



SOC Overview

Welcome to the forefront of trust and transparency in today's digital landscape! We are excited to introduce our Service Organization Controls (SOC) services, designed to safeguard and elevate the integrity of your organization's operations. In an era where data security and compliance are paramount, our SOC services are your beacon of assurance, guiding you through the intricacies of control, risk management, and accountability.

At our core, we are committed to delivering SOC services that exceed industry standards, granting you and your stakeholders unparalleled confidence in your systems, processes, and controls. We take pride in our industry-agnostic approach, offering solutions that address the distinct requirements of both private and government entities across a wide range of sectors.

Our team of seasoned experts is armed with the latest knowledge and methodologies to conduct comprehensive assessments, providing a thorough examination of your organization's controls. Whether you are seeking SOC 1, SOC 2, or SOC 3 compliance, our tailored solutions offer a roadmap to fortify your internal controls, reduce risks, and meet the evolving demands of your industry.

What distinguishes us is our commitment to transparent and reasonable pricing, coupled with exceptional client service. Our fees are straightforward and remarkably reasonable, assuring that you receive exceptional value for the trust and compliance you seek. Join us on a journey toward unparalleled trust, compliance, and exceptional service, where our SOC solutions consistently exceed your expectations.

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

©2024. Lawrence J.
Beardsley CPA, PLLC.
All Rights Reserved.

SOC Differences and Types

Although not obligatory, SOC audits are now becoming a common component of business transactions. The primary objective of a SOC engagement is to assess the effectiveness of a company's internal controls and the protective measures they've established, all the while delivering impartial and practical feedback.

There are three primary types of SOC reports: SOC 1, SOC 2, and SOC 3. SOC 1 reports are designed to evaluate the effectiveness of a service organization's internal controls over financial reporting. A SOC 2 Type 2 report is a comprehensive and valuable document that assesses the controls and safeguards put in place by a service organization to protect sensitive customer data. It focuses on the security, availability, processing integrity, confidentiality, and privacy of the data systems, often referred to as the Trust Services Criteria.












A SOC 3 report is a condensed version of the SOC 2 report. The primary purpose of a SOC 3 report is to provide a brief overview of a service organization's controls and safeguards related to the Trust Services Criteria. Unlike SOC 2 reports, SOC 3 reports are designed to be publicly available and are often used for marketing purposes.

Regardless of if you are choosing a SOC 1 or a SOC 2 report, there are two types of reports that correspond to the audit, a Type 1 and a Type 2 report. A Type 1 report evaluates the suitability of design of a service organization's controls at a specific point in time. It provides an assessment of the controls as they are designed and implemented at the moment the audit is conducted. A Type 2 report goes beyond the design assessment and evaluates the operating effectiveness of the controls over a specified period, typically covering a minimum of six months. It assesses whether these controls have been consistently applied and have effectively maintained the desired security and privacy levels over time.

These reports are particularly valuable for businesses that outsource critical financial processes. A SOC 1 Type 1 report provides an assessment of the suitability of controls in place of internal controls and direct management of the processes. In contrast, a SOC 1 Type 2 report goes a step further by illustrating that the internal controls were being followed properly. This key distinction between Type 1 and Type 2 reports lies in the depth of evaluation, with Type 2 offering a more comprehensive understanding of control performance over time.

Here is a break down of your options, let us know which report is right for you!

REPORTS	CONTROL DOMAINS	AUDIT FOCUS	AUDIENCE
SOC 1 Assesses internal controls supporting financial reporting	<ul style="list-style-type: none"> Operations and Transaction Processing IT General Controls Supplement 	Client Defined Control Objectives	Restricted Report Financial Auditors and Users of the Report
SOC 2 Assesses internal controls for compliance using the Trust Service Criteria	<ul style="list-style-type: none"> Infrastructure Software People Procedures Data 	Trust Services Categories <ul style="list-style-type: none"> Security Availability Processing integrity Confidentiality Privacy Categories covered are selected by the Client	Restricted Report Current Clients, Auditors, and Necessary Parties
SOC 3 An abridged version of the SOC 2 report, used for marketing purposes			Unrestricted Report New Potential Clients

REPORT TYPES	SOC REPORTS			TESTING SCOPE		
	SOC 1	SOC 2	SOC 3	Design	Operating Effectiveness	Results of Tests (Except for SOC 3)
Type 1 Point in Time						
Type 2 Period of Time						

SOC 1 and SOC 2 reports are restricted to protect sensitive information and maintain the confidentiality and security of the evaluated organization's internal controls and financial data, limiting access to authorized stakeholders such as management and auditors.

SOC 1 Report

A SOC 1 report is a crucial assurance document designed to provide valuable insights into a service organization's internal controls over financial reporting. These reports are essential for businesses that outsource certain financial processes to service providers, as they help assess the effectiveness of the controls in place to protect the integrity and accuracy of financial data. SOC 1 reports are particularly important for organizations subject to regulations like the Sarbanes-Oxley Act (SOX) in the United States.

SOC 1 reports come in two different types: Type 1 and Type 2. A SOC 1 Type 1 report offers an evaluation of the suitability of a service organization's control design at a specific point in time. It provides a snapshot of how the controls are intended to work. On the other hand, a SOC 1 Type 2 report goes beyond the design assessment, examining the operating effectiveness of controls over a specified period, typically covering at least three months. It assesses whether these controls have been consistently applied and whether they have effectively maintained the desired security and integrity of financial data over time.

The primary target audience for SOC 1 reports includes the service organization's customers and their auditors. Clients request these reports to gain assurance about the internal controls in place, which are critical for ensuring the accuracy and reliability of financial statements. Auditors of these clients use SOC 1 reports to understand the controls related to financial reporting processes at service organizations and to reduce the scope of their own financial statement audits. These reports are considered to be restricted use reports meaning that providers are only allowed to provide the report to their current customers.

Control Objectives in a SOC 1 report refer to the specific goals or outcomes that the internal controls are designed to achieve. These objectives are essential for maintaining the integrity and accuracy of financial information. For example, control objectives might include ensuring the proper authorization of financial transactions, the protection of financial data from unauthorized access, and the prevention of fraud or errors in financial reporting. Control objectives provide the framework for evaluating the effectiveness of the controls documented in the report, offering a clear understanding of how the service organization safeguards the financial reporting process for its clients.

Companies Requiring SOC 1 Reports

Companies across various industries may need a SOC 1 report. Typically required by companies that provide services to other organizations, and these services can impact the financial reporting of those organizations. Specifically, companies that should consider obtaining a SOC 1 report include:

- Data Centers
- Third-Party Administrators
- Managed IT Service Providers
- Payment Processors
- Loan Servicers
- Trust Companies
- Outsourced Accounting Firms

Intended Audience for SOC 1 Reports

The target audience for SOC 1 reports primarily includes the clients and their auditors of the service organization. These reports are critical for organizations that rely on the services provided by third-party service providers, as they offer assurance regarding the effectiveness of controls over financial reporting. Clients use SOC 1 reports to assess the reliability and security of the service organization's systems and processes, providing valuable information for risk management and decision-making. Auditors of the client organizations rely on these reports to evaluate the impact of the service organization's controls on their own financial statements, helping them make informed judgments about the accuracy and completeness of financial data. Additionally, regulatory bodies, shareholders, and other stakeholders may also find SOC 1 reports useful in ensuring compliance with industry regulations and best practices, fostering trust and transparency in the business ecosystem.

SOC 2 Reports

A SOC 2 report is a comprehensive assessment of the controls and safeguards implemented by a service organization to protect the security, availability, processing integrity, confidentiality, and privacy of data and systems. These reports are pivotal for businesses that rely on third-party service providers to handle their sensitive information. SOC 2 audits are conducted in accordance with the criteria established by the American Institute of Certified Public Accountants (AICPA) and are designed to provide assurance regarding the effectiveness of a service organization's control environment.

Trust Service Criteria

The SOC 2 report evaluates an organization's adherence to one or more of the Trust Service Criteria. These criteria include the following:

Security: Assesses the effectiveness of controls designed to safeguard data and systems against unauthorized access, disclosure, and damage.

Availability: It evaluates controls that ensure systems and data are available and operational when needed.

Processing Integrity: This criterion examines controls that maintain the accuracy, completeness, and timeliness of data processing.

Confidentiality: It focuses on controls that protect sensitive information from unauthorized disclosure.

Privacy: This criterion assesses the management of personal information in compliance with relevant privacy regulations.

Companies Requiring SOC 2 Reports

Companies across various industries may need a SOC 2 report. Typically, service organizations that process, store, or transmit sensitive client data or provide services critical to their clients' financial or operational functions are prime candidates. This includes:

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Data Centers
- Cloud Service Providers
- Managed IT services
- Financial Institutions
- Healthcare Providers

Clients and stakeholders often request SOC 2 reports as a means to ensure that their data is secure and that the service organization is committed to maintaining a robust control environment.

Intended Audience for SOC 2 Reports

The primary audience for SOC 2 reports includes current and potential clients of the service organization. These reports serve as a valuable tool for clients to assess and validate the security and privacy controls in place. Furthermore, these reports are critical for auditors, who rely on SOC 2 findings to better understand the controls at service organizations and to tailor their own audit procedures when evaluating their client's financial statements. Additionally, business partners, regulatory authorities, and other stakeholders interested in data security and compliance may also review SOC 2 reports to gauge the organization's commitment to data protection and operational integrity. In summary, SOC 2 reports play a pivotal role in building trust and confidence in the operations of service organizations and are critical for a wide range of stakeholders.

SOC 3 Reports

A SOC 3 report is a condensed version of the more comprehensive SOC 2 report, both of which are part of the SOC framework developed by the American Institute of Certified Public Accountants (AICPA). A SOC 3 report provides a high-level summary of the findings and conclusions from a SOC 2 audit, making it suitable for sharing with a broad audience, including prospective clients and the general public.

Unlike SOC 2 reports, SOC 3 reports are designed to be publicly available and are often used for marketing purposes. These reports communicate that a service organization has undergone a rigorous examination of its controls related to security, availability, processing integrity, confidentiality, and privacy. Service organizations that receive SOC 3 reports typically use them to demonstrate their commitment to data security and privacy to potential clients, partners, and stakeholders. By making these reports publicly accessible, organizations can provide transparency and assurance regarding their control environment, which can be a significant selling point for clients concerned about data protection and compliance. A SOC 3 report offers a way for organizations to showcase their commitment to security and compliance without sharing sensitive, proprietary information.

The LJB Approach

At LJB, our goal is straightforward: to provide you with exceptional expertise, maintain clear and open communication, and deliver your report on time. Our team consists of compliance experts who have dedicated their careers to mastering compliance knowledge, and they continually pursue further education to remain industry experts.

If your company lacks a predefined control set and requires a Readiness Assessment, we offer three tailored solutions:

1. **Control Set Enhancement:** If you have an existing control set that needs refinement to align with your SOC report.
2. **Traditional Readiness Assessment:** Tailored to your specific environment and needs.
3. **Alignment with Multiple Compliance Frameworks:** For companies looking to align controls across various compliance frameworks.

No matter which Readiness Assessment option you choose, we will provide you with a comprehensive list of control coverage gaps and guide you on necessary remediation steps. By the end of the assessment, you will not only have a refined control set but also a document request list outlining the specific requirements to successfully pass your examination.

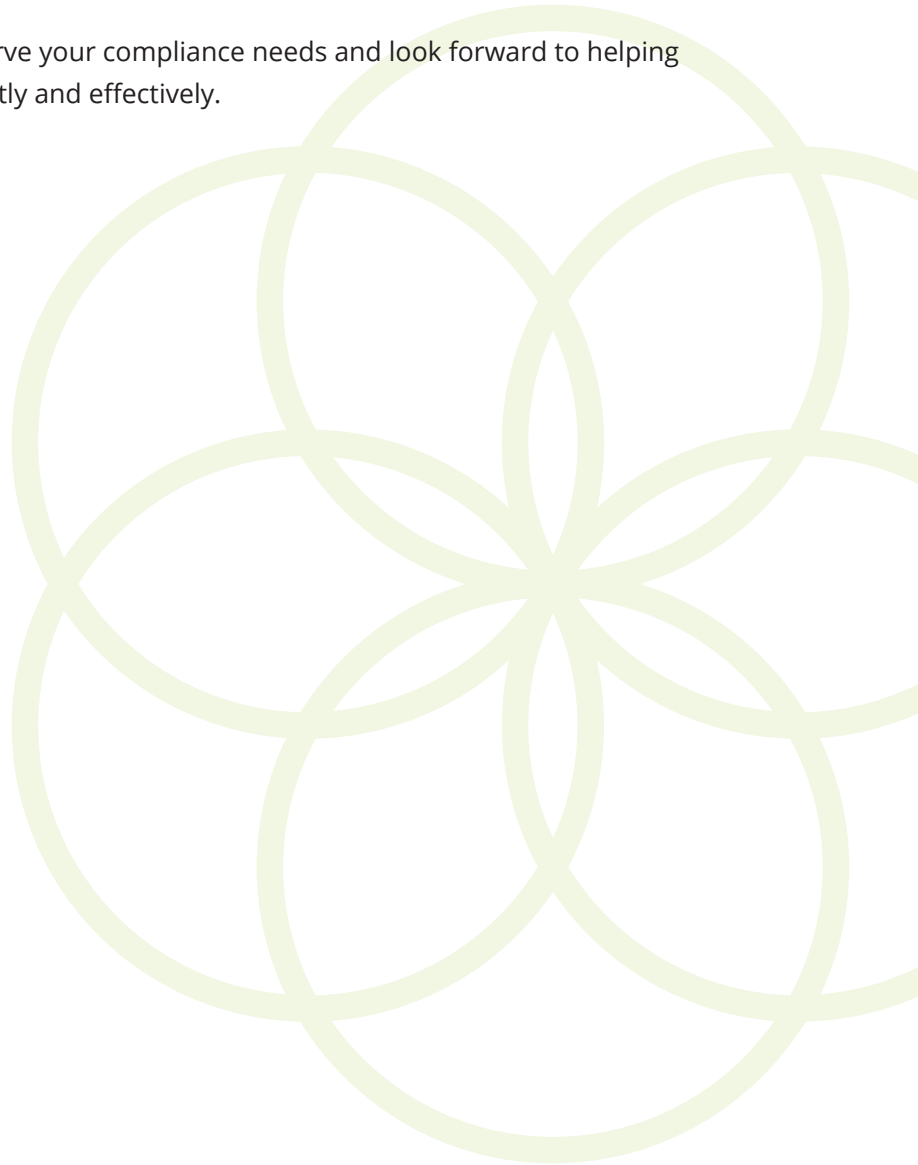
During the fieldwork phase, we prioritize simplicity and effectiveness. We conduct an internal risk assessment to tailor our testing approach to your organization, avoiding over-testing or under-testing of controls. You will receive a detailed timeline with milestones, ensuring everyone is aligned on the path to SOC compliance. We also maintain open lines of communication by scheduling weekly status meetings with your team to keep you informed and engaged. We offer flexibility by conducting fieldwork either on-site or remotely, based on your preferences and needs.

Our commitment is to deliver results efficiently. We guarantee an issuance date within 45 days from the end of the engagement period, provided that all necessary evidence is provided on schedule. This approach ensures a comprehensive evaluation of your internal controls while minimizing disruptions to your operations.

Straight-forward Pricing

For our standard SOC reports, your fee is calculated based on the number of controls, plus a base fee for report generation. We believe in transparency, with no hidden charges or administrative fees associated with our reports. The only potential additional charges may arise for travel costs related to our work or for any necessary rework of controls that have been modified after the project kick-off.

We appreciate the opportunity to serve your compliance needs and look forward to helping you achieve SOC compliance efficiently and effectively.



Meet your Leadership Team



Richard Stevenson

CPA, CISA, CCSFP, CITP, CIPM

richard@ljbcpa.com

Richard Stevenson, a seasoned professional with over a decade of experience in IT consulting, compliance, and audit services, proudly serves as the Director of Compliance and Audit. He oversees our compliance practice, managing and delivering comprehensive SOC 1, 2, and 3 examinations while providing leadership to our audit practice. Richard is dedicated to delivering high-quality, reliable

services. His extensive experience spans diverse industries, including technology, healthcare, insurance, energy, and construction. Prior to embarking on a career in public accounting, Richard spent seven years in the insurance industry, gaining valuable experience at GEICO.

An alumnus of Texas A&M University, Richard holds a bachelor's degree in finance and has called Dallas, Texas, and the DFW Metroplex home for the past forty years. He furthered his education by earning a master's degree in accounting from the University of Texas at Dallas.



Caitlin LeMaire

CPA

caitlin@ljbcpa.com

Caitlin LeMaire is passionately dedicated to inspiring clients, employees, and stakeholders to contribute positively to society and elevate humanity. As one of two partners at her firm, she has a significant role in day-to-day operations. Her responsibilities encompass firm management, staff development and training, marketing and business development, HR, and technology implementations. Additionally,

she is the partner in charge of the firm's audit and accounting practices. Caitlin is also deeply involved in strategic planning, guided by her steadfast commitment to the principles of conscious capitalism.

Her professional journey began as an auditor at Ernst & Young. Seeking a more direct impact, she transitioned to public accounting at a local firm. This move enabled Caitlin to focus on serving small and midsize businesses. Her extensive experience spans a broad range of sectors including airlines, casinos, technology, media, service, retail, entertainment, nonprofit, and construction companies.

Caitlin's academic background includes both a bachelor's and a master's degree in accounting from Louisiana Tech University. An active alumna, she mentors accounting students, offering invaluable guidance for the CPA exam and career development.

Caitlin is a licensed CPA in both Texas and Nevada and maintains active memberships with the AICPA and the Texas Society of CPAs.

Outside of her professional sphere, Caitlin enjoys boating, spontaneous weekend getaways, sampling local wineries and breweries, zoo explorations, and visiting national parks.

Contact Us

Richard Stevenson, Director

Phone: 903-229-0341

Email: richard@ljbcpa.com

Web: LJB CPA | SOC Reports Page | Arlington, TX (lbeardsleycpa.com)

About the firm

We proudly stand as your dedicated advocate. At LJB CPA, our unwavering commitment is driven by a profound sense of purpose and our guiding principles. We firmly reside at the crossroads of competency, purpose, value, and service, and we adhere to a set of foundational values that underpin our approach to serving all our stakeholders.

Our Values

Our firm consistently delivers exceptional service to our clients by upholding three core principles: Quality, Reliability, and Service. These principles are the bedrock of our operations and are non-negotiable.

With multiple offices at our disposal, we operate as a comprehensive accounting firm equipped to address all your accounting needs. Our structure is designed to cater to businesses seeking high-quality resources delivered in a collaborative team-oriented fashion. Our mission is to provide clients with the utmost level of service and value by prioritizing what is essential to them and their stakeholders. Whether you are a startup in need of foundational support, or an established firm looking to navigate compliance requirements and advance to the next level, we are here to assist you every step of the way.