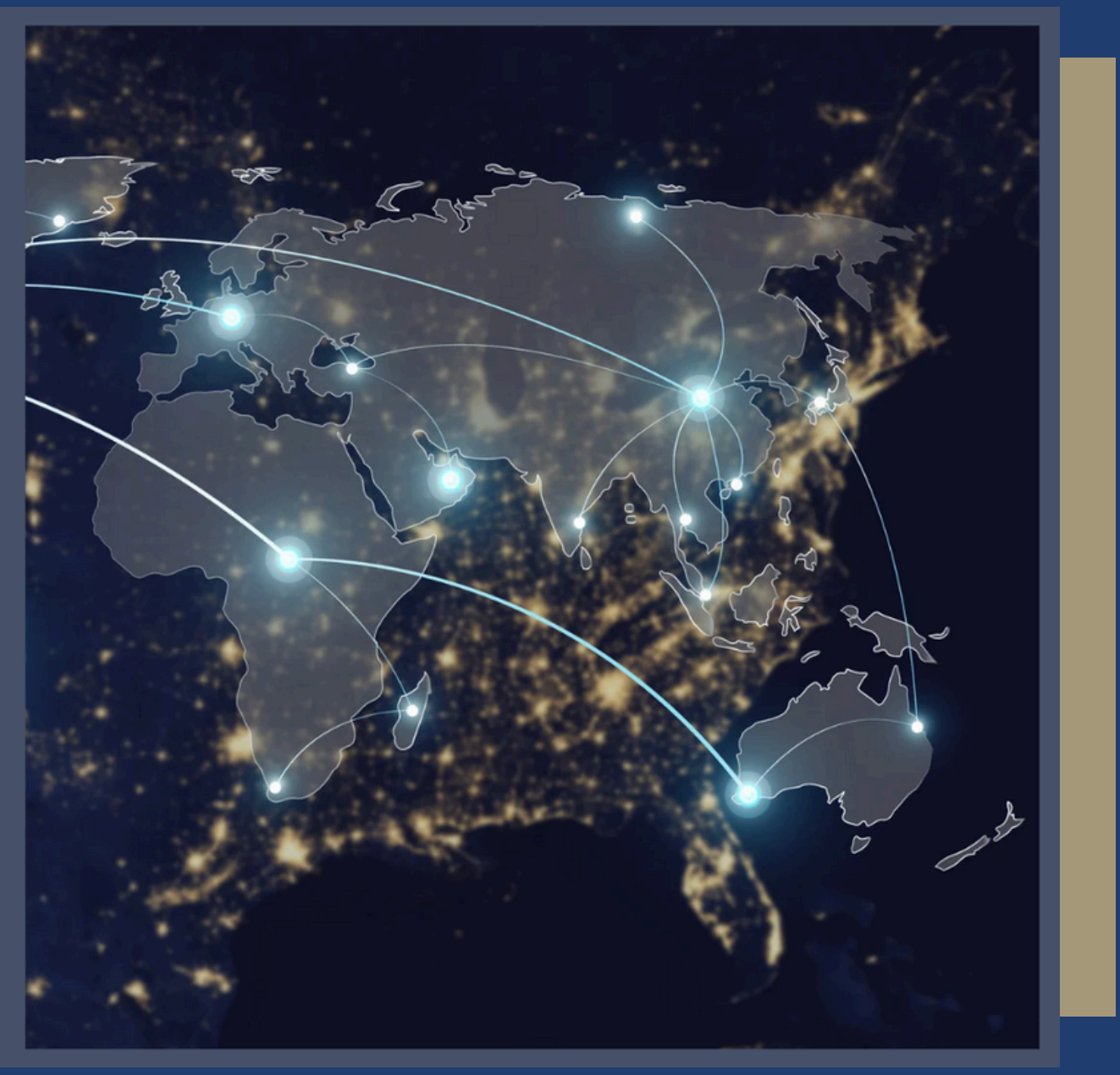
WHITE PAPER

SOC 1 VS. SOC 2: WHAT LEADERS NEED TO KNOW

ALCHEMI ADVISORY GROUP



Discover how to align your compliance strategy with growth, reduce risk, and choose the right partner to strengthen credibility and win business. This white paper cuts through the confusion between SOC 1 and SOC 2 to help technology and security leaders make smarter audit decisions.

Executive Summary

In today's climate of heightened scrutiny, buyer skepticism, and increasing regulatory pressure, SOC 1 and SOC 2 reports have become essential tools for demonstrating operational maturity and earning client trust. But choosing the right framework—and the right partner to guide you through it—requires more than technical knowledge. It demands a strategic approach.

This white paper breaks down the critical differences between SOC 1 and SOC 2, outlines the end-to-end process for each, and provides guidance tailored to both first-time audits and organizations re-evaluating existing contracts. It emphasizes the importance of starting with a readiness assessment to reduce risk, streamline timelines, and avoid costly missteps.

You'll also gain insight into what separates a transactional auditor from a true compliance partner—and why more forward-looking organizations are locking in multi-year engagements to stabilize cost, improve continuity, and align compliance efforts with business growth.

For executive leaders, SOC compliance is no longer just a technical requirement—it's a competitive differentiator. This paper will help you evaluate where you stand, where you need to go, and how to get there with confidence.

- The strategic implications of SOC 1 vs. SOC 2
- How to align your audit strategy with your growth goals
- Why starting with a readiness assessment is a smart-ROI move
- What to look for in an audit partner—not just a check the box provider
- Why two-year deals make sense

SOC 1

Mostly Relates to Financial Data

SOC 1 keeps your CFO out of hot water. SOC 2 keeps your clients from walking away. Choosing the right report—or combination—starts with understanding what's at stake.

SOC 2

Mostly Relates to Client Data

If your service impacts a client's financial reporting, you need a SOC 1. If you handle customer data or run on the cloud, you need a SOC 2. Some organizations need both—and knowing the difference protects your credibility and your contracts.

What's Really at Stake

Boardrooms are demanding stronger assurances. Clients are writing security requirements into every RFP. Regulators are tightening expectations with no sign of easing up. For today's technology and security leaders, demonstrating operational control isn't a value-add—it's the price of admission.

SOC audits have become more than a compliance exercise. They're a direct reflection of your organization's credibility, maturity, and readiness to scale. Whether you're building your first compliance roadmap or reevaluating your current audit partner, understanding the real differences between SOC 1 and SOC 2 is critical.

+68%

Customer Trust

According to a survey by the Information Systems Audit and Control Association (ISACA), 68% of organizations that achieved SOC 2 Type 2 compliance reported increased customer trust and satisfaction.

Readiness as an extension of governance

Why Starting with a Readiness Assessment Is a Smart-ROI Move

For CISOs and CTOs operating in high-stakes, regulated environments, a readiness assessment is not a preliminary formality—it's a critical mechanism for reinforcing governance and aligning internal teams ahead of a formal SOC 1 or SOC 2 audit. Diving headfirst into a SOC 1 or SOC 2 audit without a clear understanding of control gaps, team responsibilities, or documentation standards. Don't introduce unnecessary risk and disrupts execution into the process. Instead, engage with a qualified partner to lead a structured readiness assessment who will brings focus, clarity, and accountability to the process—before the audit formally begins.

Engaging with a qualified partner significantly reduces the burden on internal teams. Instead of diverting engineering, security, and operations staff to untangle compliance frameworks, a readiness partner translates requirements into actionable priorities, identifies control gaps early, and ensures documentation is both complete and audit-appropriate. This approach streamlines internal coordination and minimizes rework, while allowing your teams to remain focused on core business and innovation objectives.

Think of it this way, readiness is not about checking boxes—it's about embedding discipline and structure into your culture so that your organization moves into the audit phase prepared, aligned, and with minimal disruption.

THEALCHEMIGROUP.COM

93%

Companies that align audit strategy with go-to-market goals see a 33% faster sales cycle when selling into regulated industries.

—Forrester

82%

82% of high-growth tech companies cite SOC 2 compliance as a key differentiator when entering new markets.

—TechTarget Research

67%

67% of enterprise buyers say a lack of third-party audit reports (like SOC 2) is a deal-breaker in the procurement process.

—Gartner

How to Align Your Audit Strategy with Growth Goals

As your company scales, the stakes around risk, compliance, and customer trust rise exponentially. An audit strategy shouldn't be an afterthought or a checkbox—it should be a key driver of growth. When aligned properly, the right audit framework doesn't just meet regulatory expectations; it reinforces your operational maturity, accelerates deal cycles, and opens doors to new markets. Whether you're considering SOC 1, SOC 2, or both, the decision should support your broader vision—*not slow it down.*

Start by looking at the kinds of customers you're targeting. Are you selling into financial services, healthcare, or publicly traded enterprises? These industries often demand SOC 1 Type II reports that validate the controls relevant to financial reporting. On the other hand, if your growth plan involves scaling a SaaS platform, SOC 2 compliance may carry more weight—especially for proving security, availability, and confidentiality controls to discerning tech buyers. The right audit pathway should mirror your ideal customer profile and the level of scrutiny they expect.

Equally important is understanding the timing of your audits. If your team is mid-product launch, in funding mode, or preparing for M&A activity, rushing into a full audit can create unnecessary friction. A phased, strategic approach—such as starting with a readiness assessment—can align audit milestones with your operational bandwidth. It also signals control maturity to external stakeholders without derailing internal priorities.

CISOs, CTOs, and CFOs each bring a critical lens to this alignment. The CISO wants defensible security posture, the CTO needs scalability without bottlenecks, and the CFO seeks clean audit trails to support revenue recognition and investor confidence. A coordinated audit strategy addresses all three, creating shared accountability around data integrity, internal controls, and third-party risk management.

Most importantly, an audit strategy tied to growth isn't static. It evolves with your business. Today, you may need **SOC 2 Type I** to close enterprise accounts; next year, **SOC 2 Type II** or **ISO 27001** may become essential to support global expansion. Aligning your audit approach with your roadmap ensures you're not over-auditing—but you're also never underprepared when the next opportunity hits your desk.

A trusted audit partner will help you choose and execute the right compliance path at the right time. It's not just about passing audits—it's about using compliance to propel the next chapter of your business.

Compliane that moves the needle

Who Governs SOC 1 and SOC 2

The American Institute of Certified Public Accountants (AICPA) is the governing authority behind both SOC 1 and SOC 2 reports, establishing the standards for how service organizations demonstrate control over financial reporting and operational security. SOC 1 is rooted in the AICPA's SSAE 18 standard, while SOC 2 is built on the Trust Services Criteria—each framework is designed to address distinct types of risk. For executives, understanding these frameworks is essential not just for compliance, but for building trust with stakeholders, auditors, and risk-conscious customers.

The Trust Services Criteria (TSC) are the control framework used in SOC 2 reports. They focus on non-financial operational controls, particularly how systems and data are managed.

Understanding the Frameworks Behind SOC Audits

There are five core categories, and organizations choose the ones most relevant to their business and customer base:

- **Security:** Protecting systems from unauthorized access (required in every SOC 2).
- **Availability:** Ensuring systems are up and running when promised.
- **Processing Integrity:** Making sure systems process data accurately and on time.
- **Confidentiality:** Safeguarding sensitive business information.
- **Privacy:** Protecting personal data according to privacy commitments & regulations.

	SSAE 18 (SOC 1)	Trust Services Criteria (SOC 2)
GOVERNED BY	AICPA	AICPA
FOCUS AREA	Financial Reporting Controls	Data Security and System Control
FRAMEWORK	SSAE 18 Stsandard	Trust Services Criteria (Security, Availability, etc.)
AUDIENCE	Client CFO's Auditors	Clients. Partners, Procurement Teams
TYPICAL USER	Payroll, Fintech, Claims Processors	SaaS, cloud, healthcare tech, managed services
KEY REQUIREMENTS	Controls affecting financial statements	Controls protecting client data
REPORT TYPE	Type 1 or Type 2	Type 1 or Type 2

The TSC helps you show customers, partners, and regulators that your technology, policies, and teams are set up to protect data and run systems securely and reliably.

SOC Compliance Is No Longer Optional—It's a Strategic Imperative

Strategic Compliance For Growth & Trust

According to a 2024 benchmark study, the number of SOC 2 reports issued nearly doubled year-over-year, underscoring the growing demand for independently validated security and compliance controls. As companies face heightened scrutiny from clients, regulators, and investors, SOC reports—especially SOC 2 Type 2—have become essential tools for demonstrating maturity, trust, and readiness to scale.

While certain industries like finance and healthcare have long embraced audit reporting, others are rapidly catching up. A recent compliance study found that SOC 2 adoption in sectors such as construction, agriculture, and manufacturing—traditionally less focused on cybersecurity—has grown between 3–6%. This broadening adoption signals a shift: assurance reporting is no longer limited to regulated industries; it's now a key differentiator for any service provider seeking to win and retain enterprise business.

The cost of inaction is steep. In 2024, the average data breach cost rose to $4.88 million, reinforcing the critical role of internal controls and third-party audits in preventing operational and reputational loss. A robust SOC 2 compliance program not only mitigates risk—it signals to clients and partners that the organization is proactive, not reactive, when it comes to protecting sensitive data and ensuring business continuity.

Compliance can also drive competitive advantage. Organizations with a current SOC 2 Type 2 report experienced sales cycles up to 30% faster than those without, largely due to reduced friction during procurement, vendor assessments, and security reviews. For sales and executive teams, this translates into accelerated time-to-revenue and improved close rates—benefits that extend far beyond IT or audit departments.

Perhaps most notably, compliance is no longer viewed as a cost center or check-the-box exercise. Nearly 70% of corporate risk leaders now approach SOC and related frameworks as strategic investments. This evolution reflects a growing awareness that strong compliance programs strengthen business resilience, enhance stakeholder trust, and align teams around a unified risk posture.

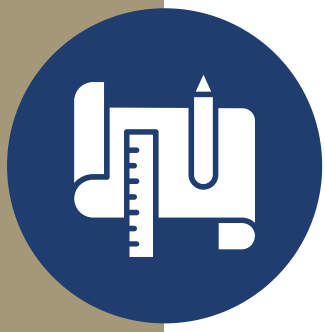
For executives deciding between SOC 1 and SOC 2, the question isn't just which report to pursue—but how to position it as part of a broader strategy for growth and long-term value creation.

Conclusions :

SOC reports have evolved from regulatory requirements into strategic instruments—demonstrating operational maturity, building stakeholder trust, and unlocking market opportunities. Whether pursuing SOC 1, SOC 2, or both, the organizations that lead don't leave success to chance. They plan deliberately, invest in readiness, and choose audit partners who go beyond the checklist. Now is the time to elevate your approach: validate your controls, align your roadmap, and engage a team that brings insight—not just oversight. A readiness assessment, a fresh perspective, and a long-term strategy aren't just smart—they're essential. Own the process. Signal your commitment. And set a higher standard.

Start With Readiness Assessment

Rushing into an audit without a readiness assessment is a common and costly mistake. Readiness assessments identify control gaps, clarify scope, and establish a realistic timeline for remediation—reducing risk and accelerating success. Key steps include stakeholder interviews, control evaluations, gap analysis, and remediation planning. Organizations that invest in this phase cut audit timelines by 20–30% and are significantly more likely to pass on the first attempt.



Choose the Right Audit Firm

Your auditor should be more than qualified—they should be strategic. Look for deep industry experience, clear communication, and a scalable approach. Ask about continuity, remediation support, and whether they offer value beyond issuing a report. If you've worked with the same partner for several years, a second opinion can uncover blind spots or more efficient approaches.

The Strategic Advantage of Two-Year Engagements

High-performing organizations increasingly opt for two-year SOC audit agreements. This model locks in pricing, preserves continuity, and allows the audit team to align with internal roadmaps. It's also a signal to the market: you're not just compliant—you're committed.

Final Takeaway

SOC reports are no longer just a checkbox—they're a strategic asset. Whether SOC 1, SOC 2, or both, success starts with clarity, planning, and the right partner. If you're navigating this process again—or for the first time—make it count. Consider a readiness assessment, get a second opinion, and take control of the process on your terms.

LET'S TALK STRATEGY

Whether you're preparing for your first SOC audit or reassessing your current approach, Alchemi Advisory Group is here to help you move forward with clarity and confidence.

Connect with our team to schedule a readiness assessment, request a second opinion, or explore a long-term SOC strategy tailored to your business.

Prefer to start with a conversation? Reach out for a confidential consultation with one of our senior advisors.

CONTACT US

Alchemi Advisory Group
info@thealchemigroup.com
(888) 590-1618
thealchemigroup.com

ALCHEMI
ADVISORY GROUP