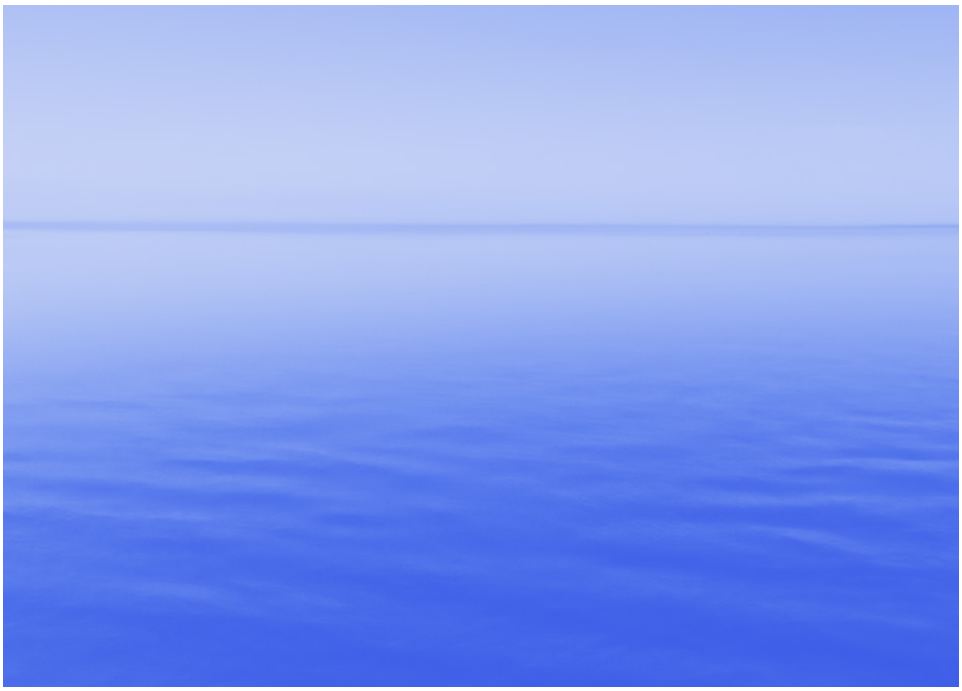
Clearwater

Whitepaper

Preparing for SOC 2: The How & Why for Healthcare Service Providers

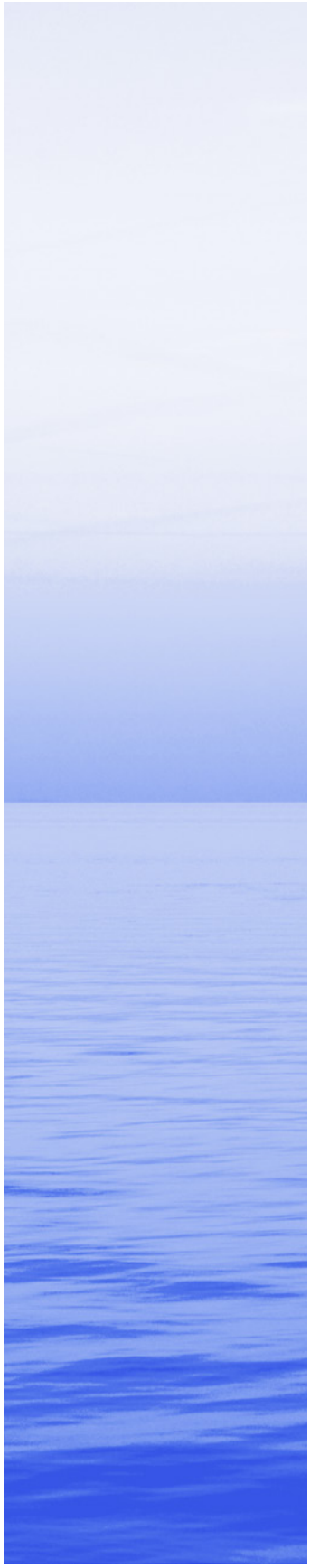
Table of Contents



© Clearwater | All Rights Reserved | 43.1

Introduction

Establishing trust and addressing customer concerns about security is paramount to success. Your customers are vigilant about the risks associated with adopting new solutions, and they expect reassurance that you have taken adequate measures to protect their organization and patients. Third-party validation, such as a SOC 2 audit or HITRUST Certification, is often a contractual requirement of your customers. However, it's essential to carefully consider the effort and cost involved in obtaining and maintaining these certifications and where you can maximize this investment. We will focus on the SOC 2 audit and the level of assurance it provides, in addition to outlining the process and the investment required and determining the optimal timing to embark on this audit journey. A big value of a SOC 2 Audit is the independent third-party assessment which can only be conducted by a licensed CPA firm or agency accredited by the American Institute of Certified Public Accountants (AICPA).



Understanding SOC 2 audit basics

A SOC 2 (System and Organization Controls 2) report is an independent audit report that evaluates the controls implemented by a service organization to protect data security, availability, processing integrity, confidentiality, and privacy. It is based on the criteria defined by the American Institute of Certified Public Accountants (AICPA).

The SOC 2 compliance report is commonly asked as a basic requirement by entities that subscribe to or partner for services, such as cloud service providers, data centers, software-as-a-service (SaaS) companies, and other organizations that may fall into the healthcare business associate category because they store, create, or process sensitive information. It assures customers and stakeholders that the organization has implemented adequate policies, procedures, and controls and follows those to protect the data in their custody.

The SOC 2 audit and subsequent report assesses an organization's internal controls and processes related to a defined criteria and scope, which typically includes security, availability, processing integrity, confidentiality, and privacy. These criteria are the AICPA Trust Services Criteria (TSC). The report is the findings prepared by an independent third-party auditor who examines the organization's controls, conducts testing, and provides an opinion on the effectiveness of those controls.

© Clearwater | All Rights Reserved | 43.1

Auditing criteria and controls

Let's look at the specific implications of the auditing criteria for healthcare business associates or digital health services:

Security:

Security is paramount in the healthcare industry due to the sensitivity of patient data and privacy. While the HIPAA security rule applies to healthcare entities, those providing services to providers or focusing on consumers regarding their health and sensitive data also need to establish strong security programs. Implementing robust security measures to protect against unauthorized access, data breaches, and other security threats depends on the type of services provided and the systems and environments foundational for the business. Being able to evaluate the systems and processes that are driving the digital health evolution needs to consider security basics but also measure the effectiveness as the development and delivery environments evolve. These would include implementing access controls, encryption, secure authentication mechanisms, network security, incident response procedures, and regular security assessments.

Availability:

Maintaining high availability ensures essential access to critical healthcare services and health or patient information. Downtime or system unavailability can have severe consequences for care coordination and outcomes. The audit will review the effectiveness of using redundant infrastructure, disaster recovery plans, data backup system integrity, and threat monitoring to ensure the continuous availability of their services.

Processing Integrity:

Processing integrity focuses on transactions and data accuracy, completeness, and overall reliability. Best practices should include designing and implementing controls to prevent data corruption and unauthorized data alterations and address or mitigate any errors during data processing. The audit will review data validation checks, error detection and correction mechanisms, audit trails, and the data reconciliation processes.

Confidentiality:

Confidentiality is crucial to protect patient privacy and also comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy rule. An audit will review

© Clearwater | All Rights Reserved | 43.1

access control implementation, encryption, the use and configuration of secure transmission protocols, data anonymization techniques, and the overall policies and procedures for handling sensitive information.

Privacy:

Privacy focuses on properly collecting, using, retaining, and disclosing personal information. Health IT and Digital Health companies must comply with relevant privacy laws and regulations, such as HIPAA, and any business applicable regulations, such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA) or other specific state or local legislation. An audit will examine the privacy policies and procedures, how consent is obtained for data usage, whether the business provides transparency about its data practices, and whether it implements appropriate safeguards to protect personal information.

This AICPA TSC is a guideline for companies to develop and maintain strong controls in their systems and operations. Compliance with these criteria and the third-party auditor findings and attestation helps builds trust and creates a stronger healthcare ecosystem by demonstrating a commitment to security, privacy, and data integrity.

SOC 2 audit scope and types

This type of audit does have some flexibility, and it is essential to review the specific details of any SOC 2 report to understand the scope of the assessment and the controls covered in the evaluation.

Depending on an organization's needs, they can limit their SOC 2 audit to the TSC of security. The auditor will review the criteria or list of requirements as identified by AICPA. The controls that you implement to meet these requirements are up to you. It will be the auditor's job to attest to the design and effectiveness of these controls in meeting the criteria. Adding more TSCs to the audit (privacy, availability, processing integrity, or confidentiality) will add to the overall requirements a business needs to meet and the controls your organization will have to implement and manage successfully. This is important when reviewing any assessment or final attestation for SOC 2 reporting.

In addition to determining which criteria are included, a SOC 2 report also indicates the timeline in which the assessment reviewed an organization's ability to meet the necessary in-scope criteria. There are two types of SOC2 reports – Type 1 and Type 2. The main difference between them lies in the period they cover and the level of assurance they provide. Here's a breakdown of each type:

© Clearwater | All Rights Reserved | 43.1

SOC 2 Type 1 Report:

A Type 1 report evaluates the design and implementation of controls at a specific point in time. It provides an independent auditor's opinion on the organization's system and control descriptions and their suitability for meeting the Trust Services Criteria (TSC) in scope. The Type 1 report assesses the controls in place at a specific moment and does not cover the effectiveness of those controls over a period of time. It is typically a one-time assessment and provides a snapshot of the organization's control environment at a specific date.

SOC 2 Type 2 Report:

A Type 2 report goes a step further and evaluates controls over a specified period, usually at least six months and up to a full year. It includes assessing control design and implementation, like a Type 1 report but also evaluates those controls' operational effectiveness over time. The Type 2 report provides a more comprehensive understanding of how well the controls have been functioning and whether they have been operating effectively throughout the assessment period.

In summary, a Type 1 report assesses controls at a specific point in time. In contrast, a Type 2 report assesses controls over a specified period and includes an evaluation of their operational effectiveness over this time period. Type 2 reports are generally considered more valuable because they provide insight into the ongoing effectiveness of controls, demonstrating an organization's commitment to continuous security and compliance.

Preparing for a SOC 2 audit

Preparing for a SOC 2 audit is a comprehensive process that requires careful planning and implementation of various controls and processes before scheduling an assessment.

Considerations before moving immediately to a formal SOC 2 audit:

- Understand the SOC 2 Trust Services Criteria (TSC) defined by the AICPA. Identify what your organizational needs are from this attestation. Should all of the TSC criteria (security, availability, processing integrity, confidentiality, and privacy) be in scope, or is security and a subset of these criteria acceptable?
- Understand your current state, specifically existing controls, and how they satisfy the criteria in scope. Have these been in place long enough or robust enough to meet the requirements for your targeted type of SOC 2 assessment? Ensure that controls are properly designed and implemented before the audit.

© Clearwater | All Rights Reserved | 43.1

- Define the business functions that will be in scope. Identifying the systems, processes, and services that will be included in the assessment. This involves identifying the relevant infrastructure, applications, data flows, and any third-party services or vendors involved. Health services and digital health are developing quickly. Review how environments like those supporting software as a service are isolated from corporate functions before a SOC 2 engagement.
- Document policies and procedures related to security, availability, processing integrity, confidentiality, and privacy. These documents should clearly outline how controls are implemented, who is responsible for them, and how they are monitored and maintained.
- Conduct internal testing and assessments to validate control effectiveness. This can include vulnerability scans, penetration testing, and internal audits to uncover any gaps or misconfigurations.
- Establish procedures for continuous monitoring and maintenance of controls. Regularly review and update your policies, conduct internal assessments, and address any changes in your systems or processes to maintain compliance with SOC 2 requirements.

Pre-assessment benefits for SOC 2 audits

A formal SOC 2 audit that does not go well immediately risks the organization's business opportunity, which drove them to seek this trust assurance in the first place. Under pressure, they now have limited time to improve or take action to remediate negative or significant recurring findings. The usefulness of the SOC 2 report, and third-party attestation, moves from an asset to a potential liability. For this reason, if your organization has not previously undergone this type of audit with success, there are benefits in performing a pre-assessment.

SOC 2 auditors only need certification from AICPA. Engaging with a reputable and independent third-party auditor with healthcare security and compliance experience before a formal SOC 2 assessment can deliver these added benefits:

- Assistance in defining the scope and value of the various options with SOC 2 Assessments, making the most of your audit investment.
- Emerging mobile, app, or cloud-built services used by digital healthcare or healthcare service provider solutions are complex. Having an auditor focused on security, IT operations, and healthcare can provide the right level of documentation details and analysis to make the subsequent SOC 2 audits easier.

© Clearwater | All Rights Reserved | 43.1

The pre-assessment deliverables give any following auditor the information to have assessments go quickly and remove any potentially high learning curve or costly additive assessment hours because of the utilization of advanced technologies or cloud environments.

- Uncover gaps in current controls and practices and obtain prioritization guidance. Where improvements or additional controls are required, understand the planning and implementation from a healthcare expert with deep operational expertise to optimize time and effort. Learn how to make the most of the needed changes and how they fulfill current requirements but can also provide value in the pursuit for additional types of assessments or certifications.

A SOC 2 pre-assessment will assess your controls, conduct testing, and provide an opinion on your compliance with the compliance criteria to ensure you achieve the favorable attestation needed to achieve your security and compliance goals.

Determining the right time for a SOC 2 audit

The decision to pursue a SOC 2 audit should be based on careful evaluation of the organization's needs, market demands, and competitive landscape. Factors to consider include the size of your organization, the complexity of your information systems, the nature of your customer base, and the level of regulatory oversight.

In general, healthcare services or digital healthcare companies should consider a SOC 2 audit when they have reached a stage of maturity where they can demonstrate a robust and well-documented information security program.

Determining the right time for a SOC 2 audit involves considering various factors. Here are some key considerations to help determine the optimal timing:

Business maturity is generally recommended so there are established processes, controls, and a solid foundation before undergoing a SOC 2 audit. Ensure that your organization has reached operational stability with well-defined policies and procedures. This includes the availability of financial and human resources needed to support the audit process.

Customer expectations and market demands can drive the need for a SOC 2 audit. If your customers increasingly request SOC 2 reports or a third-party validation of your security controls, it's likely a good indication that it's time to invest and pursue this audit. Responding to customer demands can enhance

© Clearwater | All Rights Reserved | 43.1

your competitiveness opening up new business opportunities.

Contractual obligations with customers, partners, or stakeholders. They may stipulate the need for a SOC 2 report or similar certification as a condition for doing business. Ensure you understand these obligations and align your audit plans accordingly.

Ultimately, the right time for a SOC 2 audit will depend on a combination of factors specific to your organization. It is beneficial to consult with internal stakeholders, compliance professionals, and experienced auditors to assess readiness and make an informed decision about the optimal timing for your company.

Coordinating other audits with SOC 2

As you consider SOC 2 Audits, there is much overlap with other healthcare-focused compliance assessments that you may also benefit from. Coordinating audits can help streamline processes, reduce duplication, and optimize resource allocation. While SOC 2 has become a defacto standard, its focus allows any type of organization to demonstrate the basic parameters for ensuring that they have considered and implemented controls to cover the AICPA Trust Services Criteria (TSC).

Other assessments that go beyond this general business trust attestation is one that looks at how healthcare services or digital healthcare organizations manage to ensure compliance with the HIPAA Security and Privacy Rules. Not necessarily a formal external report of attestation to be shared with customers and external entities but just as important for emerging and growing companies to perform that provides a third-party evaluation for executive, legal, investor and early contractual purposes.

Many healthcare business associates are also being asked to undergo and maintain a level of HITRUST certification. HITRUST-certified assessors review and report findings based on an organization meeting HITRUST CSF standards. This is meant to provide organizations a flexible and efficient approach to regulatory/standards compliance and risk management as HITRUST CSF continues to update and integrate changes to state and local privacy, security, and compliance requirements into its framework, minimizing the resources needed by smaller healthcare organizations to keep abreast of the compliance landscape.

© Clearwater | All Rights Reserved | 43.1

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact

© Clearwater | All Rights Reserved | 43.1