a point in time; Type II reports attest to controls over a period of time. These distinctions shape the information content of the report and how issuers and recipients respond to it.

SOC attestations contain a matrix of control objectives with rows describing each control and columns showing the auditor's tests and results. In practice, this means the report reads like a detailed checklist. For each area (e.g., business continuity, change management, logical access, financial-relevant controls), the SOC auditor documents what the third-party service provider claims, how it was tested, and whether the control operated effectively.

Monitoring modalities for third party risk include remote standardized reports (SOC, ISO attestations), vulnerability scans, and when needed on-site inspections. The tradeoff between remote assurance and on-site inspections is central. Remote reports are scalable and standardized, but on-site visits provide richer, tacit information (soft signals) about culture, norms or asset specifics, that written reports cannot fully capture.

Table 1 summarizes the structures of SOC reports and distinguishes Type I and Type II.

Table 1. Types of system and organization controls reporting.

	SOC 1	SOC 2	SOC 3
Focus	Financial Reporting.	Security, processing integrity, availability, privacy.	Summary version of SOC 2 for Non-expert audience.
Access	User Auditor and User Controller's office.	NDA with management, regulators, others.	Publicly available.

Continued

Period	SOC 1 Type I financial audit at point in time. SOC 1 Type II financial audit period of time.	SOC 2 Type I compliance audit at point in time. SOC 2 Type II compliance audit period of time.	Distilled from same criteria and procedures as SOC 2. SOC examinations may be Type I or Type II, but usually Type II.
Reporting	Widely applicable standard to attest financial reporting per AICPA methods.	Widely applicable standard to attest system compliance (including details) per AICPA methods.	Used also by vendor to summarize and assure that SOC 1 and SOC 2 reliability.

Empirical studies complement this taxonomy: archival work maps adoption patterns and cost effects, while experiments probe stakeholder responses.

The literature on critical digital services (CDS) increasingly highlights the pivotal role of System and Organization Controls (SOC) assurance in mitigating third-party risk. The AICPA's guidance on SOC 1, SOC 2, and SOC 3 establishes a common framework that links control objectives (availability, confidentiality, privacy, processing integrity and security) to audit evidence, and has become the de-facto standard for providers such as AWS, Microsoft, and Oracle.

Empirical work by Schoenfeld (2024) demonstrates that approximately 30% of S&P 500 firms currently obtain SOC audits, yet the presence of a SOC is among the largest predictors of audit-related fee variation, underscoring the economic salience of this assurance mechanism.

Complementing this archival perspective, Perols (2025) finds that people respond more favorably to comprehensive SOC disclosures a when they follow a major incident. In contrast, proactive SOC reports tend to draw a more muted reaction, pointing to a timing-dependent signaling effect.

Theoretical foundations from signaling theory (Spence, 1973) explain why firms deploy SOCs to reduce information asymmetry and monitoring costs. Moreover, the media-richness lens highlights the trade-off between remote, standardized assurance and the richer, tacit information obtained through on‑site in-person examination.

Existing archival and experimental evidence shows that SOC assurance is associated with higher perceived resilience, improved stakeholder confidence, and changes in audit-related assessments. These studies identify relationships and stakeholder responses, but they do not establish that SOC adoption itself causes improvements in operational or financial outcomes.

2.1. Review Methods

The structured literature review occurred to identify archival and experimental studies relevant to System and Organization Controls (SOC) reporting. The bib-

liographic databases and sources include: Web of Science, Scopus, Google Scholar, SSRN, JSTOR, ProQuest, and AICPA guidance/trust center pages, using combinations of the keywords: "*SOC*", "*SOC* 1", "*SOC* 2", "*SOC* 3", "*system and organization controls*", "*third-party assurance*", "*third-party risk*", and "*assurance reporting*". Searches covered publications and working papers through July 2026. The database searches were supplemented with backward and forward citation searches of key papers (e.g., Schoenfeld 2024) and with practitioner materials (AICPA, n.d.).

2.2. Inclusion Criteria

The criteria for inclusion required that a study (a) empirically examine SOC reporting or closely related third-party assurance practices, or (b) experimentally tests stakeholder responses to SOC or comparable assurance disclosures, or (c) provides theoretical or practitioner guidance directly relevant to SOC reporting. Synthesized findings using a narrative, thematic approach. Studies were grouped by empirical design (archival, experimental, theoretical/practice), by outcome domain (market valuation, audit fees, procurement, operational resilience), and by SOC feature (SOC type, trust categories, Type I vs Type II). Where possible, tabulation occurred by study designs, data sources, and main results to highlight consistent patterns and gaps.

3. Signaling, Transaction Costs, and Media Richness

Three theoretical lenses clarify why firms obtain SOCs and how stakeholders respond.

3.1. Signaling Theory

SOC attestations function as observable signals of governance and control quality. SOC disclosure allows well-governed service providers and better-governed entities to distinguish themselves by making their controls and practices visible.

The credibility of that signal rests on auditor reputation and the scope of the examination. AICPA templates and certification practices standardize what is reported and how, which improves reliability, consistency, and comparability across issuers.

Service providers use SOCs to demonstrate their willingness and ability to submit systems and processes to independent assessment. Customer firms use SOCs to signal a commitment to their compliance. SOCs are increasingly minimum "table stakes", creating a barrier to entry for new or under-qualified entrants.

As organizations make large, complex IT investments to deliver critical digital services, SOC controls are increasingly essential for managing risk, and sustaining stakeholder trust. Taken together, these dynamics make SOC reporting an increasingly important assurance mechanism, especially as firms expand their AI-related infrastructure.

3.2. Transaction Costs

Outsourcing arrangements that involve high asset specificity (systems or investments tightly tailored to a particular provider), and high uncertainty tend to create conditions where opportunism is more likely. Williamson (1985) argues that these situations benefit from governance mechanisms that reduce information gaps and limit costly bargaining by third-party after the fact.

SOC assurance helps address these concerns by reducing information asymmetry and lowering the transaction costs of monitoring third-party performance. They complement contractual safeguards, contingency planning and, when needed, on-site verification. In this way, SOCs help firms manage the risks that arise when critical systems are entrusted to specialized external providers.

3.3. Media Richness

Different monitoring modalities vary in the richness of information they convey. On site visits and person-to-person interviews offer high-richness communication, conveying tacit knowledge and cultural context. In contrast, SOC reports provide low-richness, standardized, codified evidence suitable for scalable assurance.

The appropriate monitoring approach depends on the nature of the decision at hand. Routine, well-structured tasks may be adequately supported by standardized SOC reporting, whereas high-stakes, ambiguous or poorly structured risks often call for richer modalities. This contrast between on-site inspections and standardized SOC reports reflects Daft and Lengel's (1986) media-richness theory, which explains why richer communication channels convey nuanced tacit cues that lean, codified reports cannot.

4. Empirical Evidence and Adoption Patterns

Recent studies suggest the nature of demand and supply for SOC attestation.

4.1. Large-Sample Archival Evidence

Hand-collected SOC status and 10-K text for S&P 500 firms (2019) reveal that a substantial minority of large firms obtain SOCs and that business-model exposure to technology predicts SOC adoption. One finding from the Schoenfeld (2024) research explains: "29% of firms in the S&P 500 receive these audits." Moreover, the research finds that SOCs are associated with higher audit-related fees, higher attestation efforts and overall cost.

4.2. Experimental Evidence on Stakeholder Perceptions

A between-subjects experiment measured participants' confidence and perceived assurance quality. The experiment finds that investors value comprehensive third-party assurance when disclosed in response to a reported incident, However, SOCs proved less valuable when SOCs were proactively disclosed in absence of major incident. This pattern suggests SOCs function as a reactive signal that

reduces uncertainty after adverse events, whereas proactive disclosures may be expected and therefore discounted.

The experimental findings reported in Perols (2025) provide insights into how SOC assurance disclosures are perceived. The study uses a randomized, between-subjects experiment with 133 participants, each assigned to one of five treatment conditions that vary both the type of assurance and the presence or absence of a prior incident. Participants rate perceived assurance quality using seven-point scales.

The experiment provides associational evidence about stakeholder reactions rather than causal effects. When an incident precedes assurance, participants exhibit significantly higher willingness to invest in the more comprehensive SOC for security condition (mean = 5.54) compared with the less comprehensive vulnerability and penetration test (mean = 4.15, $p < 0.001$). As the study reports, "when a security incident precedes assurance, people are significantly more willing to invest ($p < 0.001$) in the presence of a more comprehensive SOC for security (5.54) than a less comprehensive vulnerability and penetration test (4.15)." In contrast, when no incident has occurred, the difference between the more comprehensive (mean = 5.60) and less comprehensive (mean = 5.35) assurance services is not statistically significant ($p = 0.168$).

These findings indicate a timing-dependent signaling effect. Comprehensive SOC disclosures are associated with stronger reactions when issued after an incident. These results reflect stakeholder perceptions and correlational patterns, not demonstrated causal improvements in resilience, financial performance, or audit effort. These findings motivate the causal identification approaches proposed below.

4.3. Limitations

Archival studies face omitted variable bias and reverse causality. Experimental results face external validity concerns because samples and vignette simulations vary from actual stakeholders' contexts. The two approaches are deemed complementary because archival work maps real-world adoption and costs, while experiments isolate signaling mechanisms.

5. How SOC Affects Stakeholders

SOC mechanisms influence three stakeholder groups differently:

5.1. Auditors

SOCs that document controls over data integrity and financial reporting relevant processes can change the scope of external auditors' procedures. Archival evidence indicates SOCs are among the largest predictors of variation in audit related fees, consistent with auditors allocating more effort when third-party controls are substantive, or when SOC reports require review and corroboration. The additional training and AICPA certification to produce SOC are also factors.

5.2. Customers

For buyer firms, SOCs reduce due diligence costs and can be used in vendor selection and contract negotiation. However, SOCs do not alleviate a need for complementary user entity controls. CUEC's are stipulated within SOC processes diligence, and internal monitoring. Moreover, the buyer retains partial responsibility for secure configuration and operational practices.

5.3. Service Providers

SOC disclosures are often viewed through the lens of incident timing and report comprehensiveness. After an incident, a SOC can reduce uncertainty about remediation and residual risk. Proactively disclosed SOCs may be anticipated and may have relatively muted effects.

6. Research Design and Identification Strategies

To move from association to causation, researchers need settings where SOC adoption changes for reasons outside the firm's control. I propose three complementary strategies.

6.1. Event-Study around Third-Party Outages

Sudden, unanticipated outages at major cloud providers (e.g., availability zone failures) can sharply change customers' perceptions of risk. If firms respond by disclosing SOCs, researchers can measure abnormal returns and liquidity changes around the shock event. To address anticipation, restrict the sample to firms with no prior public signals of SOC adoption and use matched controls.

6.2. Regulatory or Contractual Shocks

Changes in regulation (e.g., sectoral guidance requiring third-party assurance for critical workloads) or large customer procurement requirements can serve as instruments for SOC adoption. A difference-in-differences design comparing affected and unaffected firms before and after the shock can isolate causal effects on audit fees, disclosure practices, and market valuation. Difference-in-Differences compares how an affected group changes over time relative to a similar unaffected group, helping isolate the impact of a policy or event from background trends.

6.3. Matched Firm and Instrumental Variable Approaches

Use firm-level predictors of SOC adoption (technology exposure, vendor concentration, prior incidents) to construct propensity scores and match adopters to non-adopters. Where available, use instruments such as local auditor supply shocks (e.g., entry of SOC-qualified audit teams) or exogenous changes in vendor offerings, such as a major service provider begins to offer a new SOC package to identify causal impacts.

6.4. Data Needs

Hand-collected SOC indicators from filings and trust centers, incident logs, public breach databases, and procurement/contract disclosures are needed. The hand-collected indicators can also discern SOC content to measure scope and Type I versus Type II distinctions.

7. Policy and Practical Implications

7.1. Firms

Decide SOC scope and timing strategically. SOCs can be valuable after incidents to restore stakeholder confidence, but proactive SOCs may be anticipated and yield limited market benefit. Firms must balance transparency with confidentiality and operational risk. More granular disclosures can help customers and auditors but may reveal sensitive operational details.

7.2. Auditors

The practice of SOC assurance affects audit planning and evidence collection. Auditors should evaluate SOC scope, and complementary user entity controls (CUEC) when relying on third party reports. The additional audit effort associated with SOCs and the magnitude of fees suggests auditors are not simply rubber stamping the attestations.

7.3. Sourcing

Standardized assurance (SOC, ISO, ISAE) can reduce due diligence costs and harmonize expectations across jurisdictions. However, cross-border differences in auditing standards and national qualification regimes (e.g. AICPA standards) complicate global reliance on SOCs to-date. Auditing standards and qualifications vary internationally, which affects comparability and trust.

8. Extensions and Future Research

Three promising directions are highlighted below.

8.1. Heterogeneity by SOC Features

Disaggregate effects by SOC type (SOC 1 vs SOC 2 vs SOC 3), Type I vs Type II, and by the trust service categories tested (security, availability, processing integrity, confidentiality, privacy). Which trust elements drive auditor, customer, provider and stakeholder responses?

8.2. Interaction with Vendor Concentration and Criticality

If a firm relies on a single cloud provider for mission critical workloads, the value of SOCs and on-site verification differs from diversified vendor portfolios. Study how vendor concentration moderates SOC effects.

8.3. Market Outcomes beyond Stock Returns

Examine effects on insurance premiums, procurement outcomes, and operational resilience metrics (downtime, recovery time objectives, recovery point objectives, etc.). The presence or absence of SOC practices may affect contractual terms and insurance pricing.

9. Conclusion

SOC reports are a practical governance response to the growing reliance on critical digital services. Experimental evidence suggests that stakeholders may value SOCs especially when disclosed after major incidents. Archival evidence shows growing adoption among large firms.

When a firm's systems or equipment are entrusted to a supplier not easily moved, the prospect of switching becomes expensive and risky. In those situations, a standardized SOC report often will not show subtle, relationship-specific factors. To supplement relying on SOC, firms may need stronger protections, clearer contracts, and on-site inspections to detect issues that a remote standard report can overlook. Overall, the evidence reinforces that SOCs offer a meaningful, yet necessarily incomplete approach to managing third-party risks. SOCs reduce information asymmetry and monitoring costs but are less effective in situations where ambiguity and asset specificity are high.

SOCs are insightful for attesting operational rigor and process integrity. Complementary modalities may offer additional benefits when systems and organizations are highly complex, and the stakes of failure are high. Future empirical work should focus on causal identification, heterogeneity across SOC features, and consider, for example, if currently voluntary SOCs need to be mandatory, strengthened and simplified, especially as AI growth accelerates.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

AICPA (n.d.). *SOC for Service Organizations: Overview and Guidance.* American Institute of Certified Public Accountants.

Daft, R. L., & Lengel, R. H. (1986). Organizational Information Requirements, Media Richness and Structural Design. *Management Science, 32,* 554-571. https://doi.org/10.1287/mnsc.32.5.554

Perols, J. L. (2025). How Do Investors Perceive System and Organization Controls (SOC) for Cybersecurity? *Current Issues in Auditing, 19,* P60-P66.

Powell, J. H. (2021). *Press Conference Following the Federal Open Market Committee Meeting.* Board of Governors of the Federal Reserve System. https://www.federalreserve.gov/mediacenter/files/FOMCpresconf20210428.pdf

Schoenfeld, J. (2024). Cyber Risk and Voluntary Service Organization Control (SOC) Audits. *Review of Accounting Studies, 29,* 580-620.

https://doi.org/10.1007/s11142-022-09713-0

Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics, 87,* 355-374. https://doi.org/10.2307/1882010

Williamson, O. E. (1985). *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting.* Free Press.