

Non-Financial Audits: Evidence from the Technology Sector*

Jordan Schoenfeld
Dartmouth College

July 2020

Abstract

A modern firm has many types of stakeholders, each of whom interacts with different parts of the firm. While financial audits are useful for some stakeholders, other stakeholders may benefit from supplemental audits of other parts of the firm (“non-financial audits”). This study provides some of the first large-scale evidence on such audits. Using hand-collected data from public companies, I find that the large audit firms are often hired to evaluate internal controls over technology systems. The audit reports are meant for a company’s customer market, and the scope of these audits typically includes controls over data security, processing integrity, and privacy. In addition, a company’s business-model reliance on technology is predictive of its decision to receive these audits, and these audits are associated with a large increase in audit-related fees that is economically significant when compared to the fees for other corporate accounting services. These findings highlight the importance of non-financial audits in our attempts to understand the market for audit services.

Keywords: Audit; big data; internal control, technology

JEL Classification: M40, M49, O33

*I appreciate the helpful comments from Sarah McVay, Mike Minnis, Nemit Shroff, and seminar participants at the Accounting Insights Webinar and Columbia Business School. Corresponding author: Jordan Schoenfeld, Dartmouth College, Hanover, NH 03755; e-mail: jordan.m.schoenfeld@tuck.dartmouth.edu; tel: (440) 759-2506.

1 Introduction

A modern firm has many types of stakeholders, each of whom typically interacts with a different part of the firm’s business model. For example, customers may be more interested in the firm’s product safety and privacy, employees may be more interested in career advancement opportunities offered by the firm, and investors may be more interested in maximizing the returns on their financial investments in the firm. While financial audits of the firm are useful for some stakeholders, these audits are generally based on a predetermined set of procedures and provide only a coarse signal of a qualified or unqualified opinion. The theoretical reason for this is articulated in Kreps (1990, p. 763-764), who argues that certifying to a coarse rule enables auditors to maintain their reputation in a repeated game setting despite constantly changing business conditions. As a result, there may be a demand by diverse stakeholders for supplemental audits of other parts of the firm (“non-financial audits”). In fact, these types of audits are routinely performed by the large audit firms. However, despite their theoretical importance, accounting audit research has largely not studied these audits (e.g., DeFond and Zhang, 2014; Knechel and Willenborg, 2016).

To better understand the scale and scope of non-financial audits, it is necessary to assess the existence, and potential importance, of these types of audits. This study therefore provides some of the first large-scale evidence that robustly shows that non-financial audits performed by the large audit firms play an important role in a key setting, namely evaluating the internal controls over companies’ technology systems. This market for audits is important for several reasons. First, technology is now ubiquitous: by one account, 98 percent of companies use at least one “big data” service (Dell, 2020). Second, the audits examined in this study are distinct from financial audits. For example, weak data security protocols at a company do not directly impact a financial account. Third, the Securities and Exchange Commission (SEC) recently expressed concern over the security of prominent enterprise

technologies.¹ These institutional considerations reinforce the theory in Kreps (1990) that financial audits may not meet the needs of all stakeholders.

I begin by assembling one of the first datasets of Service Organization Control (SOC) audit reports for all S&P 500 corporations in 2019. SOC audit reports are documents that are separate from financial audit reports, and the term *service organization* simply refers to any company that uses technology in its service offerings (banks, cloud computing companies, etc.). Unlike financial audits, SOC audits are not mandated by explicit legislative provisions. Section 2 elaborates further on the AICPA’s SOC audit framework.

Given the paucity of SOC audits in the literature, it is helpful to have some context for how the scope of these audits compares to the scope of financial audits. I therefore use a novel feature of my data, namely that SOC audit reports often list the internal controls tested by the auditor, to analyze the types of internal controls evaluated in SOC audits. I find that the scope of these audits typically includes controls over data security, processing integrity, and privacy. For example, Amazon receives SOC audits from Ernst & Young for Amazon Web Services (AWS).² For its SOC audit, AWS identified 114 services, 88 geographical regions (physical technology is often distributed geographically), and 92 critical internal controls as in-scope for the audit. These controls represent many processes within AWS, including cryptographic data transfers, software development, and assessments of security threats such as hacking. Section 4 provides a more systematic analysis of these results for the full sample.³

With this evidence demonstrating the scope of SOC audits, I next assess a company’s decision to receive a SOC audit. Using a combination of cross-sectional firm-level data, I hypothesize and find that a company’s business-model reliance on technology is predictive

¹See <https://www.sec.gov/ocie/announcement/risk-alert-network-storage>. Echoing the SEC’s concerns, many economists have argued that corporate technology systems necessitate independent audits (e.g., Acemoglu et al., 2019; Mullainathan, 2019).

²AWS stores and processes data for many businesses through its pay-as-you-go cloud platform. Amazon’s 2018 10-K notes that AWS generated about \$26 billion in revenue and \$7 billion in operating income, representing about half of Amazon’s total operating income for that year.

³As Section 4.1 explains, the framework for evaluating controls in financial audits is generally based on the Internal Control–Integrated Framework developed by the Committee of Sponsoring Organizations (COSO), which does not encompass such technology controls (e.g., Altamuro and Beatty, 2010, Section 2.1).

of its decision to receive a SOC audit. To construct measures for this demand, I employ a linguistic measure derived from the annual report, and a variety of industry indicators and other relevant company attributes. I then use a firm’s SOC audit decision to examine whether audit fees vary as a function of these audits. In the most stringent specification, I include fixed effects, firm size, business segment counts, and other firm-level variables known to be associated with audit fees. I document a very robust positive relationship between audit fees and SOC audits, suggesting that SOC audits are a key component of the market for audit services. Specifically, SOC audits are associated with a \$900,000 or 70 percent increase in audit-related fees per year.⁴

To gauge the magnitudes of these effects, I then relate the \$900,000 average fee for SOC audits to several well-researched accounting services. I find that the average company pays accounting firms about \$330,000 per year for tax planning services (De Simone et al., 2015, p. 746). In addition, Sarbanes-Oxley internal control audits have been estimated to cost about \$73,000 per year for the average firm exempt from this regulation (Ge et al., 2017, Section 4). Furthermore, assuming that the average blended hourly billing rate for SOC audits is about \$300 (De Simone et al., 2015, p. 746), the \$900,000 in additional audit-related fees per year translates to 3,000 billable hours for a SOC audit. Taken together, these findings suggest that SOC audits are highly economically significant when compared to other corporate accounting services.

I next assess audit firms’ legal standing in this setting and how auditors potentially acquire technology expertise. Although SOC audits must be performed by CPA-licensed firms, passing the CPA exam would likely not be sufficient to perform these audits. Indeed, many audit firms directly educate their staff in technology and employ technology consultants on their audit teams. For example, Deloitte’s Cloud Institute is widely used by its workforce,

⁴Audit-related fees are distinct from any tax and technology consulting fees paid to an audit firm, which are included in different line items on the proxy statement (e.g., De Simone et al., 2015). See Section 4.2 for more detail on this point.

and Ernst & Young offers an in-house “Tech MBA” to its staff.⁵ It is also imperative that one not think of auditors as being technologically superior to management in this setting; rather, auditors’ expertise is in *evaluating* controls (see Appendix A for an example). Just as management is the expert on their own financial statements, management is the expert on their own technology, and it is their responsibility to implement good controls over it. Moreover, just as financial audits do not guarantee against fraud and misstatements, SOC audits do not guarantee against data breaches and other technology failures, and audit firms typically cannot be held liable for such events. It is also implausible to expect to observe whether companies confidentially hire audit firms to perform other types of technology audits. Thus, my evidence on the prevalence of non-financial audits is conservative as it pertains only to SOC audits. Section 5 elaborates further on these points.⁶

This study makes several contributions to the literature. A longstanding theoretical proposition is that audits facilitate relationships between the firm and its stakeholders by mitigating agency problems such as information asymmetry between these entities (e.g., Jensen and Meckling, 1976, Section 2.4; Watts and Zimmerman, 1983, p. 615). However, the empirical audit literature focuses almost exclusively on financial audits that are meant mainly for investors (e.g., DeFond and Zhang, 2014; Knechel and Willenborg, 2016).⁷ This study supplements that research by providing some of the first evidence on non-financial audits in the setting of U.S. public firms. In contrast to financial audits, the SOC audits in my setting are meant mainly for the client’s customer or user markets. Section 2 provides direct evidence on this point.

This study also contributes to the literature on internal control audits. Although accounting textbooks emphasize that internal controls can play an important role in many parts of a firm’s business model (e.g., Knechel and Salterio, 2016), prior research focuses

⁵For more information on these programs, see <https://www2.deloitte.com/us/en/pages/technology/solutions/cloud-computing-training.html> and https://www.ey.com/en_gl/news/2020/06/ey-announces-first-ever-virtual-corporate-mba-free-to-all-ey-people.

⁶Section 4.4 also relates SOC audits to the quality of the client’s financial internal controls.

⁷For example, see Kausar et al. (2016), Mansi et al. (2004), Weber and Willenborg (2003), and Willenborg (1999). Exceptions include Dufflo et al. (2013, 2018), who examine corporate environmental audits in India.

mainly on the audits of internal controls in the financial reporting process. However, there are substantive differences in the economics of SOC audits and financial audits. Perhaps most notably, unlike financial internal control audits, SOC audits do not center on the financial reporting process, are not performed in accordance with GAAS, and are not explicitly mandated by legislation.⁸ Rather, SOC audits are focused on a company’s technology product offerings and performed in accordance with their own professional standards set by the AICPA. Moreover, SOC audits are meant for a different audience than financial audits. As a result, it is not surprising that SOC audits differ from financial audits in their prevalence and scope. Also, SOC audits are routinely accompanied by significant detail on the exact tests performed by the auditor and the outcomes of those tests, which is not a common feature of financial audits.

In addition, because SOC audits are not mandated by explicit legislative provisions, my findings illustrate some of the market frictions (i.e., supply and demand factors) associated with these audits. Such findings for audit services are rare for public firms that, in the well-researched setting of financial audits, exhibit no variation in the choice to receive or not receive an audit (e.g., Gerakos and Syverson, 2015). Over the coming years, SOC audits may play an increasingly important role in the audit market. For example, corporate use of cloud computing providers (a key recipient of SOC audits) is forecasted to increase dramatically (Gartner, 2019). Another driver of growth in SOC audits may be compliance risks created by new regulations. For example, California and Europe recently implemented new data security laws, and the Department of Justice, the Federal Trade Commission, and several other regulators are currently debating similar laws (Schechner and Pop, 2020; Stupp, 2019; Wakabayashi, 2018). SOC audits may also become entwined with the emerging practice of taxing digital revenues based on where data are processed (e.g., Govindarajan et al., 2019).

The remainder of this study is organized as follows. Section 2 motivates the institutional setting and hypotheses. Section 3 discusses the data. Section 4 provides the empirical results.

⁸Nonetheless, depending on a company’s business model, companies that do not receive a SOC audit may be penalized by the customer market by way of lost sales. See Section 2 for more detail on this point.

Section 5 compares SOC audits to financial audits. Section 6 concludes.

2 Institutional background and hypothesis motivation

As background, it is helpful to have some context for the broader market for audits. A theoretical reason for audits is expressed in Jensen and Meckling (1976, Section 2.4), who argue that audits can help verify and add credibility to management’s provision of information about their business model, thereby making this information more valuable to its recipients. The most visible and well-researched audit setting is financial audits, which is likely a result of legislative provisions that mandate financial statement audits. While financial audits of the firm are of interest to some stakeholders, these audits are limited to the financial reporting process and provide only a coarse signal of a qualified or unqualified opinion. Kreps (1990, p. 763-764) argues that committing to release such a coarse signal enables auditors to maintain their reputation and independence in a repeated game setting despite ever-changing business conditions. As a result, there may be a demand by diverse stakeholders for supplemental non-financial audits of other parts of the firm.

In my setting, companies that sell technology as a service typically have complex internal controls over their systems. Due to agency problems such as information asymmetry, a company’s assertions about these controls may not be directly verifiable or understood by such stakeholders as the customer market. As a result, these companies routinely receive SOC audits that evaluate these controls (I discuss the audit framework shortly). For example, the company Oracle operates a business model that derives value from its customers’ willingness to transfer large amounts of sensitive data to Oracle’s servers for processing. Accordingly, Oracle’s customer agreements and website make many assertions regarding the integrity of its systems, and Oracle receives SOC audits of these assertions. Attesting to the importance of this audit in the customer market, Oracle’s website states that its SOC audit “promotes trust and builds confidence in third-party service provider relationships.” Several other companies

operate similar business models and receive SOC audits, including Amazon, Google, and Salesforce. Even banks such as Goldman Sachs receive SOC audits (investment banks often store their clients' proprietary trading algorithms). This is unlike, for instance, a mining company that requires comparatively less of its customers' data to operate.

Since SOC audits are relatively new to the literature, I next briefly describe the AICPA's framework for these audits. The SOC audit framework first emerged in 2011 from the AICPA's release of SSAE 16, *Reporting on Controls at a Service Organization*, and was significantly revised in 2017 by SSAE 18 and the AICPA's Trust Services Criteria (TSC).⁹ The term *service organization* simply refers to any company that uses technology in its service offerings (banks, cloud computing companies, etc.). The customers of such service organizations are referred to as "user entities" in the AICPA's standards. Under the SOC framework, SOC audits must be performed by a CPA firm based on SSAE 18 and the TSC.¹⁰ As defined in the bullet points below, the TSC are criteria for attestation engagements that evaluate the internal controls over the security, availability, processing integrity, confidentiality, and privacy of technology systems (Table 1 expands on these definitions):

- "Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- Availability. Information and systems are available for operation and use to meet the entity's objectives.
- Processing integrity. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

⁹Before 2011, audit firms often used Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, as a framework for their internal control audits over technology systems. However, the SAS 70 guidance applied only to controls that may impact the financial statements of a service company's *customers*, and not to other controls that may affect the integrity of technology systems (like SOC audits, SAS 70 audits are not systematically made public and have received limited research attention). Thus, due to the absence of a better standard, audit firms were improperly using SAS 70, and companies used terms such as "SAS 70 certified" to indicate that their technology controls were audited (AICPA, 2011). This confusion led the AICPA to create the SOC framework.

¹⁰The AICPA's Assurance Services Executive Committee (ASEC) created and implemented the TSC framework following standard due process procedures, including soliciting public comment on the proposed criteria. The TSC framework complements the Internal Control-Integrated Framework created by COSO, which centers on the controls over the recognition of revenues and expenses.

- Confidentiality. Information designated as confidential is protected to meet the entity’s objectives.
- Privacy. Personal information is collected, used, retained, disclosed, and disposed to meet the entity’s objectives.” (AICPA, 2017)

The TSC elaborates further on issues such as logical and physical access controls, system operations, change management, and risk mitigation. At the discretion of a company’s management, these controls can be evaluated by the audit firm (1) across an entire company, (2) at a specific subsidiary or operating unit of a company, (3) for a specific business function in a company, or (4) for specific technology systems in a company. This approach differs from financial audits, which are typically required to evaluate all material financial reporting aspects of a company. The TSC framework was designed such that it can accommodate different types of business models. For example, a telecommunications company may have a variety of critical internal controls over physical infrastructure that need to be evaluated, whereas other companies may have no such infrastructure.

SSAE 18, the TSC, and the AICPA’s Attestation Standards Section 101 set the groundwork for audit firms to issue three types of SOC audit reports. The first is a SOC 1 audit report, which evaluates a company’s technology internal controls that are relevant only to its *customers’* financial statements. These reports are useful when a company processes financial information such as tax or payroll data for its customers (Automatic Data Processing, or ADP, is a well-known example of this).¹¹ The second type of report is a SOC 2 audit report, which evaluates a company’s technology controls using the broad set of TSC standards (security, availability, processing integrity, confidentiality, and privacy). The third type of report is a SOC 3 audit report, which is meant for audiences who need assurance on SOC 2 controls but do not require all the supporting evidence in those reports (see Ap-

¹¹It is important to emphasize that the internal controls evaluated for SOC 1 audits differ from the controls evaluated for financial audits in that the former apply to the client’s *customers’* financial statements (not to those of the client). To illustrate, consider the case of a company that processes its payroll using ADP’s software platform. The security controls over this platform may not necessarily directly (and materially) impact ADP’s financial statements, but likely will impact its customer’s financial statements. Therefore, ADP’s SOC 1 audit would evaluate the security controls over this platform, whereas its financial audit may not. Section 4.3 directly tests whether SOC audit work complements or substitutes for financial audit work.

pendix A for an example). Note that similar to financial audits, the controls that are in scope for SOC audits are determined by management. Table 2 summarizes the types of SOC audit reports.¹² Due to the data limitations discussed in Section 3, the subsequent analyses often do not differentiate between SOC 1 and SOC 2 audits. Although this masks some of the audit heterogeneity, both types of audits are meant to provide assurance on technology controls and are equally relevant to the main hypotheses that follow.

At the conclusion of a SOC audit, the audit firm renders an opinion on the fairness of the client’s description of its controls and whether these controls are designed and/or operating effectively. The report is effective as of a specific date or over a date range. As with financial audits, auditors performing SOC audits obtain evidence using a variety of sampling and verification procedures. In addition, if an audit firm does not design or operate SOC-related controls at a client, it is appropriate for that audit firm to perform both a financial audit and a SOC audit at that client. Alphabet and Amazon, for example, use Ernst & Young for their financial audit and SOC audit, whereas other companies vary their auditors.

With this institutional background established, I turn to the empirical analysis. A complete empirical model of SOC audits would explicitly account for how all firms, SOC auditors, and other stakeholders such as customers match with each other. This study does not build such a model, but instead examines the nature of SOC audits based on firm-level attributes and other factors motivated by prior research. This approach is common in the financial audit literature, where the underlying market for firms, financial auditors, and investors is often left unmodeled (e.g., DeFond and Zhang, 2014; Knechel and Willenborg, 2016). I next relate my study to this literature.

Prior accounting audit research focuses mainly on the financial reporting process. With respect to internal controls in this setting, Ge et al. (2017) estimate the fees of internal control audits mandated by the Sarbanes-Oxley Act (SOX). Carnes et al. (2019), Hammer-

¹²For global context, SOC audits performed internationally follow the International Standard for Assurance Engagements (ISAE) 3402 framework, which was developed in cooperation with the AICPA and follows the same principles as SSAE 18 and the TSC. Just as in the U.S. market, the ISAE 3402 framework generates SOC 1, SOC 2, and SOC 3 audit reports.

sley et al. (2008), and Zhang (2007) examine whether investors perceive value in audits of and deficiencies in SOX-related controls. Cheng et al. (2013), Feng et al. (2015), and Harp and Barnes (2018) find that effective SOX-related controls enhance corporate investment, operating efficiency, and acquisition decisions, respectively. Coates and Srinivasan (2014) and Roychowdhury et al. (2019, Section 2) further survey this literature and conclude that effective SOX-related controls and unqualified SOX audit opinions generally have positive effects on firms. Beyond the setting of financial reporting, there is very limited research on the existence and scope of audits performed at public companies.

In my setting, the extent to which audit firms can audit internal controls over technology depends on their domain expertise and competencies in this area. From an economic perspective, the incentive to achieve competitive advantages and increase fees, coupled with the demand for audits arising from diverse stakeholders, has spurred audit firms to develop a variety of audit specializations and expertise (e.g., Johnson and Lys, 1990; Minutti-Meza, 2013). Indeed, as mentioned in Section 1 and discussed further in Section 5, many audit firms now directly educate their staff in technology and use technology consultants on their audit teams. As a result, there is ample reason to believe that audit firms can acquire both technical expertise in the SOC audit standards and independence from management to be able to objectively perform effective SOC audits. My first assumption is that these audits in fact evaluate technology-related internal controls. I test this assumption using descriptive analyses:

Hypothesis 1: *SOC audits evaluate internal controls that are critical to the client's technology service products.*

Next, for financial audits of public firms, explicit regulatory mandates requiring these audits eliminate variation in their prevalence, so there is no path to examine why a public firm does or does not elect to receive a financial audit (e.g., Gerakos and Syverson, 2015). This is not the case for SOC audits; instead, management's decision to receive a SOC audit is likely driven by their choice to enter certain product markets and the competitive forces

in these markets. That is, depending on a company's business model, companies that do not receive a SOC audit may be penalized by the customer market by way of lost sales. For example, some customers may not entrust their data to companies without SOC audits (e.g., Redman and Waitman, 2020). In such settings where management's choice to receive audits is not explicitly mandated by legislation (e.g., private firms), researchers have sought to study the market frictions (i.e., supply and demand factors) that may be driving a firm's audit decision. In these studies, it is common to build reduced-form empirical models of the audit decision (Lennox and Pittman, 2011, Table 6; Minnis, 2011, Section 4.2). Given the lack of SOC audits in the literature, this is the approach that I take as well. These considerations lead to my second hypothesis:

Hypothesis 2: *The prevalence of SOC audits is significantly positively associated with companies whose business models rely crucially on technology and electronic data systems.*

To the extent the evidence for Hypothesis 2 shows that not all firms receive SOC audits, this would imply that some firms trade off the benefits of receiving a SOC audit against the fees for these audits (e.g., as in the audit cost-benefit framework of Simunic, 1980). Assuming audit firms are generating measurable fees from SOC audits, they will likely charge the client an amount that is based on the extent of the audit work, and that also compensates for engagement risks such as litigation exposure (e.g., Bell et al., 2001, 2008; Seetharaman et al., 2002) and reputational concerns (e.g., Skinner and Srinivasan, 2012; Weber et al., 2008). Alternatively, it is entirely possible that some of the SOC audit procedures are already accomplished as part of a financial audit, in which case the incremental fee for a company of having its financial auditor produce a SOC audit report may be small or immeasurable.¹³ Recent research suggests that audit fees are one of the best indicators of all these factors (e.g., Rajgopal et al., 2020). Thus, it is informative to examine whether SOC audits are associated with the audit fee environment, and how the fees for SOC audits compare to the fees for other well-researched accounting services such as financial audits and tax planning.

¹³Section 2 (p. 9) discusses the dual role an audit firm can play as a financial and SOC auditor.

This analysis can give insight into how much auditor effort goes into SOC audits, and how SOC audits shape the audit fee environment.

The above considerations lead to my third hypothesis:

***Hypothesis 3:** SOC audits are significantly positively associated with audit-related fees.*

3 Data overview

To assemble the sample of SOC audit reports, I focus on S&P 500 firms because the process of collecting SOC audit reports is very labor-intensive and time-consuming. The reason is that unlike financial audit reports, companies are not obligated by law to publicly release SOC audit reports, and these audit reports are not systematically collected by the SEC or other data providers. I therefore must hand collect the audit reports by directly contacting companies, and as discussed in the prior section, I must focus on a recent year because the current SOC audit framework has been in place only since 2017. For precedent on this approach in the early literature on financial audits, Frankel et al. (2002) and Simunic (1980) use one year of data due to the labor required to collect audit fees. When I began the data-collection process, the S&P 500 index accounted for about 80 percent of total market capitalization, indicating that these firms represent the overwhelming majority of public firms in terms of market value.

With the S&P 500 firms as of mid-2019 as my sample, I use the following procedure to determine whether a firm receives any type of SOC audit: (1) I directly use a firm's website to determine whether it makes a SOC audit report publicly available from 2018 onward, (2) if I find no SOC audit report in step one, I directly contact that firm's investor relations department and inquire whether it received a SOC audit from 2018 onward (or confirm that it did not). This approach resulted in an answer for all firms, with about 12 percent of the sample's SOC status determined in step one by way of a successful collection, and 88 percent of the sample determined in step two. To help insure against type I errors, I performed step

two on a sample of firms for which I had already determined the existence of a SOC audit in step one, and all these firms confirmed that they do indeed receive SOC audits.¹⁴

Importantly, the sample is large enough for reliable statistical analyses and represents a deep cross-section of firms that vary by industry, size, and other factors. Furthermore, Schoenfeld (2017, p. 57) notes that S&P’s decision to include a firm in its index is not strategic (index additions typically result from acquisitions or mergers of existing index firms), and does not reflect any private belief about that firm.¹⁵

I denote firms that receive SOC audits as “SOC Audit” firms. One potential limitation of the data is that although all firms communicated to me whether they receive SOC audits, some firms were more forthcoming with detail about their audit than others. In some cases, I obtained a company’s SOC audit report with all its accompanying detail. In other cases, I was only told by the company that it receives a SOC audit, or I was told that I would need to establish a customer account with the company to receive the SOC audit report in its entirety. In many of these instances, I could not obtain the SOC audit firm’s name or differentiate between SOC 1 and SOC 2 audits.

Due to the data limitations above, the subsequent analyses often do not differentiate between firms that receive SOC 1 and SOC 2 audits or their sub-types. Although this masks some of the audit heterogeneity, it is important to note that both SOC 1 and SOC 2 audits are meant to provide assurance on technology controls, and thus both types of audits are equally relevant to my main hypotheses. In addition, my approach of using a simple designation for firms that receive SOC audits mitigates the noise or measurement error that may arise if I were to use inexact or partial evidence to form tests that focus exclusively on the presence of either a SOC 1 or SOC 2 audit report. Future research may be able to further explore this issue.

¹⁴Such subsample analyses are also used by researchers in other settings, including venture capital investment (e.g., Kaplan and Strömberg, 2003, 2004), debt contracts (e.g., Roberts, 2015; Roberts and Sufi, 2009; Smith and Warner, 1979), shareholder contracts (e.g., Schoenfeld, 2020), and supplier contracts (e.g., Costello, 2013; Joskow, 1987). See footnote 19 for the applicability of my findings to firms outside the S&P 500 index.

¹⁵For additional detail on the index, see <http://us.spindices.com/indices/equity/sp-500>.

After assembling the sample, I link each firm to data in Compustat and Audit Analytics. I also construct a firm-level business-model data exposure measure using a firm’s most recent annual report as of mid-2019, computed as each annual report’s frequency count of the terms *analytics*, *big data*, *cloud platform*, *database*, *digital*, and *digitization*, divided by the total number of words in the annual report. I then denote firms as being data exposed if their value for this measure falls in the top tercile of the sample. In generating this measure, I use all sections of the annual report because Loughran and McDonald (2016, Section 2.1) emphasize that parsing annual reports by sections can create “systemic errors” given the inconsistencies in how firms use section headers and HTML/XML tags. More important, based on a manual reading of several annual reports, information on firms’ business-model exposure to data can appear in many sections of these reports. The variables are described further in Section 4 and Appendix B.

4 Empirical results

4.1 Hypothesis 1: The scope of SOC audits

Given the lack of SOC audits in the literature, Hypothesis 1 examines the scope of the work performed by audit firms in SOC audits.¹⁶ This hypothesis does not lend itself to hypothesis testing using standard econometric methods. Instead, the evidence for this hypothesis is based on the SOC audit reports and accompanying audit-level detail collected from the firms in the sample. Recall that a novel feature of SOC audit reports is that the audit opinion is often accompanied by a worksheet containing all the internal controls that managers identify as being in-scope for the audit, and descriptions of all the tests performed by the audit firm and the outcome of those tests (this differs from financial audits where we observe only the audit opinion).

¹⁶DeFond and Zhang (2014, p. 294) and Efendi et al. (2006) argue that we have limited research on auditors’ expertise and competencies in areas beyond financial audits.

Each control that managers identify as in scope for a SOC audit typically maps directly to one or more TSC (security, availability, processing integrity, confidentiality, or privacy) or common criteria (CC) that applies to all the TSC. For example, controls over user entities' passwords might map to TSC CC 1.1, which covers user access rights, and controls over user entities' cryptographic data transfers might map to TSC CC 6.1, which covers vulnerabilities of data and system components. In practice, a single in-scope control often maps to several different TSC, and may require an auditor to perform several different types of tests.

Based on the direct examination of the SOC audit reports in the sample, Table 3 documents the types of internal controls that managers commonly designate as in scope for their SOC audits. These controls pertain to the delegation of authority over data-related processes, physical and virtual access rights over data, cryptographic and encryption protocols, network security configuration, external vulnerability threats, vendor policies, data storage, login protocols, and coding environments. In a SOC audit, all these controls would be tested by the audit firm. I next briefly discuss a few of these controls.

Consider internal control three in Table 3 over cryptographic custodians. Data encryption is a security process whereby data are encoded using an encryption key, thereby rendering the data scrambled or useless to any entity without the correct decryption key. Data encryption as a security device is only as good as the security used to protect decryption keys. As a result, decryption keys are often known by a small number of cryptographic custodians, and the decryption keys and custodians are often cycled out every few months. A strong key management system includes policies on the key lifecycle (e.g., generating, using, storing, and retiring keys) and physical and logical access to the key servers. In one SOC audit report from the sample, the auditor tested the controls over cryptographic custodians by inquiring of the cryptography manager that the roles and responsibilities for cryptographic custodians were formally documented and agreed to by those individuals. The auditor then selected a sample of employees from the group of cryptographic custodians, evaluated their access to systems that store or use encrypted data, and reconciled their inspected roles and

responsibilities to internal company policy and documentation.

Next, consider internal control four in Table 3 over two-factor authentication. Two-factor authentication ensures that users attempting to access an account are who they claim they are, and is usually implemented using a cellphone application, USB drive, fingerprint, or voice scan. In one SOC audit report from the sample, the auditor tested this control by interviewing system managers to ensure that the client requires users to use two-factor authentication to access the network. Then, the auditor inspected the authentication configuration to determine that authentication to the firm’s internal network from remote locations required two-factor authentication. Then, the auditor attempted to login to the client’s network from a remote location and determined that a physical token and password were required to access the client’s network. In another control related to login, the auditor inspected the system configurations, observed an engineer attempt to login to a physical host without the appropriate access, tested a large sample of logins to physical hosts, and inspected the client’s firewall settings to ensure it was operational.

Next, consider internal control 16 in Table 3 over maintaining separate production and development coding environments. Developing software is a continuous process, and the main reason to not mix the production and development coding environments is that development requires testing and debugging. One wrong line of code can disable an entire enterprise system. In one SOC audit report from the sample, the auditor tested this control in a few ways. First, the auditor interviewed software managers to ensure the client had policies in place to maintain separate coding environments for production and development. Then, the auditor selected a large sample of coding changes migrated from the development environment to the production environment and inspected the deployment channels to determine whether the production and development environments were in fact kept separate.

I next use Amazon and Google as short case studies. Both firms receive a SOC audit from Ernst & Young for several of their services across many geographic regions. A user familiar with Amazon Web Services (AWS—Amazon’s cloud service) would recognize many of these

services. For example, among 114 service lines, AWS’s popular Elastic Compute Cloud (EC2) is included, as are its data storage services Glacier and Simple Storage Service (S3). Google likewise receives a SOC audit of Gmail, Google Calendar, and Google Cloud, among many of its other services. Other companies in my SOC audit sample include Facebook, Goldman Sachs, Oracle, and Salesforce.

To further put the internal controls evaluated during SOC audits in perspective, Figure 1 provides a word cloud that illustrates the terminology in the corpus of the SOC audit reports that I obtained. I apply this procedure to the list of SOC internal controls identified by management and tested by the auditor. I include only the top 40 words and omit common stop words such as *and* and *the*. The word sizes are proportional to their frequency in the corpus of the SOC audit reports. Consistent with the prior evidence, Figure 1 shows that the words *access*, *customer*, and *data* occur the most frequently in the reports. Other words such as *key* and *security* are also commonly used in the reports.

Overall, the evidence in this section is consistent with Hypothesis 1 that the controls evaluated for SOC audits relate to the client’s technology systems. The evidence also shows that SOC audits evaluate internal controls that differ significantly from the controls evaluated for financial audits. For example, the Internal Control–Integrated Framework created by COSO does not encompass the controls documented above (e.g., Altamuro and Beatty, 2010; Schroeder and Shepardson, 2016; Yoon et al., 2015).

4.2 Hypothesis 2: The prevalence of SOC audits

Hypothesis 2 predicts that a company’s decision to receive or not receive a SOC audit is driven mainly by the extent of the company’s technology service offerings to the customer market. To test this idea, I follow prior studies and analyze management’s decision to receive a SOC audit using reduced-form empirical models (e.g., Lennox and Pittman, 2011, Table 6; Minnis, 2011, Section 4.2). The aim of this analysis is to explicitly illustrate some of the supply and demand factors associated with SOC audits.

In this setting, firms that derive value from collecting and processing large amounts of sensitive data will likely need to design and enforce complex internal controls over data security and integrity, and provide assurance to stakeholders such as customers that these controls are designed and/or operating effectively. Thus, companies in technology and other data-driven industries are good candidates for SOC audits. By contrast, firms that do not collect large amounts of data (e.g., mining companies) may forego a SOC audit due to its cost. As a result, firms' industry classifications can be thought of as good proxies for managerial and customer demand for SOC audits.

Table 4 provides an industry breakdown of the prevalence of SOC audits. Consistent with the expectations above, about 62 percent of firms in the information technology industry (e.g., Salesforce) receive SOC audits. Other industries with a large fraction of firms that receive SOC audits include communication services (e.g., Facebook) at 48 percent, financials (e.g., Goldman Sachs) at 48 percent, and healthcare (e.g., United Health Group) at 30 percent. By contrast, SOC audits are relatively rare in the materials industry at 8 percent of firms, the utilities industry at 11 percent, and the energy industry at 11 percent.

Table 5 shows that overall, about 29 percent of firms in the sample receive SOC audits, and the firms that receive SOC audits are significantly larger and more data exposed than firms that do not receive SOC audits. To put these results in perspective, in other settings where management's decision to receive an audit is not explicitly mandated by legislation, about 23 percent of private firms choose to receive financial audits (Minnis, 2011, Table 3), and 13 percent of SOX-exempt firms elect to receive audits of internal controls over financial reporting (Ge et al., 2017, Section 3). Firms that receive SOC audits also have significantly lower leverage and more current assets as a proportion of overall assets. The full sample is relatively comparable on the dimensions of ROA and business segments. There are also significant differences in audit and audit-related fees across companies that receive SOC audits versus those that do not (Section 4.3 examines audit fees in more detail).

Fully addressing Hypothesis 2 necessitates assembling many variables into a regression

framework because industry may be proxying for size and leverage or vice versa. Following prior research, I next construct a reduced-form empirical model of the probability that a firm receives a SOC audit conditional on several variables motivated by past studies and my institutional setting. Specifically, I include industry factors, firm size, and the variables from Table 3 of DeFond and Zhang (2014) that have been linked to other attributes of a firm’s audit environment, such as leverage and profitability (e.g., DeFond and Jiambalvo, 1991; Doyle et al., 2007; Hay et al., 2006; Kinney and McDaniel, 1989). To better accommodate fixed effects, I use linear probability models in this analysis, although all the results are similar in terms of statistical significance using logit and probit models. I specify the initial regression as follows:

$$\begin{aligned}
 SOC\ Audit_i = & \alpha + \beta_1 Industry_i + \beta_2 \text{Log}(Assets)_i + \beta_3 Leverage_i + \beta_4 Loss\ Firm_i \\
 & + \beta_5 ROA_i + \beta_6 \frac{Current\ Assets}{Total\ Assets}_i + \beta_7 Quick\ Ratio_i + \beta_8 Segments_i \quad (1) \\
 & + \beta_9 December\ YE_i + \epsilon_i,
 \end{aligned}$$

where index i represents the firm, $SOC\ Audit$ represents an indicator variable for whether firm i receives a SOC audit, and $Industry$ represents firm i ’s GICS industry or sub-industry depending on the test. Appendix B provides the exact formulas for all the variables.

Table 6, column 1 shows that including all the industry factors and the other variables explains about 20 percent of the variation observed in the prevalence of SOC audits. This finding compares well to Table 6 of Minnis (2011), whose model of the financial audit choice in private firms explains about 23 percent of the variation. Table 6, column 1 also shows that the prevalence of SOC audits is explained in part by firm size as measured by the log of total assets (1% level) and the ratio of current assets to total assets (10% level). Table 6, column 2 shows that after controlling for industry, SOC audits are significantly positively associated with firms whose business models are more data exposed (1% level). This finding suggests that business-model exposure to data (and not just a firm’s industry) is an important driver of SOC audits.

To further explore the association between SOC audits and firms' business-model exposure to data, I next regress the SOC audit indicator variable on the industry indicators one at a time, which lets the baseline probability of a SOC audit equal the average of the SOC audit variable after controlling for firm size and other factors. Table 6, columns 3 through 6 include the two largest positive and negative statistically significant coefficients from these tests. Table 6, columns 3 and 4 show that a firm is 37.4 percent more likely to receive a SOC audit if it is in the information technology industry, and 20.2 percent more likely to receive a SOC audit if it is in the financials industry (1% level for both). There is no significant result for the communications industry, which could be due to low power since this industry has only 23 firms in total. Table 6, columns 5 and 6 show that there is a negative association between SOC audits and the consumer staples industry at 20.5 percent (5% level), and the energy industry at 19.6 percent (5% level). These findings further support the idea that firms' business-model exposure to data is important in the SOC audit setting.

An advantage of using GICS industries is that they accommodate a variety of new sub-industries such as data processing. To further test Hypothesis 2, Table 7 regresses the prevalence of SOC audits on several sub-industries that likely derive value from sensitive data. As before, I insert the industry indicators one at a time. Table 7 shows that the prevalence of SOC audits is significantly associated with data processing services at a 47.2 percent increased likelihood (1% level), internet services and infrastructure at a 71.7 percent increased likelihood (1% level), application software at a 52.8 percent increased likelihood (1% level), investment banking at a 60.9 percent increased likelihood (1% level), internet marketing at a 57.2 percent increased likelihood (5% level), and information technology consulting at a 32.0 percent increased likelihood (10% level). The economic magnitude of the result for internet services and infrastructure is the largest among the industries and sub-industries, which attests to the ubiquity of SOC audits in this industry.

Overall, the evidence is consistent with Hypothesis 2, and robustly suggests that the demand for SOC audits arises mainly from industries that derive value from collecting and

processing data. Importantly, the magnitudes of these findings are economically meaningful, ranging from about a 20 to a 70 percent increase in the likelihood that a firm receives a SOC audit.

4.3 Hypothesis 3: SOC audits and the audit fee environment

Hypothesis 3 predicts that SOC audits are significantly positively associated with audit-related fees. The prior evidence for Hypothesis 2 demonstrates that not all firms receive SOC audits, which implies that for some firms, the fees for SOC audits outweigh their benefits. These fees are likely based on the extent of the audit work and engagement risks for which the auditor must be compensated. Alternatively, it is possible that some of the SOC audit procedures are already accomplished as part of a financial audit, in which case the incremental cost to a company of having its financial auditor produce a SOC audit report may be small. In any case, the magnitudes of any association between SOC audits and audit fees, and how they compare to the fees for other corporate accounting services, are ultimately empirical questions. These issues are important because they can provide insight into how SOC audits shape the audit fee environment and contribute to the market for audit services.

Specifically, I examine whether SOC audits are associated with audit fees and audit-related fees. Audit fees consist of fees paid to an audit firm for performing a financial statement audit. By contrast, audit-related fees consist of fees paid to an audit firm for audit services that are beyond the scope of a financial statement audit. Therefore, SOC audits should not be associated with audit fees unless the procedures for a SOC audit substitute for some of the financial audit procedures. There is some indirect evidence of this in Liu (2020), who finds that the quality of the financial audit is associated with the likelihood of a data breach at the client. There is also evidence of audit “spillover effects” in other settings (e.g., Bell et al., 2001, 2015; Davis et al., 1993; Lim and Tan, 2008; Palmrose, 1986; Simunic, 1984; Whisenant et al., 2003).

At the univariate level, Table 4 provides preliminary evidence that SOC audits are as-

sociated with audit fees. However, it is well established that firm size and other factors contribute to audit fees, and prior research has developed and relied on good empirical models for explaining audit fees. Specifically, Table 3 of DeFond and Zhang (2014) recommends several variables to include in an empirical model of audit fees. The subsequent audit fee regressions include these variables, industry-fixed effects, and the indicator variable for a SOC audit (I cannot include firm- and year-fixed effects given the sample’s composition).¹⁷ As in prior audit research, the key identifying assumption is that there is no systematic omitted factor that is significantly correlated with both SOC audits and audit fees (I cannot test this condition). Note that many other empirical designs such as propensity score matching are inappropriate for this setting (e.g., Gow et al., 2016; Larcker and Rusticus, 2010; Shipman et al., 2017). In addition, a feature of using the indicator variable for SOC audits is that it accommodates any non-linearities in the association between SOC audits and audit fees.

The initial audit fee regression is specified as follows:

$$\begin{aligned}
 \text{Log}(\text{Audit Fees})_i = & \alpha + \beta_1 \text{SOC Audit}_i + \beta_2 \text{Log}(\text{Assets})_i + \beta_3 \text{Leverage}_i \\
 & + \beta_4 \text{Loss Firm}_i + \beta_5 \text{ROA}_i + \beta_6 \frac{\text{Current Assets}}{\text{Total Assets}}_i + \beta_7 \text{Quick Ratio}_i \\
 & + \beta_8 \text{Segments}_i + \beta_9 \text{December YE}_i + \sum \beta_n \text{Industry FE} + \epsilon_i,
 \end{aligned} \tag{2}$$

where index i represents the firm, $\text{Log}(\text{Audit Fees})$ represents the natural log of financial statement audit fees from Audit Analytics, SOC Audit represents an indicator variable for whether firm i receives a SOC audit, and the industry-fixed effects represent the 11 GICS industries. The main coefficient of interest is β_1 . Following Ashbaugh-Skaife et al. (2007), DeFond et al. (2002), and Doyle et al. (2007), I control for log of total assets because smaller firms may require less audit work; leverage because debt may necessitate audit work around covenant compliance; ROA, loss firms, the ratio of current to total assets, and the quick

¹⁷I omit an indicator variable for going concern audit opinions because no firms in the sample receive these opinions. I also do not include the indicator variable for firms that are data exposed, as this would necessitate a structural path model given that business-model data exposure is a correlated channel for the demand for SOC audits in Section 4.2 (Greene, 2002, p. 397).

ratio because firms in financial distress may require more audit work; segments because more complex firms may require more audit work; and December fiscal year end. Appendix B provides the exact formulas for all the variables.

Consistent with there being no systematic spillovers between financial statement audits and SOC audits, Table 8, column 1 shows that there is no significant association between audit fees and SOC audits at conventional levels ($p > 0.1$). Nonetheless, the audit fee regression explains about 56 percent of the variation in audit fees, which suggests that this regression is well-specified (see Section 2.3.2 and footnote 42 of DeFond and Zhang, 2014). In contrast, regressions of commonly used measures of audit quality often explain about five to ten percent of the variation in these measures (DeFond and Zhang, 2014, Section 2.3.2).

I next examine the more likely candidate for capturing SOC audit fees, audit-related fees, which consist of fees paid to audit firms for audit services provided beyond the financial statement audit. Note that audit-related fees are distinct from any tax and technology consulting fees paid to an audit firm, which are included in different variables provided by Audit Analytics that draw from different line items on a firm's proxy statement (e.g., De Simone et al., 2015).¹⁸ To test whether SOC audits are associated with audit-related fees, I replace audit fees in Eq. (2) with audit-related fees as follows:

$$\begin{aligned}
 \text{Log}(\text{Audit-Related Fees})_i = & \alpha + \beta_1 \text{SOC Audit}_i + \beta_2 \text{Log}(\text{Assets})_i + \beta_3 \text{Leverage}_i \\
 & + \beta_4 \text{Loss Firm}_i + \beta_5 \text{ROA}_i + \beta_6 \frac{\text{Current Assets}}{\text{Total Assets}}_i + \beta_7 \text{Quick Ratio}_i \quad (3) \\
 & + \beta_8 \text{Segments}_i + \beta_9 \text{December YE}_i + \sum \beta_n \text{Industry FE} + \epsilon_i,
 \end{aligned}$$

where index i represents the firm, $\text{Log}(\text{Audit-Related Fees})$ represents the natural log of audit-related fees from Audit Analytics, SOC Audit represents an indicator variable for whether firm i receives a SOC audit, and the industry-fixed effects represent the 11 GICS industries.

¹⁸The ability to separate these fees is a relatively recent innovation driven by new regulatory mandates and large third-party datasets. In contrast, prior studies often aggregate all non-financial-statement-audit fees into one amount, making it difficult to disentangle the different services provided by audit firms (e.g., Frankel et al., 2002; Kinney and Libby, 2002; Whisenant et al., 2003).

The main coefficient of interest is β_1 , and I include the same control variables as in Eq. (2).

Table 8, column 2 shows that, as expected, SOC audits are significantly positively associated with audit-related fees (1% level). Specifically, I observe about a 69 percent increase in audit-related fees per year for firms with SOC audits after controlling for size, industry-fixed effects, and other factors. Table 8, column 3 shows that this finding translates to approximately \$900,000 in additional audit-related fees per year (1% level). To put the economic magnitudes of these results in perspective, Ge et al. (2017, Section 4) find that SOX audits are associated with about a 30 percent increase in audit fees per year. In addition, De Simone et al. (2015, p. 746) find that on average, companies pay accounting firms about \$330,000 per year for tax compliance and consulting services. De Simone et al. (2015, p. 746) also assume that the average blended hourly billing rate for these services is about \$300. Assuming that the average blended hourly billing rate for SOC audits is also about \$300, the \$900,000 in additional audit-related fees per year corresponds to approximately 3,000 billable hours for a SOC audit. Overall, these findings suggest that with respect to the audit workload and fee environment, SOC audits are highly economically significant when compared to other corporate accounting services.¹⁹

To further put the above results in perspective, Ge et al. (2017, Section 4) find that firms exempt from SOX internal control audits saved on aggregate \$388 million in audit fees from 2007 to 2014, which translates to about \$49 million per year on aggregate.²⁰ By comparison, if the 146 firms in the sample that receive SOC audits pay on average \$900,000 per year for these audits, firms in the S&P 500 alone spend about \$131 million on SOC audits *per year*

¹⁹Recall that as of mid-2019, the S&P 500 index accounts for about 82 percent of total market capitalization, and I code the SOC audit indicator based on information obtained directly from S&P 500 firms. It is an open question as to whether firms outside the S&P 500 receive SOC audits to a similar extent. Also, the industry-fixed effects represent the 11 GICS industries. I cannot include GICS sub-industry-fixed effects because among the 146 firms with SOC audits, 75 GICS sub-industries are represented, which precludes me from using a large part of the sample due to sub-industries with only one firm.

²⁰Ge et al. (2017, Section 4) estimate this value by multiplying the difference in the percentage growth in audit fees from 2003 to 2014 for SOX-exempt versus non-exempt firms by the mean audit fee for SOX-exempt firms, and then multiplying that value by 5,302, which represents the SOX-exempt firm-years in their 2007 to 2014 sample.

on aggregate.²¹ In addition, the average audit-related fee in the sample is about \$1.5 million, which suggests that SOC audits are an economically significant component of audit-related fees. These findings further corroborate the inference that SOC audits are valuable to firms and represent a key element of the audit fee environment.

4.4 Additional analyses

The next analyses are motivated by findings from prior audit research in different settings. I start by testing whether SOC audits are associated with the attributes of a company's financial audit. Managers responsible for the decision to receive a SOC audit may also oversee, or communicate with other managers who oversee, some of the internal controls over financial reporting. As a result, the prevalence of SOC audits may relate to the attributes of financial audits. For example, a firm with deficient internal controls over financial reporting may not seek a SOC audit for fear that it would raise more concerns and yield yet another unfavorable audit opinion. Such spillover effects are evident in other organizational settings such as corporate tax planning and financial reporting (e.g., De Simone et al., 2015; Francis, 2006; Gleason and Mills, 2011; Kinney et al., 2004). Table 9, columns 1 through 3 therefore regress the SOC audit indicator variable on indicator variables for whether a firm, in its most recent financial statement audit as of mid-2019, received a qualified opinion on its internal controls over financial reporting, a qualified opinion on its financial reports, or a qualified opinion on either its internal controls or its financial reports. After controlling for the variables in Table 6 and industry-fixed effects, Table 9, columns 1 through 3 show that there are no significant associations between the prevalence of SOC audits and deficiencies in financial audits. This finding suggests that a company's decision to receive a SOC audit is a process that is separate from its financial reporting choices.

I next test whether SOC audits are more prevalent in firms whose financial statements

²¹In a few instances, I find that firms footnote their SOC audit fees in their proxy statement or financial statements. For example, Google's parent company Alphabet paid about \$6.2 million for SOC audits in 2018 (Alphabet is a large provider of cloud computing and other technology services). However, not all firms break out their SOC audit fees in this way, necessitating the regression analysis.

are audited by the big four audit firms (Deloitte, Ernst & Young, KPMG, PwC). DeFond and Zhang (2014, p. 301) argue that given client heterogeneity, large audit firms likely have economies of scale and expertise in different domain areas (e.g., Aobdia, 2015; Haislip et al., 2016; Minutti-Meza, 2013). Thus, if any single audit firm is particularly competent in SOC audits, it may be more likely than other audit firms to suggest SOC audits to their financial audit clients, which could yield a correlation between a company’s financial auditor and its decision to receive a SOC audit. This issue is particularly salient in the SOC audit setting because an audit firm is typically permitted to perform both a financial audit and a SOC audit at a single client. Table 9, columns 4 through 7 therefore regress the indicator variable for a SOC audit on indicator variables representing a company’s financial auditor and the control variables from Table 6.²² I do not find significant coefficients for any of the individual audit firms, suggesting that no single audit firm systematically exerts outsized influence over a company’s decision to receive a SOC audit.

5 Comparing SOC audits to financial audits

As a final synthesis of the results, I next summarize the key differences between SOC audits and financial audits. Note first that SOC audit reports are completely separate from financial audit reports that opine only on the client’s financial statements and controls over revenue and expense recognition. As Section 4.3 shows, SOC audits do not reduce or substitute for auditor effort put toward a client’s financial audit, as measured by audit fees. Given this study’s focus and sample composition, I center the following analysis on the audit environment for public firms as opposed to private firms. Table 10 summarizes this discussion.

Conceptually, SOC audit reports and financial audit reports are similar in that both can be used to mitigate agency problems such as information asymmetry between firms and their

²²The big four audit firms perform financial audits at 491 of the companies in the sample. There is no significant association between SOC audits and big four versus non-big four audit firms (untabulated).

stakeholders (e.g., Jensen and Meckling, 1976, Section 2.4; Watts and Zimmerman, 1983, p. 615). However, unlike financial audits, SOC audits do not focus exclusively on the client’s financial statements. Moreover, although it is required that CPA-licensed firms perform SOC audits, a traditional training in accounting and passing the CPA exam would likely not be sufficient to perform these audits. Indeed, many of the large audit firms now educate their staff in technology. For example, Deloitte’s Cloud Institute is widely used by its workforce, and Ernst & Young offers an in-house “Tech MBA” to its staff (footnote 5 provides more detail on these programs). This may also help to explain why in 2018, non-accounting hires represented about 31 percent of all new graduate hires at large accounting firms, an 11 percentage point increase from 2016 (AICPA, 2019). As a result, there is ample reason to believe that audit firms can appropriately perform SOC audits. Of course, it is implausible to expect to observe whether companies confidentially hire audit firms to perform other types of technology audits. Thus, my evidence on the prevalence of non-financial audits is conservative as it pertains only to SOC audits.

SOC audit reports and financial audit reports are also similar in that they are likely of interest to multiple audiences or stakeholders. For example, financial audit reports are useful to shareholders, lenders, and regulators, among other entities. By comparison, SOC audit reports are useful to the customer markets and customers’ auditors. SOC audit reports may also be useful to companies attempting to demonstrate their commitment to their technology systems to attract new customers. With respect to the decision to receive a SOC audit, management may elect to receive SOC audits on their own, or they may do so only when demand for a SOC audit materializes from other stakeholders. Rather than construct explicit empirical path models for each of these mechanisms (Greene, 2002, p. 397), I primarily use a company’s business-model exposure to technology and data to proxy for management’s demand for SOC audits.²³

²³In the financial audit setting for public firms, explicitly modeling supply and demand mechanisms for audits is difficult because these audits are required by law. One solution is to build an analysis around a structural model, but this imposes strict identifying assumptions (e.g., Gerakos and Syverson, 2015). As a result, most studies take financial audits as given and examine their attributes and outcomes.

SOC audits and financial audits also yield similar types of audit opinions (unqualified, qualified, etc.). Moreover, just as financial audit reports do not guarantee against client fraud or misstatements, SOC audit reports do not guarantee against client data breaches and other technology failures. It is ultimately management’s responsibility to run their firm appropriately, and audit firms typically cannot be held liable for such events absent negligence on their part. In addition, SOC audits are not designed to advise a client on how to implement better controls to avoid technology failures; rather, the auditor’s expertise is in evaluating controls. In fact, as with financial auditors, SOC auditors maintain their independence by not advising their clients on operational aspects of the firm.

6 Conclusion

A modern firm has many types of stakeholders, each of whom interacts with different parts of the firm. While financial audits are useful for some stakeholders, other stakeholders may benefit from supplemental audits of other parts of the firm (“non-financial audits”). This study provides some of the first large-scale evidence on such audits. Using hand-collected data from public companies, I find that the large audit firms are often hired to evaluate internal controls over technology systems. The audit reports are meant mainly for a company’s customer market, and the scope of these audits typically includes controls over data security, processing integrity, and privacy. In addition, these audits are not explicitly mandated by legislation, and a company’s business-model reliance on technology is predictive of its decision to receive these audits. These audits are also associated with a large increase in audit-related fees that is economically significant when compared to the fees for other accounting services. Overall, these findings highlight the importance of non-financial audits in our attempts to understand the market for audit services.

In their recent survey of the accounting literature, Gow, Larcker, and Reiss (2016, Section 4.4) argue that any new research area should begin with simple and descriptive statistical

evidence before advancing to more complicated methods. Given the paucity of SOC audits in the literature, this is the path taken by the current study. Building an equilibrium model of the underlying matching process between companies, auditors, and customers may lead to new insights on SOC audits. In fact, research on financial audits began with descriptive evidence (e.g., Simunic, 1980; Watts and Zimmerman, 1983) and culminated in these types of analyses. Future research could also examine the markets for other types of non-financial audits.

References

- Acemoglu, D., Makhdoumi, A., Malekian, A., Ozdaglar, A., 2019. Too Much Data: Prices and Inefficiencies in Data Markets. Working Paper.
- AICPA, 2011. New SOC Reports for Service Organizations Replace SAS 70 Reports (https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2011/CPA/Feb/SOCReplaceSAS70Reports.jsp).
- AICPA, 2017. Trust Services Criteria Issued by the AICPA Assurance Services Executive Committee (<https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf>).
- AICPA, 2019. Trends in the supply of accounting graduates and the demand for public accounting recruits (<https://www.aicpa.org/content/dam/aicpa/interestareas/accountingeducation/newsandpublications/downloadabledocuments/2019-trends-report.pdf>).
- Altamuro, J., Beatty, A., 2010. How does internal control regulation affect financial reporting? *Journal of Accounting and Economics* 49, 58–74.
- Aobdia, D., 2015. Proprietary information spillovers and supplier choice: evidence from auditors. *Review of Accounting Studies* 20, 1504–1539.
- Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., 2007. The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics* 44, 166–192.
- Bell, T., Causholli, M., Knechel, W. R., 2015. Audit Firm Tenure, Non-Audit Services, and Internal Assessments of Audit Quality. *Journal of Accounting Research* 53, 461–509.
- Bell, T. B., Doogar, R., Solomon, I., 2008. Audit Labor Usage and Fees under Business Risk Auditing. *Journal of Accounting Research* 46, 729–760.
- Bell, T. B., Landsman, W. R., Shackelford, D. A., 2001. Auditors’ Perceived Business Risk and Audit Fees: Analysis and Evidence. *Journal of Accounting Research* 39, 35–43.
- Carnes, R. R., Christensen, D. M., Lamoreaux, P. T., 2019. Investor Demand for Internal Control Audits of Large U.S. Companies: Evidence from a Regulatory Exemption for M&A Transactions. *The Accounting Review* 94, 71–99.

- Cheng, M., Dhaliwal, D., Zhang, Y., 2013. Does investment efficiency improve after the disclosure of material weaknesses in internal control over financial reporting? *Journal of Accounting and Economics* 56, 1–18.
- Coates, J. C., Srinivasan, S., 2014. SOX after Ten Years: A Multidisciplinary Review. *Accounting Horizons* 28, 627–671.
- Costello, A., 2013. Mitigating incentive conflicts in inter-firm relationships: Evidence from long-term supply contracts. *Journal of Accounting and Economics* 56, 19–39.
- Davis, L. R., Ricchiute, D. N., Trompeter, G., 1993. Audit Effort, Audit Fees, and the Provision of Nonaudit Services to Audit Clients. *The Accounting Review* 68, 135–150.
- De Simone, L., Ege, M. S., Stomberg, B., 2015. Internal Control Quality: The Role of Auditor-Provided Tax Services. *The Accounting Review* 90, 1469–1496.
- DeFond, M., Zhang, J., 2014. A review of archival auditing research. *Journal of Accounting and Economics* 58, 275–326.
- DeFond, M. L., Jiambalvo, J., 1991. Incidence and Circumstances of Accounting Errors. *The Accounting Review* 66, 643–655.
- DeFond, M. L., Raghunandan, K., Subramanyam, K., 2002. Do Non–Audit Service Fees Impair Auditor Independence? Evidence from Going Concern Audit Opinions. *Journal of Accounting Research* 40, 1247–1274.
- Dell, 2020. Global Data Protection Index (<https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm>).
- Doyle, J., Ge, W., McVay, S., 2007. Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics* 44, 193–223.
- Duflo, E., Greenstone, M., Pande, R., Ryan, N., 2013. Truth-telling by Third-party Auditors and the Response of Polluting Firms: Experimental Evidence from India. *The Quarterly Journal of Economics* 128, 1499–1545.
- Duflo, E., Greenstone, M., Pande, R., Ryan, N., 2018. The Value of Regulatory Discretion: Estimates From Environmental Inspections in India. *Econometrica* 86, 2123–2160.
- Efendi, J., Mulig, E. V., Smith, L. M., 2006. Information Technology and Systems Research Published in Major Accounting Academic and Professional Journals. *Journal of Emerging Technologies in Accounting* 3, 117–128.

- Feng, M., Li, C., McVay, S. E., Skaife, H., 2015. Does Ineffective Internal Control over Financial Reporting affect a Firm's Operations? Evidence from Firms' Inventory Management. *The Accounting Review* 90, 529–557.
- Francis, J. R., 2006. Are Auditors Compromised by Nonaudit Services? Assessing the Evidence. *Contemporary Accounting Research* 23, 747–760.
- Frankel, R. M., Johnson, M. F., Nelson, K. K., 2002. The Relation between Auditors' Fees for Nonaudit Services and Earnings Management. *The Accounting Review* 77, 71–105.
- Gartner, 2019. Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019 (<https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g>).
- Ge, W., Koester, A., McVay, S., 2017. Benefits and costs of Sarbanes-Oxley Section 404(b) exemption: Evidence from small firms' internal control disclosures. *Journal of Accounting and Economics* 63, 358–384.
- Gerakos, J., Syverson, C., 2015. Competition in the Audit Market: Policy Implications. *Journal of Accounting Research* 53, 725–775.
- Gleason, C. A., Mills, L. F., 2011. Do Auditor-Provided Tax Services Improve the Estimate of Tax Reserves? *Contemporary Accounting Research* 28, 1484–1509.
- Govindarajan, V., Srivastava, A., Warsame, H., Enache, L., 2019. The Problem with France's Plan to Tax Digital Companies. *Harvard Business Review*, July 17, 2019.
- Gow, I., Larcker, D., Reiss, P., 2016. Causal inference in accounting research. *Journal of Accounting Research* 54, 477–523.
- Greene, W., 2002. *Econometric Analysis*, Fifth Edition. Pearson Education, Inc., Upper Saddle River, NJ.
- Haislip, J. Z., Peters, G. F., Richardson, V. J., 2016. The effect of auditor it expertise on internal controls. *International Journal of Accounting Information Systems* 20, 1–15.
- Hammersley, J. S., Myers, L. A., Shakespeare, C., 2008. Market reactions to the disclosure of internal control weaknesses and to the characteristics of those weaknesses under section 302 of the Sarbanes Oxley Act of 2002. *Review of Accounting Studies* 13, 141–165.
- Harp, N. L., Barnes, B. G., 2018. Internal control weaknesses and acquisition performance. *The Accounting Review* 93, 235–258.

- Hay, D. C., Knechel, W. R., Wong, N., 2006. Audit Fees: A Meta-analysis of the Effect of Supply and Demand Attributes. *Contemporary Accounting Research* 23, 141–191.
- Jensen, M., Meckling, W., 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3, 305–360.
- Johnson, W. B., Lys, T., 1990. The market for audit services: Evidence from voluntary auditor changes. *Journal of Accounting and Economics* 12, 281–308.
- Joskow, P., 1987. Contract Duration and Relationship-Specific Investments: Empirical Evidence from Coal Markets. *American Economic Review* 77, 168–185.
- Kaplan, S., Strömberg, P., 2003. Financial Contracting Theory Meets the Real World: An Empirical Analysis of Venture Capital Contracts. *Review of Economic Studies* 70, 281–315.
- Kaplan, S., Strömberg, P., 2004. Characteristics, Contracts, and Actions: Evidence from Venture Capitalist Analyses. *Journal of Finance* 59, 2177–2210.
- Kausar, A., Shroff, N., White, H., 2016. Real effects of the audit choice. *Journal of Accounting and Economics* 62, 157–181.
- Kinney, W. R., Libby, R., 2002. Discussion of The Relation between Auditors' Fees for Nonaudit Services and Earnings Management. *The Accounting Review* 77, 107–114.
- Kinney, W. R., McDaniel, L. S., 1989. Characteristics of firms correcting previously reported quarterly earnings. *Journal of Accounting and Economics* 11, 71–93.
- Kinney, W. R., Palmrose, Z.-V., Scholz, S., 2004. Auditor Independence, Non-Audit Services, and Restatements: Was the U.S. Government Right? *Journal of Accounting Research* 42, 561–588.
- Knechel, R., Salterio, S., 2016. *Auditing: Assurance and Risk*. Routledge.
- Knechel, W. R., Willenborg, M., 2016. Economics-based Auditing Research Published in JAR. *Journal of Accounting Research Virtual Issue*.
- Kreps, D., 1990. *A Course in Microeconomic Theory*. Princeton University Press.
- Larcker, D. F., Rusticus, T. O., 2010. On the use of instrumental variables in accounting research. *Journal of Accounting and Economics* 49, 186–205.
- Lennox, C. S., Pittman, J. A., 2011. Voluntary Audits versus Mandatory Audits. *The Accounting Review* 86, 1655–1678.

- Lim, C.-Y., Tan, H.-T., 2008. Non-audit Service Fees and Audit Quality: The Impact of Auditor Specialization. *Journal of Accounting Research* 46, 199–246.
- Liu, L. Y., 2020. Do Auditors Help Prevent Data Breaches? Working Paper.
- Loughran, T., McDonald, B., 2016. Textual Analysis in Accounting and Finance: A Survey. *Journal of Accounting Research* 54, 1187–1230.
- Mansi, S., Maxwell, W., Miller, D., 2004. Does Auditor Quality and Tenure Matter to Investors? Evidence from the Bond Market. *Journal of Accounting Research* 42, 755–793.
- Minnis, M., 2011. The Value of Financial Statement Verification in Debt Financing: Evidence from Private U.S. Firms. *Journal of Accounting Research* 49, 457–506.
- Minutti-Meza, M., 2013. Does Auditor Industry Specialization Improve Audit Quality? *Journal of Accounting Research* 51, 779–817.
- Mullainathan, S., 2019. Biased Algorithms Are Easier to Fix Than Biased People. *The New York Times*, December 6, 2019.
- Palmrose, Z.-V., 1986. The Effect of Nonaudit Services on the Pricing of Audit Services: Further Evidence. *Journal of Accounting Research* 24, 405–411.
- Rajgopal, S., Srinivasan, S., Zheng, X., 2020. Measuring audit quality. *Review of Accounting Studies* Forthcoming.
- Redman, T. C., Waitman, R. M., 2020. Do You Care About Privacy as Much as Your Customers Do? *Harvard Business Review*, January 28, 2020.
- Roberts, M. R., 2015. The role of dynamic renegotiation and asymmetric information in financial contracting. *Journal of Financial Economics* 116, 61–81.
- Roberts, M. R., Sufi, A., 2009. Control Rights and Capital Structure: An Empirical Investigation. *Journal of Finance* 64, 1657–1695.
- Roychowdhury, S., Shroff, N., Verdi, R. S., 2019. The effects of financial reporting and disclosure on corporate investment: A review. *Journal of Accounting and Economics* 68, 1–27.
- Schechner, S., Pop, V., 2020. Google Pushes ‘Sensible’ Ideas for How to Regulate AI. *The Wall Street Journal*, January 20, 2020.

- Schoenfeld, J., 2017. The effect of voluntary disclosure on stock liquidity: New evidence from index funds. *Journal of Accounting and Economics* 63, 51–74.
- Schoenfeld, J., 2020. Contracts between Firms and Shareholders. *Journal of Accounting Research* Forthcoming.
- Schroeder, J. H., Shepardson, M. L., 2016. Do SOX 404 Control Audits and Management Assessments Improve Overall Internal Control System Quality? *The Accounting Review* 91, 1513–1541.
- Seetharaman, A., Gul, F. A., Lynn, S. G., 2002. Litigation risk and audit fees: evidence from UK firms cross-listed on US markets. *Journal of Accounting and Economics* 33, 91–115.
- Shipman, J. E., Swanquist, Q. T., Whited, R. L., 2017. Propensity Score Matching in Accounting Research. *The Accounting Review* 92, 213–244.
- Simunic, D. A., 1980. The Pricing of Audit Services: Theory and Evidence. *Journal of Accounting Research* 18, 161–190.
- Simunic, D. A., 1984. Auditing, Consulting, and Auditor Independence. *Journal of Accounting Research* 22, 679–702.
- Skinner, D. J., Srinivasan, S., 2012. Audit Quality and Auditor Reputation: Evidence from Japan. *The Accounting Review* 87, 1737–1765.
- Smith, C., Warner, J., 1979. On financial contracting: An analysis of bond covenants. *Journal of Financial Economics* 7, 117–161.
- Stupp, C., 2019. European Privacy Regulators Find Their Workload Expands Along With Authority. *The Wall Street Journal*, April 12, 2019.
- Wakabayashi, D., 2018. California Passes Sweeping Law to Protect Online Privacy. *The New York Times*, June 28, 2018.
- Watts, R. L., Zimmerman, J. L., 1983. Agency Problems, Auditing, and the Theory of the Firm: Some Evidence. *The Journal of Law and Economics* 26, 613–633.
- Weber, J., Willenborg, M., 2003. Do Expert Informational Intermediaries Add Value? Evidence from Auditors in Microcap Initial Public Offerings. *Journal of Accounting Research* 41, 681–720.
- Weber, J., Willenborg, M., Zhang, J., 2008. Does auditor reputation matter? The case of KPMG Germany and ComROAD AG. *Journal of Accounting Research* 46, 941–972.

- Whisenant, S., Sankaraguruswamy, S., Raghunandan, K., 2003. Evidence on the Joint Determination of Audit and Non-Audit Fees. *Journal of Accounting Research* 41, 721–744.
- Willenborg, M., 1999. Empirical Analysis of the Economic Demand for Auditing in the Initial Public Offerings Market. *Journal of Accounting Research* 37, 225–238.
- Yoon, K., Hoogduin, L., Zhang, L., 2015. Big Data as Complementary Audit Evidence. *Accounting Horizons* 29, 431–438.
- Zhang, I. X., 2007. Economic consequences of the Sarbanes–Oxley Act of 2002. *Journal of Accounting and Economics* 44, 74–115.

Appendix A

SOC 3 report for Google. Source: Alphabet Inc. Investor Relations



Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110
Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Google LLC:

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls over the G Suite, Other Google Services and Supporting Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality" (Assertion), that Google's controls over the G Suite, Other Google Services and Supporting Services System (System) were effective throughout the period 1 May 2018 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management Responsibilities

Google's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the G Suite, Other Google Services and Supporting Services (System) and describing the boundaries of the System
- Identifying its principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of its system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Google's



relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Google's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Google's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Google's controls over the system were effective throughout the period 1 May 2018 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

10 September 2019
San Jose, CA

Appendix B

Variable Construction

This appendix provides the formula for each variable used in this study. Index i represents each firm. Financial data are taken from a firm's most recent annual report or proxy statement as of mid-2019. Any logged variables in the analyses use the natural log. Data source AA = Audit Analytics; C = Compustat; HC = hand collected.

Variable	Definition	Source
SOC Audit $_i$	1 if a firm receives a service organization control (SOC) audit based on the procedure defined in Section 3, 0 otherwise	HC
Audit Fees $_i$	Audit fees from the proxy statement	AA
Audit-Related Fees $_i$	Audit-related fees from the proxy statement (note that audit-related fees are distinct from any tax and technology consulting fees, which are included in different AA variables)	AA
Data Exposed $_i$	1 if a firm's annual report is in the top tercile of the sample's firm-level data exposure measure, computed as the frequency count of <i>analytics</i> , <i>big data</i> , <i>cloud platform</i> , <i>database</i> , <i>digital</i> , and <i>digitization</i> divided by the total number of words in the annual report; 0 otherwise	HC
Total Assets $_i$	Total assets	C
Market Value $_i$	Shares outstanding \times stock price	C
Leverage $_i$	Total debt \div total assets	C
Loss Firm $_i$	1 if net income is less than 0, 0 otherwise	C
ROA $_i$	Net income \div total assets	C
Current Assets \div Total Assets $_i$	Current assets \div total assets	C
Quick Ratio $_i$	(Cash + cash equivalents + marketable securities + accounts receivable) \div current liabilities	C
Segments $_i$	Total business segments	C
December Year End $_i$	1 if a firm's fiscal year ends in December, 0 otherwise	C
Qualified Audit (Financials) $_i$	1 if auditor issues a non-unqualified opinion on the financial statements, 0 otherwise	AA
Qualified Audit (Controls) $_i$	1 if auditor issues a non-unqualified opinion on internal controls over the financial statements, 0 otherwise	AA
Any Qualified Audit $_i$	1 if auditor issues a non-unqualified opinion on either the financial statements or internal controls over the financial statements, 0 otherwise	AA

Figure 1: Word Cloud for Service Organization Control Audit Reports

This figure provides a word cloud summary created from the corpus of SOC audit reports in the sample. The 40 most frequently occurring words are included (omitting stop words such as *and* and *the*), and the word sizes are proportional to their frequency in the corpus of reports.



Table 1: The AICPA’s Trust Services Criteria

Source: AICPA (2017)

Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity’s ability to meet its objectives. Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability. Information and systems are available for operation and use to meet the entity’s objectives. Availability refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing integrity. System processing is complete, valid, accurate, timely, and authorized to meet the entity’s objectives. Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity.

Confidentiality. Information designated as confidential is protected to meet the entity’s objectives. Confidentiality addresses the entity’s ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity’s control in accordance with management’s objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Privacy. Personal information is collected, used, retained, disclosed, and disposed to meet the entity’s objectives. Although the confidentiality applies to various types of sensitive information, privacy applies only to personal information. The privacy criteria are organized as follows: i. Notice and communication of objectives. The entity provides notice to data subjects about its objectives related to privacy. ii. Choice and consent. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects. iii. Collection. The entity collects personal information to meet its objectives related to privacy. iv. Use, retention, and disposal. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy. v. Access. The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy. vi. Disclosure and notification. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy. vii. Quality. The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy. viii. Monitoring and enforcement. The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Table 2: Types of Service Organization Control Audit Reports

Report Name	Title and Description (Adapted from the AICPA)
System and Organization Controls for Service Organizations: ICFR (SOC 1)	Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR). These reports are intended to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements. There are two types of reports for these engagements. Type 1 is a report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and implementation of the controls to achieve the related control objectives included in the description at a specific point in time. Type 2 is a report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design, implementation, and operating effectiveness of the controls to achieve the related control objectives included in the description over a minimum six-month period. Use of these reports is often restricted to the management of the service organization, user entities, and user auditors.
System and Organization Controls for Service Organizations: Trust Services Criteria (SOC 2)	Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in: oversight of the organization, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight. Similar to a SOC 1 report, there are two types of reports. Type 1 is a report on management's description of a service organization's system and the suitability of the design and implementation of controls at a specific point in time. Type 2 is a report on management's description of a service organization's system and the suitability of the design, implementation, and operating effectiveness of controls. Use of these reports is often restricted to the management of the service organization, user entities, and user auditors.
System and Organization Controls for Service Organizations: Trust Services Criteria for General Use Report (SOC 3)	Trust Services Report for Service Organizations. These reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing, integrity, confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. Because they are general use reports, SOC 3 reports can be freely distributed.

Table 3: Descriptions of Internal Controls Evaluated for Service Organization Control Audits

The internal controls in this table are adapted from the SOC audit reports in the sample.

Internal Control Description
1. We have defined structures and reporting lines with assigned authority and responsibilities to appropriately meet data requirements relevant to security, availability, confidentiality, and privacy.
2. We maintain a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact our business objectives, regulatory requirements, and customers.
3. Roles and responsibilities for cryptographic custodians are formally documented and agreed to by those individuals when they assume the role or when responsibilities change.
4. We require two-factor authentication over an approved cryptographic channel to access our internal network from remote locations.
5. Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
6. We perform external vulnerability assessments at least quarterly, identified issues are promptly investigated and tracked to resolution.
7. We enable customers to articulate who has access to our cloud services and resources that they own. We prevent customers from accessing resources that are not assigned to them via access permissions.
8. We perform application security reviews for externally launched products, services, and significant feature additions prior to launch to evaluate whether security risks are identified and mitigated.
9. We configure network devices to only allow access to specific ports on our server systems.
10. External data access is logged with the following information: data accessor IP address, object and operation. Logs are retained for at least 90 days.
11. Physical hosts have host-based firewalls to prevent unauthorized access.
12. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
13. We enable secure communication by SSH configuration by generating a unique host-key and delivering the key's fingerprint to the user over a trusted channel.
14. Customer master keys used for cryptographic operations are logically secured so that no single employee can gain access to the material.
15. We use a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved.
16. We maintain separate production and development coding environments.
17. Customer information, including personal information, and customer content are not used in test and development environments.
18. We compare user provided checksums to validate the integrity of data in transit and reject data transfers with failed checksum matches.

Table 4: Industry Breakdown of Service Organization Control Audits for S&P 500 Firms in 2019

GICS Industry	(1) Firms	(2) Firms with SOC Audit	(3) $\frac{\text{Column (2)}}{\text{Column (1)}}$	Examples of Firms Receiving SOC Audits
Communication Services	23	11	0.48	AT&T, Facebook, Verizon
Consumer Discretionary	63	9	0.14	Amazon.com, Expedia, Target
Consumer Staples	33	4	0.12	Colgate, Proctor & Gamble, Walmart
Energy	28	3	0.11	Baker Hughes, Devon, National Oilwell
Financials	67	32	0.48	Goldman Sachs, Synchrony Financial, T. Rowe Price
Health Care	61	18	0.30	Cigna, Pfizer, United Health Group
Industrials	69	17	0.25	IHS Markit, Northrop Grumman, Raytheon
Information Technology	68	42	0.62	ADP, Microsoft, Salesforce
Materials	28	2	0.07	LyondellBasell, Newmont Goldcorp
Real Estate	32	5	0.16	CBRE, Digital Realty Trust, Iron Mountain
Utilities	28	3	0.11	CenterPoint, Entergy, Exelon
Total	500	146	-	

Table 5: Descriptive Statistics for Service Organization Control Audits for S&P 500 Firms in 2019

All variables representing dollar amounts are in thousands. Index i represents each firm in the sample. The statistical significance of all the subsequent results is similar when I winsorize the continuous variables at the 1% level and 99% level (unless a variable's lower bound is zero, in which case it is winsorized only at the 99% level). Appendix B provides the exact formulas for the variables. The "Diff." column provides the t-statistic from a two-tailed t-test of the difference in means between firms with SOC audits and firms without SOC audits.

Variable	Full Sample ₁			Firms w/ SOC Audit ₂		Firms w/o SOC Audit ₃		Diff.
	N ₁	Mean ₁	σ_1	N ₂	Mean ₂	N ₃	Mean ₃	
SOC Audit _{<i>i</i>}	500	0.29	0.46	146	1.00	354	0.00	(.)
Data Exposed _{<i>i</i>}	500	0.33	0.47	146	0.47	354	0.27	(4.16)
Total Assets _{<i>i</i>}	500	70,094,268.63	219,252,276.32	146	116,968,283.25	354	50,762,047.92	(2.50)
Market Value _{<i>i</i>}	500	45,128,631.39	84,932,143.08	146	74,536,431.75	354	32,999,990.56	(3.62)
Audit Fees _{<i>i</i>}	500	10,053.82	11,032.51	146	13,896.72	354	8,468.90	(4.10)
Audit-Related Fees _{<i>i</i>}	500	1,504.10	3,892.72	146	2,824.24	354	959.64	(3.57)
Leverage _{<i>i</i>}	500	0.31	0.21	146	0.26	354	0.33	(3.35)
Loss Firm _{<i>i</i>}	500	0.05	0.22	146	0.04	354	0.06	(0.75)
ROA _{<i>i</i>}	500	0.07	0.07	146	0.07	354	0.07	(0.54)
Current Assets ÷ Total Assets _{<i>i</i>}	500	0.27	0.22	146	0.30	354	0.26	(2.03)
Quick Ratio _{<i>i</i>}	500	1.14	0.86	146	1.25	354	1.09	(1.65)
Segments _{<i>i</i>}	500	6.26	8.33	146	5.83	354	6.44	(0.71)
December Year End _{<i>i</i>}	500	0.75	0.43	146	0.69	354	0.78	(1.92)
Qualified Audit (Financials) _{<i>i</i>}	500	0.24	0.43	146	0.21	354	0.26	(1.09)
Qualified Audit (Controls) _{<i>i</i>}	500	0.03	0.17	146	0.03	354	0.03	(0.51)
Any Qualified Audit _{<i>i</i>}	500	0.26	0.44	146	0.24	354	0.27	(0.67)

Table 6: Reduced-Form Model of Service Organization Control Audits for S&P 500 Firms in 2019

Index i represents each firm in the sample. Financial data are taken from a firm's most recent annual report or proxy statement as of mid-2019. Appendix B provides the exact formulas for the variables. Linear probability regressions are used to accommodate fixed effects. Standard errors are in parentheses and robust to heteroscedasticity. ***, **, and * indicate statistical significance at the two-tailed 1%, 5%, and 10% level, respectively. Note that column 1 has the largest R^2 value because it includes all the industry-fixed effects.

	Dependent Variable: SOC Audit $_i$					
	(1)	(2)	(3)	(4)	(5)	(6)
Data Exposed $_i$		0.220*** (0.040)				
Information Technology $_i$			0.374*** (0.061)			
Financials $_i$				0.202*** (0.072)		
Consumer Staples $_i$					-0.205** (0.083)	
Energy $_i$						-0.196** (0.087)
Log(Assets) $_i$	0.076*** (0.018)	0.091*** (0.017)	0.092*** (0.017)	0.080*** (0.018)	0.096*** (0.017)	0.094*** (0.017)
Leverage $_i$	-0.077 (0.102)	-0.070 (0.099)	-0.184* (0.095)	-0.091 (0.104)	-0.164* (0.099)	-0.203** (0.098)
Loss Firm $_i$	0.017 (0.096)	-0.040 (0.094)	-0.034 (0.095)	0.007 (0.099)	-0.011 (0.098)	0.008 (0.099)
ROA $_i$	0.479 (0.352)	0.654* (0.344)	0.306 (0.348)	0.437 (0.359)	0.491 (0.362)	0.409 (0.360)
Current Assets ÷ Total Assets $_i$	0.227* (0.122)	0.222* (0.119)	0.149 (0.109)	0.366*** (0.114)	0.280** (0.110)	0.268** (0.110)
Quick Ratio $_i$	-0.038 (0.027)	-0.039 (0.026)	-0.001 (0.025)	0.014 (0.026)	0.011 (0.026)	0.023 (0.026)
Segments $_i$	0.000 (0.002)	-0.001 (0.002)	-0.001 (0.002)	0.002 (0.002)	-0.000 (0.002)	-0.000 (0.002)
December Year End $_i$	-0.061 (0.050)	-0.048 (0.049)	-0.019 (0.048)	-0.104** (0.049)	-0.108** (0.049)	-0.070 (0.048)
Industry-Fixed Effects	Y	Y	N	N	N	N
Observations	500	500	500	500	500	500
R^2	0.20	0.25	0.15	0.10	0.10	0.10

Table 7: Sub-Industry Regressions of Service Organization Control Audits for S&P 500 Firms in 2019

Index i represents each firm in the sample. Financial data are taken from a firm's most recent annual report or proxy statement as of mid-2019. Appendix B provides the exact formulas for the variables. Linear probability regressions are used to accommodate fixed effects. Standard errors are in parentheses and robust to heteroscedasticity. ***, **, and * indicate statistical significance at the two-tailed 1%, 5%, and 10% level, respectively.

	Dependent Variable: SOC Audit $_i$					
	(1)	(2)	(3)	(4)	(5)	(6)
Data Processing Services $_i$	0.472*** (0.127)					
Internet Services & Infrastructure $_i$		0.717*** (0.256)				
Application Software $_i$			0.528*** (0.141)			
Investment Banking/Brokerage $_i$				0.609*** (0.200)		
Internet Marketing $_i$					0.572** (0.235)	
I.T. Consulting $_i$						0.320* (0.181)
Controls from Table 6	Y	Y	Y	Y	Y	Y
Industry-Fixed Effects	N	N	N	N	N	N
Observations	500	500	500	500	500	500
R^2	0.11	0.10	0.11	0.10	0.10	0.09

Table 8: Service Organization Control Audits and Audit Fees for S&P 500 Firms in 2019

All variables representing dollar amounts are in thousands. Index i represents each firm in the sample. Financial data are taken from a firm's most recent annual report or proxy statement as of mid-2019. Appendix B provides the exact formulas for the variables. Standard errors are in parentheses and robust to heteroscedasticity. ***, **, and * indicate statistical significance at the two-tailed 1%, 5%, and 10% level, respectively.

	(1)	(2)	(3)
	Log(Audit Fees) $_i$	Log(Audit-Related Fees) $_i$	Audit-Related Fees $_i$
SOC Audit $_i$	0.000 (0.071)	0.687*** (0.240)	898.897*** (268.706)
Log(Assets) $_i$	0.528*** (0.028)	1.063*** (0.094)	1510.330*** (145.095)
Leverage $_i$	0.461*** (0.159)	0.391 (0.535)	-128.712 (822.943)
Loss Firm $_i$	0.315** (0.150)	0.913* (0.505)	2276.265*** (776.070)
ROA $_i$	-0.384 (0.553)	-1.680 (1.856)	1946.677 (2852.884)
Current Assets \div Total Assets $_i$	0.838*** (0.192)	1.297** (0.644)	380.134 (990.196)
Quick Ratio $_i$	-0.078* (0.042)	-0.210 (0.140)	178.329 (215.425)
Segments $_i$	0.015*** (0.004)	0.004 (0.013)	21.712 (19.770)
December Year End $_i$	-0.036 (0.078)	0.171 (0.263)	372.209 (404.491)
Industry-Fixed Effects	Y	Y	Y
Observations	500	500	500
R^2	0.56	0.36	0.29

Table 9: Additional Tests of Service Organization Control Audits for S&P 500 Firms in 2019

All variables representing dollar amounts are in thousands. Note that the auditor-specific independent variables represent a company's financial auditor. Index i represents each firm in the sample. Financial data are taken from a firm's most recent annual report or proxy statement as of mid-2019. Appendix B provides the exact formulas for the variables. Linear probability regressions are used to accommodate fixed effects. Standard errors are in parentheses and robust to heteroscedasticity. ***, **, and * indicate statistical significance at the two-tailed 1%, 5%, and 10% level, respectively.

	Dependent Variable: SOC Audit $_i$						
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Qualified Audit (Controls) $_i$	0.117 (0.120)						
Qualified Audit (Financials) $_i$		-0.063 (0.046)					
Any Qualified Audit $_i$			-0.044 (0.045)				
Deloitte $_i$				-0.022 (0.048)			
Ernst & Young $_i$					0.011 (0.041)		
KPMG $_i$						0.055 (0.049)	
PwC $_i$							-0.037 (0.042)
Controls from Table 6	Y	Y	Y	Y	Y	Y	Y
Industry-Fixed Effects	Y	Y	Y	Y	Y	Y	Y
Observations	500	500	500	500	500	500	500
R^2	0.20	0.20	0.20	0.20	0.20	0.20	0.20

Table 10: Comparison of SOC Audits to Financial Statement Audits for Public Firms

	Typical SOC Audit	Typical Financial Statement Audit
Mandated by Regulators	No	Yes
Audit Objectives	To provide an objective independent evaluation of the client’s internal controls over data security and integrity	To provide an objective independent evaluation of the client’s financial statements and controls over revenue and expense recognition
Internal Controls Evaluated	Internal controls over data security and integrity	Internal controls over the recognition of revenues and expenses
Key Audit Report Users	Customers (user entities) and their auditors	Shareholders, lenders, and regulators
Litigation Risk	SOC audits do not guarantee against data breaches and other data-related issues at the client. Audit firms typically cannot be held liable for such events absent negligence on their part.	Financial statement audits do not guarantee against fraud or misstatements at the client. Audit firms typically cannot be held liable for such events absent negligence on their part.
Consulting Environment	Audit firms are typically not permitted to have concurrent consulting engagements with the client. SOC audits are meant to evaluate the client’s controls in place, not to advise the client on how they can implement better controls to avoid data breaches and other technology failures.	Audit firms are typically not permitted to have concurrent consulting engagements with the client. Financial statement audits are not meant to advise the client on how they can avoid fraud and other issues.
Potential Audit Opinions	Unqualified opinion, qualified opinion, adverse opinion, disclaimer of opinion	Unqualified opinion, qualified opinion, adverse opinion, disclaimer of opinion
Other Audit Outputs	SOC audit reports often include worksheets containing all the internal controls that managers identified as in-scope for the audit, and descriptions of all the tests performed by the audit firm and the outcomes of those tests.	The audit opinion is typically the only document released by the audit firm.