Phonexa®

SOC COMPLIANCE CHECKLIST: CONTROL OBJECTIVES, COMPLIANCE CRITERIA & MORE

Service Organization Control compliance is critical for companies that handle, store, process, or impact their user entities' and clients' financial or other sensitive data. This checklist and guide offers robust detail and direction on what tech companies subject to SOC 1 and SOC 2 data audits can do to ensure compliance.

Table Of Contents

SOC 1 & SOC 2 Basics: Objectives, Audits, & Reports

Testing Methods & Examination of User Controls

Types of Reports

Checklist: Pain Points, Misinterpretations, & Qualified Opinions

Defining the Main Objectives of SOC 1 and SOC 2 Compliance

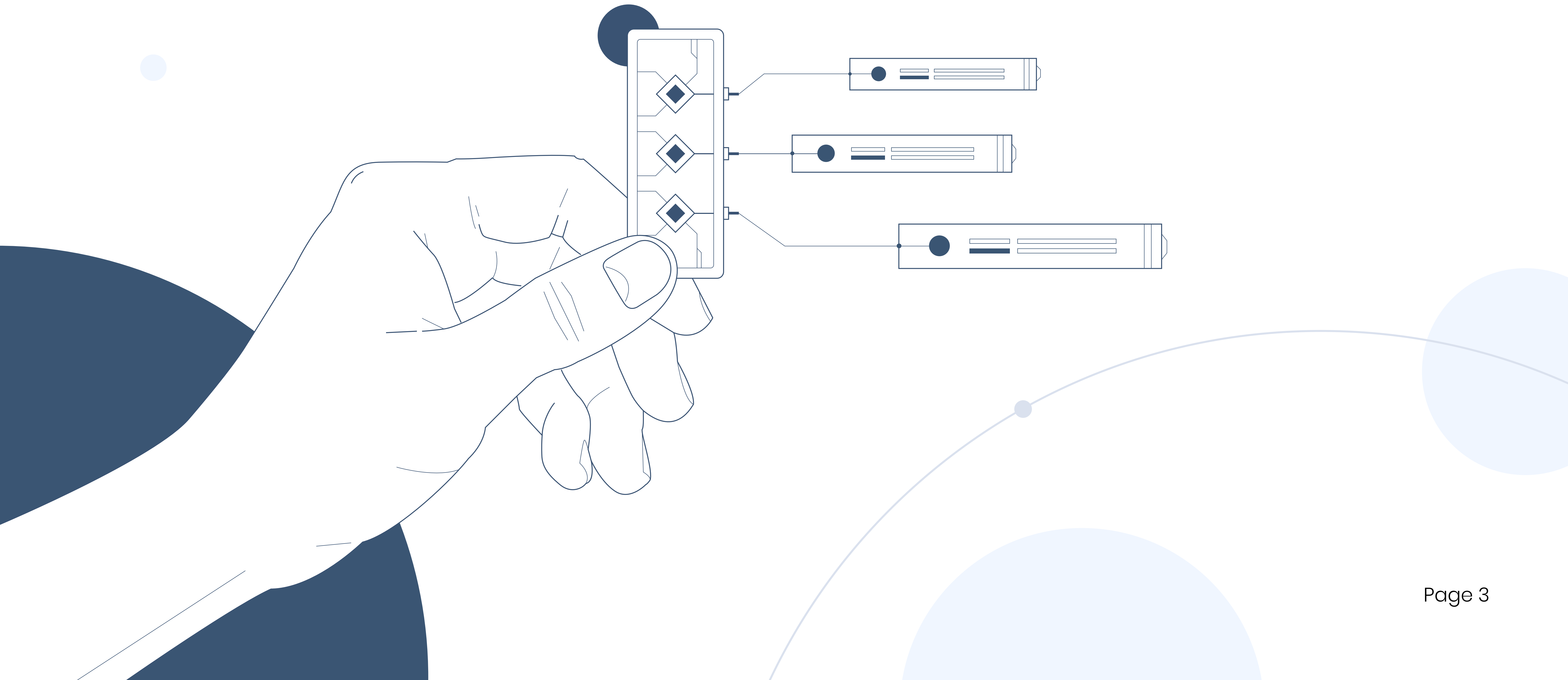
There are common misconceptions around the topic of issuing SOC reports, and if they are mandatory or not. Although SOC compliance may not be not required for all, for some companies, it becomes mandatory because of the clients they work with, or the services they provide. However, issuing a SOC report illustrates to partners and clients that an organization is fully capable of securing confidential information.

SOC 1 and 2 reports help subjected bodies better understand processes and controls by testing the security of their information systems. The main objective is to ensure service organizations adhere to set controls and objectives designed to protect customer information, confidential human resource data, personally identifiable information (PII) of employees, and intellectual property.

SaaS providers aren't legally required to comply with SOC 2 regulations. However, SOC 2 compliance provides clients with peace of mind by enhancing a SaaS organization's security posture. A SOC 2-compliant organization is equipped with industry-leading security that builds trust with clients by ensuring customer data is safeguarded at all times.

The standards of SOC 1 and SOC 2 audits are upheld by the SSAE 18 (Statement on Standards for Attestation Engagements), a series of improvements developed to enhance the quality of SOC reporting. After an organization's controls are analyzed, a determination is made on whether its controls are adequate.

SOC 1 and SOC 2 reports are divided into two categories — SOC 1 Type I and Type II reports and SOC 2 Type I and Type II reports.



The Latest Revisions on SOC Compliance, as Enforced by the AICPA

During the fourth quarter of 2022, the AICPA revised its guidance on applying Trust Services Criteria and Description Criteria for SOC 2 reports. The Description Criteria is a set of benchmarks to be utilized by a service organization when generating a description of its internal controls for a SOC 2 audit.

The revisions guide technological vulnerabilities, threats to confidentiality, privacy issues, and disclosures made by service organizations when preparing a SOC 2 report. These modifications are intended to improve the way organizations serve the information needs of their partners and clients.

As a result, these organizations can better assess whether changes to their internal controls — and consequently their SOC 2 reporting — are necessary.

This is especially important for incident response teams dealing with SOC fatigue, which can result in employee burnout, increased vulnerability to security incidents, and diminished financial returns.

SOC Compliance Framework: Audit Standards & Reports

SOC 1 Framework

A SOC 1 audit is conducted by an independent Certified Public Accountant (CPA) who must adhere to the most recent updates to each type of audit established by the American Institute of Certified Public Accountants (AICPA).

Audit reports examine how financial information related to clients is handled by service organizations to assess whether the subject data is managed securely. SOC 1 reporting evaluates a service organization's defined controls and capacity for protecting client information and mitigating financial risk.

SOC 2 Framework

SOC 2 protocols specified by the AICPA are based on Trust Services Criteria, encompassing security, availability, processing integrity, confidentiality, and privacy. A SOC 2 audit examines information security related to operations and compliance and is performed by an auditor from a licensed CPA firm.

The SOC 2 report outlines the ability of a service organization — one that supplies systems and services (such as Phonexa) to client organizations — to safely secure business-critical information and client privacy.

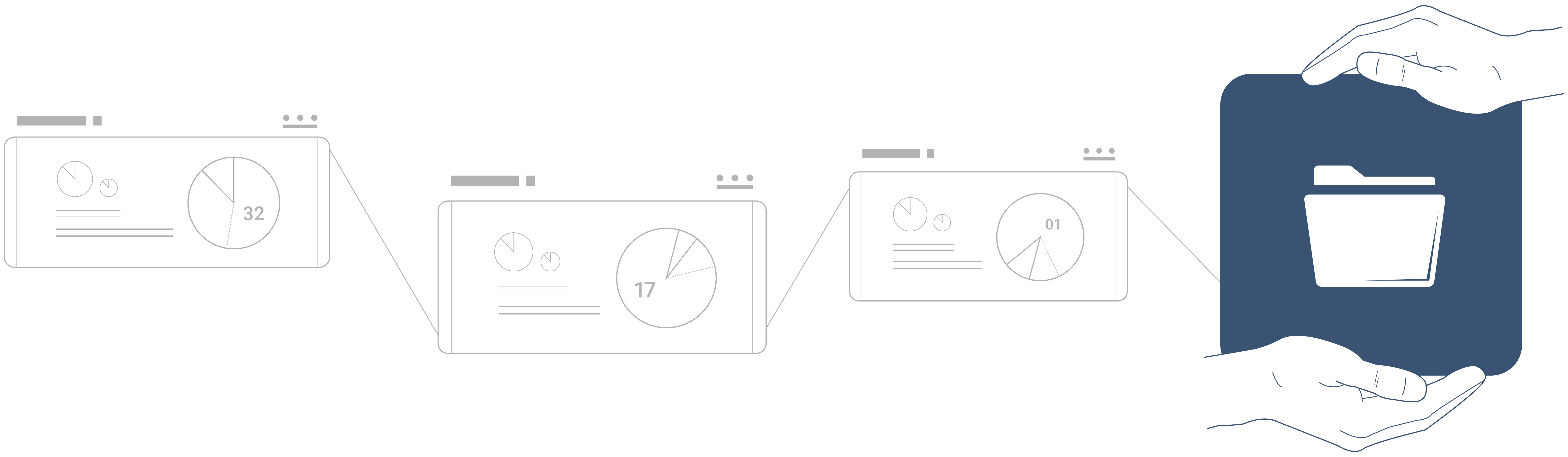
What Types of Organizations are Subject to SOC Audits?

SOC 1 Audits

SOC 1 audits apply to organizations that handle financial information for clients, and a report is generated by a third-party SOC Audit service. Organizations subject to SOC 1 auditing include SaaS managed service providers, loan servicers, registered investment advisors, trust departments, payroll processing firms, and employee benefit or retirement plan administrators.

SOC 2 Audits

SOC 2 audits are conducted to assess the design (Type I) and operating (Type II) efficacy of a service organization's controls for securing business-critical information and client privacy. Examples of service organizations subject to SOC 2 auditing include SaaS providers, managed IT and security service providers, software developers, host data centers, cloud service providers, business intelligence and analytics companies, human resource management services, and financial consultancy and accounting services.



Testing Methods

SOC 1 and SOC 2 auditors employ four testing methods designed to help them determine how suitable the design and how effective the operating controls in place are for the service organization in audit.

Read on to learn more about each method and the procedures they entail.

Inquiry Method

When utilizing the inquiry method, auditors probe the service organization's management and staff to gather information on how it stores its financial and data security records. The answers collected are then taken into consideration, but auditors do not solely rely on the responses as confirmation of the controls an organization currently has in place. As such, the inquiry method is typically used jointly with other testing methods to determine whether additional testing criteria are needed.

Observation Method

The observation method focuses on activities and operations — for example, observing the installation of a security camera system. This method proves useful for operation controls that lack proper documentation.

Examination Method (Inspection of Evidence)

The examination method, or inspection of evidence, determines if manual controls are being implemented through a thorough examination of organizational records and written documentation about system databases, employee manuals, and visitor logs.

Re-performance Method

The re-performance method requires an auditor to enforce controls manually and is used when the aforementioned methods cannot certify whether controls are operating effectively.

Examination of User Controls

As additional entities gain access to a service organization’s confidential data, the organization becomes exposed to possible risks including but not limited to unauthorized access, data breaches, and other security incidents. To evaluate the risks associated with systems and controls, a SOC auditor examines them and issues a report for management, clients, or other stakeholders, depending on the type of report generated from the audit.

Type I vs. Type II Reports

Type I and Type II reports differ in length and detail, yet both SOC 1 and SOC 2 audits share similar desired outcomes. Each type of report for both SOC 1 and SOC 2 audits should:

- Probe a service organization's internal controls (Objective)
- Offer expert opinion from the CPA who conducted the audit (Attestation)
- Specify all internal controls employed by a service organization (Controls)

Apart from these commonalities, SOC 1 and SOC 2 Type I and Type II reports evaluate different aspects of a service organization's internal controls.

SOC 1 Type I and Type II Reports

Auditors can conduct two SOC 1 audits — a SOC 1 Type I audit and a SOC 1 Type II audit.

A SOC 1 Type I audit reviews a service organization's financial reporting controls for a specified time period. This audit also helps auditors assess if the controls are appropriately designed and set up but don't verify their effectiveness.

A SOC 1 Type II audit inspects a service organization's internal controls over a period — typically a six- to 12-month review period — to determine whether or not these controls are properly designed and implemented. A Type II report also demonstrates if these controls operate effectively over a period of time.

SOC 1 reports are intended for review by internal auditors and management.

SOC 2 Type I and Type II Reports

Similar to SOC 1 audits, SOC 2 Type I and Type II audits also assess the design and operating efficacy of the controls employed by a service organization. However, a report generated from a SOC 2 audit focuses only on non-financial controls and must be conducted by the Trust Services Criteria established by the AICPA.

SOC 2 reports are generated for external stakeholders, including investors, customers, and suppliers.

Trust Services Criteria for SOC 2 Compliance

Trust Services Criteria defined by the AICPA is the framework for SOC 2 compliance. The Trust Services Criteria (TSC) encompasses five core elements for an organization's cybersecurity infrastructure.

The 5 Trust Service Categories

The Trust Service Criteria (TSC) include the following five categories:

1. **Security Criteria:** Assessing an organization's capability to protect confidential information from unauthorized access. Auditors using this criterion typically analyze an organization's cybersecurity infrastructure and any factors that may negatively or positively affect data security, such as multi-factor authentication.
2. **Availability Criteria:** Verifying that an organization's systems are reliable for employees and clients to complete tasks. Evaluating availability controls is especially imperative for SaaS and cloud service providers to identify threats that can disrupt business continuity.
3. **Processing Integrity Criteria:** Ensuring that internal systems function correctly helps auditors illustrate the types of data an organization needs to operate. This, in turn, allows organizations to resolve any detected errors.
4. **Confidentiality Criteria:** Limiting access, storage, and use of confidential information for a predetermined period of time. When the retention period expires, all confidential data must be destroyed.
5. **Privacy Criteria:** Securing Personal Identifiable Information (PII) from unauthorized access. Service organizations that collect PII from customers must obtain consent, limit the amount of data gathered, and collect all sensitive information lawfully. Service organizations must properly dispose of all PII upon using customer data for previously outlined purposes.

Which TSC Is Required for SOC 2 Compliance?

Complying with TSC standards is mandatory for all SOC 2 audits. The Security Criteria are tested using the SOC 2 Common Criteria list (CC series), which includes the following subcategories:

- **Control Environment (CC1):** Evaluates an organization's commitment to integrity and security.
- **Communication and Information (CC2):** Shows how policies, procedures, and other control objectives are communicated to internal and external parties.
- **Risk Assessment (CC3):** Assesses an organization's analysis of risks and how it tracks potentially impactful changes.
- **Monitoring Activities (CC4):** Documents how an organization evaluates and communicates the usefulness of its internal controls.
- **Control Activities (CC5):** Illustrates the types of processes, controls, and technologies employed to mitigate risks.
- **Logical and Physical Access Controls (CC6):** Demonstrates the security measures used to safeguard data and prevent physical access to servers.
- **System Operations (CC7):** Reviews the functionality of an organization's systems.
- **Change Management (CC8):** Determines how an organization tests and approves material system changes.
- **Risk Mitigation (CC9):** Evaluates whether proper business processes and vendor management is in place to limit potential risk.

It's important to note that the other four TSC categories may also be required depending on your organization's services.

Common Pain Points & How to Overcome Them

Preparing for an audit is a multilayered process, especially a SOC 2 audit, which usually takes five weeks to three months to complete. When an audit takes longer to complete, service organizations are often left scrambling to appease customers during the prolonged process. In this instance, an organization's management can issue a ***bridge letter*** to customers that bridges the gap between its previous SOC 2 report and the current period.

Issuing a SOC 2 Bridge Letter

A bridge letter is typically used to communicate that no substantial changes to internal controls have occurred since an organization's most recent SOC 2 report. In the event that material changes have occurred since the previous report, a bridge letter can communicate to customers that these changes haven't affected the results of the report's findings.

Keep in mind that a bridge letter does not serve as an updated SOC 2 report and only covers a period of three months.

Overcoming SOC Fatigue

SOC fatigue occurs when IT staff become desensitized to frequent alerts stemming from any detected irregularity. According to a study conducted by Trend Micro, 55% of the 2,303 IT security and SOC decision-makers polled admitted that they lack confidence in their ability to prioritize alerts and respond to and manage them in a timely manner.

Service organizations can alleviate SOC fatigue by implementing the following solutions:

- **AI:** Organizations subject to SOC audits can employ AI solutions to prioritize high-severity alerts while decreasing the frequency of low-severity alerts. AI solutions can identify and analyze security alerts and prioritize them based on the severity of the irregularity or threat detected.

- **Automation:** In addition to utilizing AI solutions, service organizations can leverage real-time automation to automate responses to alerts that don't require human intervention. Doing so greatly reduces the workload for response teams, providing them with more time to focus on analyzing patterns and identifying potential threats before they occur.

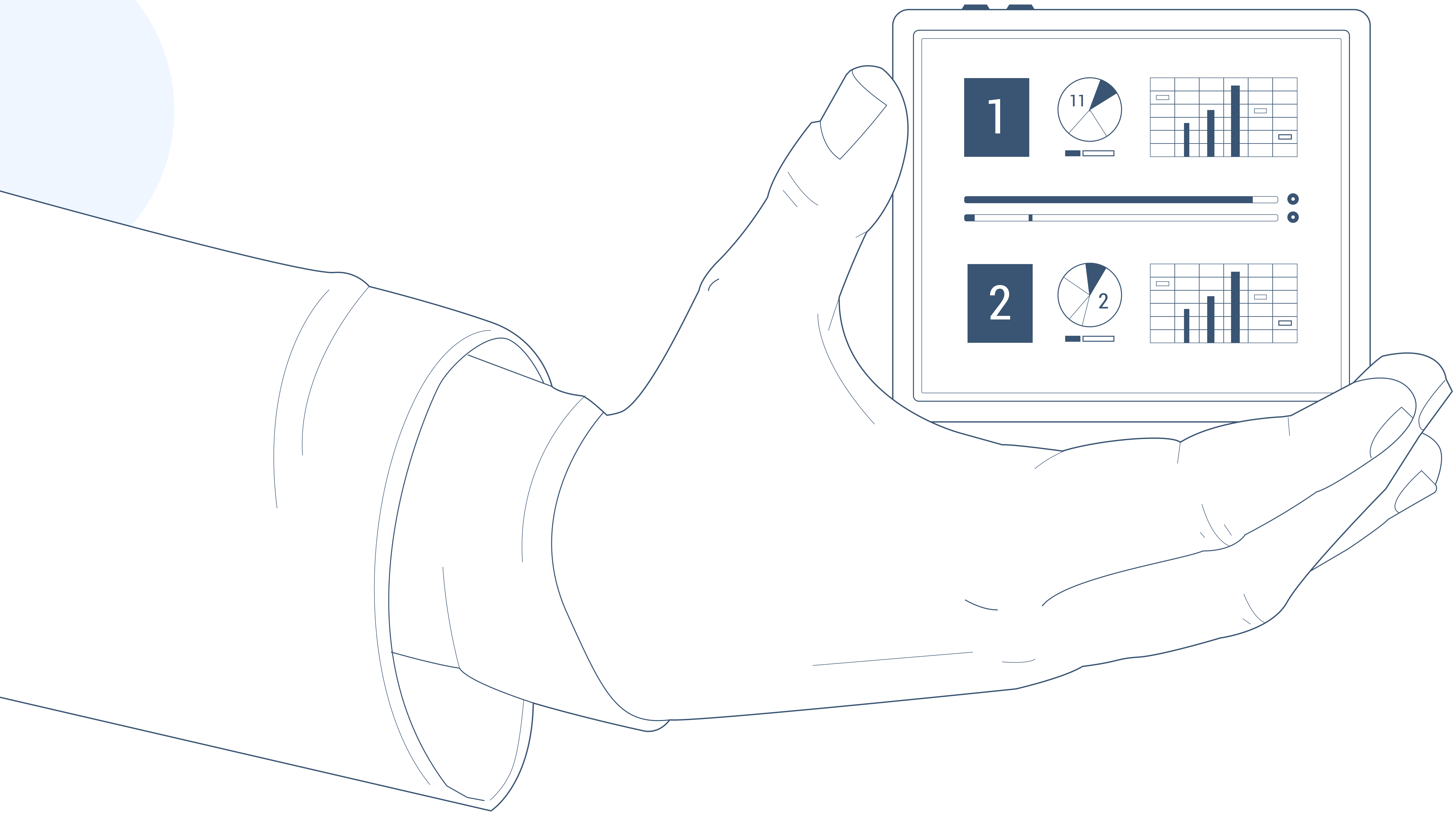
- **User Behavior Recording & Analytics:** Organizations can better identify and assess imminent threats by recording and analyzing user behavior on their websites and web pages. Specifically, behavior analytics help response teams uncover abuse of privilege and potential insider threats.

Should Your Organization Comply With SOC 1 or SOC 2? Factors To Consider

Issuing a SOC report is good practice since customers can request a report and, in some cases, may even be required as part of their contract with your organization.

SOC 1 reports are beneficial for organizations that have revised their internal controls or amended the services they offer since their most recent SOC audit. In some cases, an organization may have yet to be audited, which is more reason to generate and issue a SOC 1 report.

SOC 2 reports provide transparency regarding a service organization's commitment to securing its internal controls. A SOC 2 report also helps communicate whether any significant changes have been made to the organization’s systems, controls, or operations. Maintaining a high level of transparency and accountability is invaluable for SaaS and cloud service providers.



Check Yourself: Is Your Organization Compliant?

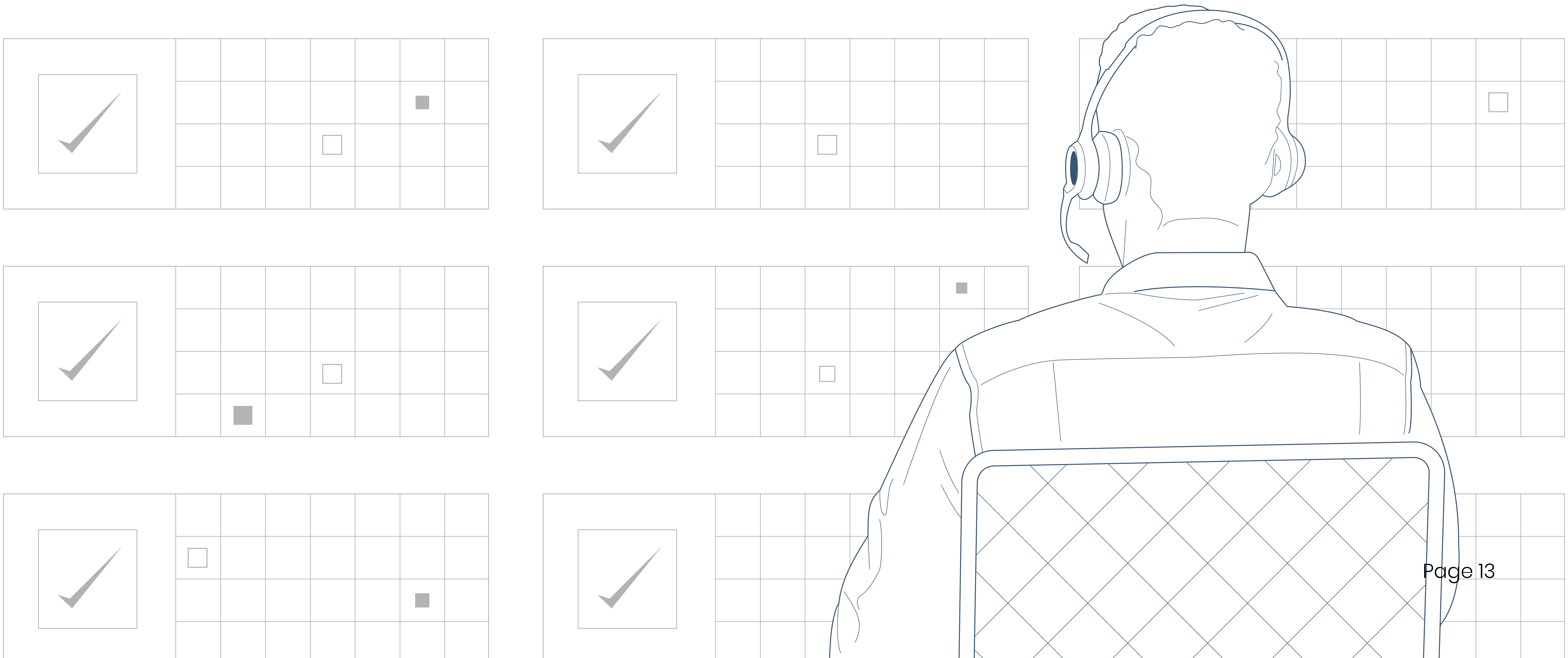
It should be noted that there are no specific guidelines provided by the AICPA on how to prepare for a SOC 2 audit. However, organizations can begin preparing by distinguishing between SOC 1 and SOC 2 standards to determine which assessment best suits their operational needs.

Organizations willing to undergo a SOC 1 audit can prepare by following these four critical steps:

☑ Select a reputable CPA firm to perform the audit
☑ Perform a scoping and readiness assessment to determine which controls require remediation
☑ Compile all the necessary information security and operational documents needed for review by auditors
☑ Identify which control objectives must be outlined in the SOC 1 report

Organizations seeking a SOC 2 audit report can start the process by following these three steps:

☑ Complete a readiness review to define its business process and identify internal controls needing remediation
☑ Conduct a risk assessment of key operational initiatives, including developing an emergency contingency plan and enforcing employee security awareness training
☑ Collect all the necessary logs, reports, and other documentation required by SOC 2 auditors for review



The Benefits of Working With SOC 1 & SOC 2 Compliant Tech Providers

Business relationships are built on transparency and trust, especially for service organizations operating in the tech industry.

Phonexa has met security requirements for the present and future with SOC 2 Type 1 & 2 Certifications due to its most recent audit from an independent auditor, which means that Phonexa clients get:

- Security against attacks
- Processing integrity
- Data confidentiality

SOC 1 Compliant Tech Providers

As tech service providers expand into different verticals, SOC 1 compliance allows these organizations to strengthen their GRC (governance, risk, and compliance) posture. SOC 1 compliance ensures that an organization has the proper controls — general IT controls and business-process-related controls — in place to fulfill control objectives.

SaaS companies and other tech service providers unsure if they should invest in SOC 1 certification must consider the following benefits:

☑ An external auditor can identify vulnerabilities to an organization's controls that an internal auditor may have overlooked during prior assessments. This is often the case for startups that fail to comply with SOC 1 regulations.

☑ Once policies and procedures are assessed during a SOC 1 audit, an organization can pinpoint areas for improvement and make necessary adjustments to enhance its operations.

☑ Most importantly, obtaining a SOC 1 report helps establish trust between a service organization and its clients.

SOC 2 Compliant Tech Providers

SaaS providers that offer software fortified with SOC 2 certification have an advantage over their competitors by providing clients and partners with assurance that their security controls comply with globally recognized standards.

Among the many benefits of a SOC 2 audit for SaaS companies and other tech service providers are the following:

☑ The vulnerability scans and pentests (penetration testing) performed in preparation for a SOC 2 audit allow organizations to properly evaluate their cybersecurity posture and make any necessary adjustments or improvements.

☑ Several of the prescribed measures used by service organizations to get ready for a SOC 2 audit overlap with other regulatory requirements. Thus, a SOC 2 audit also serves as preparation for future audits pertaining to other compliance requirements.

☑ Ultimately, SOC 2 compliance builds trust among potential partners and clients, increasing the likelihood of establishing new relationships and driving revenue.

Phonexa Is a Tech Company That Touts SOC 2 Type 1 & 2 Compliance

Gain peace of mind by beginning the journey of working with a tech platform with SOC 2 certification.

Learn more

about how Phonexa's SOC 2 Type 1 & 2 compliance affects users, clients, partners, and its internal operations.

Follow Phonexa's Content Hub

to stay current and receive more content and tips on consumer privacy laws and regulations currently affecting the SaaS industry.

Phonexa is a performance marketing software and all-in-one marketing automation solution for calls, leads, clicks, email, SMS, accounting, and more. The company powers direct advertisers and lead generators alike across all businesses and industries by optimizing inbound web and call campaigns, and outbound call, email, and SMS campaigns — all while having the ability to enhance the consumer journey along every step of the way. Complete with a suite of turnkey marketing products and solutions, Phonexa's customizable tools are uniquely designed to maximize workflow efficiency and revenue. Phonexa has the scalability, tools, and partnerships to serve clients across industries, especially those with high consumer demand products and services. The company is headquartered in Los Angeles with additional offices in the United Kingdom and Ukraine. For more information, please visit **www.Phonexa.com**.

Contact us

Phone: **818-800-0000** Email: **sales@phonexa.com**

505 North Brand Boulevard, 16th Floor, Glendale, CA 91203

Schedule a consultation