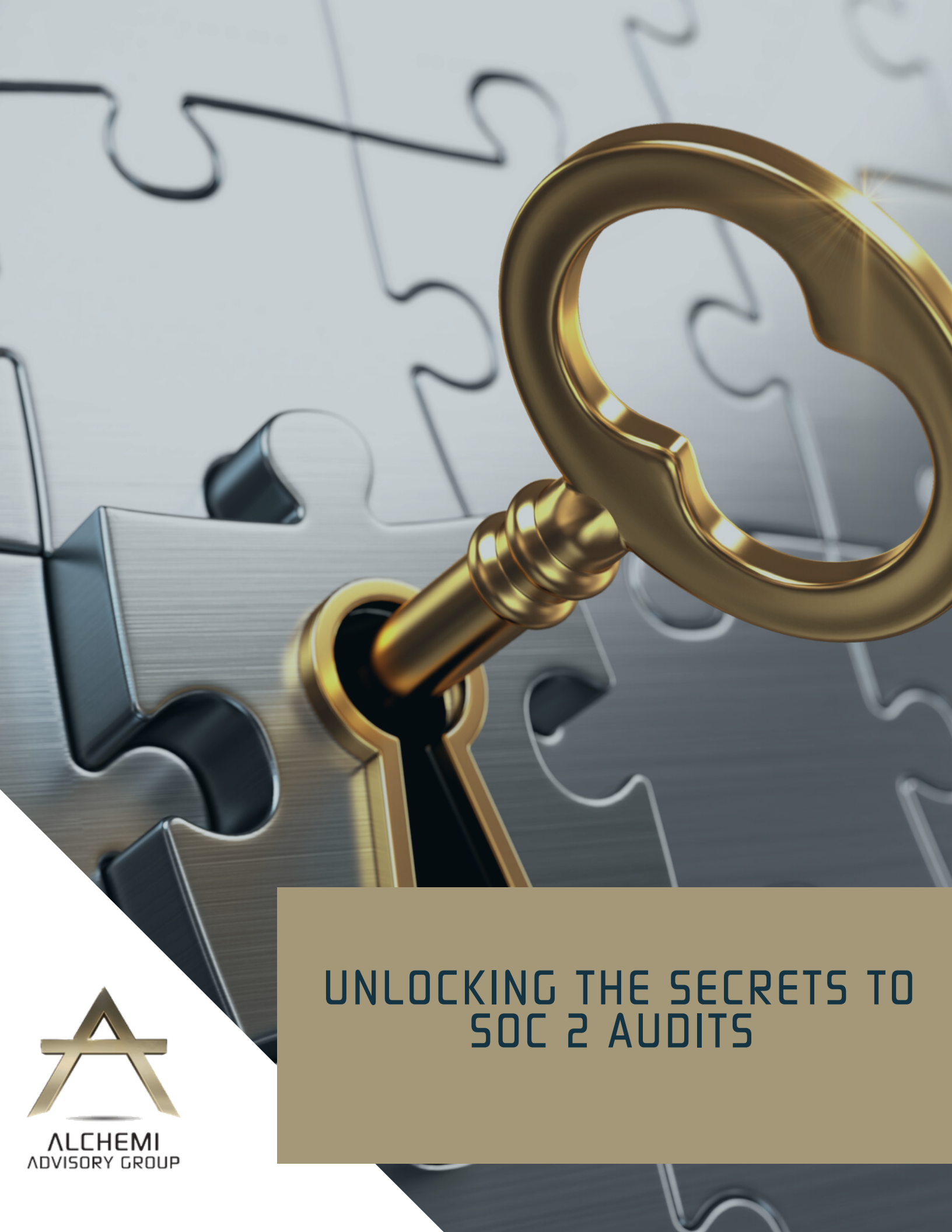


UNLOCKING THE SECRETS TO SOC 2 AUDITS

ALCHEMI
ADVISORY GROUP

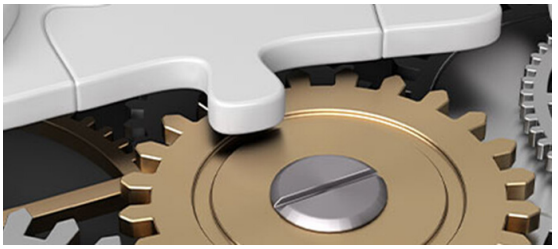
SOC 2 Audits and Reports Deliver Expert, Essential Information Security Advantages

Business and IT leaders face ever-increasing strategic and operational complexities and choices when tracking, supporting, managing and securing the information of customers, employees and business partners. Documenting and regularly assessing the systems, processes, controls and resources of your information security operation provide the foundation of trust necessary for your organization to compete, succeed and grow. Without such a foundation, and the attention, investment and resources to assess and verify information security on an ongoing basis, IT and business management put themselves, their employees, their partnerships, their very enterprise at serious risk, every day.

Fortunately, information security expertise, services and tools are growing at an unprecedented pace to meet demand. As the responsibility for understanding, managing and reporting on information security and IT risk grows, many organizations, across multiple industry sectors, supplement internal teams with expert advisors. These resources bring focus and discipline to answer the groundswell of time-consuming security and control questionnaires, and vendor audits, of processes, operations, applications and services in the era of SaaS managed- and cloud-based services, and distributed data centers. Third parties bring experience, authority, integrity, uniformity, rigorous processes and documentation to examine and verify that infrastructure, systems, software and services are reliable and can be trusted.

SOC 2 Reports on the Rise

One approach rising in infosecurity importance across technology-driven enterprises and increasingly contractually mandated in vendor monitoring programs are audits and reports based on the System and Organization Controls (SOC) 2 framework. Introduced by the American Institute of Certified Public Accountants (AICPA), SOC 2 was particularly designed for technology and cloud computing entities. SOC 2 attestation reports require a controls audit performed by a CPA firm, known as a Service Auditor, and provide a report on different levels of assurance and detail. Service Auditors are experts in the SOC 2 framework and how to assess a service organization's internal controls against the framework's five Trust Services Criteria (TSCs): *Security*, *Availability*, *Confidentiality*, *Processing Integrity*, and *Privacy*



SOC 2 is relevant for technology and cloud computing entities.

The TSCs align with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 17 internal control framework principles. Just as important, SOC 2 can serve as a reporting framework for any organization focused on information security and privacy issues, and using common standards such as the National Institute of Standards and Technology's Cybersecurity Framework, the International Organization for Standardization (ISO) 27001, and information security requirements rom Cloud Security Alliance, HITRUST and the Health Insurance Portability and Accountability Act (HIPPA) and other regulations.

SOC 2 certification is not a one-and-done exercise.

Embarking on a SOC 2 certification is not a one-and-done exercise. It is important to note that there is no industry or legal requirement behind SOC 2. And, for business and IT leaders, there will be important commitments: that controls will be performed consistently and that financial and other resources will support service auditor experts who will perform testing over a desired period and issue the attestation report. Initial examination periods can cover 6 to 12 months and there are typically annual reports after the initial assessment. In moving ahead, organizations realize their culture and practices must shift to a more formal framework of controls and testing, to help ensure favorable audit results—known as an unqualified opinion -- and satisfied customers and other business benefits.

The SOC 2 Audit Process and Project Management

Here's How It Works

Before describing the SOC 2 audit and report processes in some detail below, here's a brief list of key activities

- Determine the organization's SOC 2 audit business and technology drivers, and relevant systems to those drivers
- Determine audit scope, including applicable TSCs and critical processes
- Initial assessment and control design
- Remediation and readiness testing to correct control and design gaps, until results are in an acceptable range, as outlined below
- Reporting

The TSCs align with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 17 internal control framework principles. Just as important, SOC 2 can serve as a reporting framework for any organization focused on information security and privacy issues, and using common standards such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, the International Organization for Standardization (ISO) 27001, and information security requirements from Cloud Security Alliance, HITRUST and the Health Insurance Portability and Accountability Act (HIPPA) and other regulations.

Scope Considerations

The scope of a SOC 2 report depends on the type of service an organization provides, as well as the needs of its customer base. A thorough scoping exercise should determine which TSCs customers will require in the report outcomes, and which systems and components relate to those outcomes. The organization should also identify regulatory requirements to be included. This information is typically documented in contracts, service agreements, terms of use, and client requests.

Those involved should regularly apply key questions to filter the scoping exercise, such as: "Which Trust Services Criteria are relevant to our commitments to customers?" and "What period of time should be covered by the examination?" Another scope and timing consideration is when delivery date/timing for the report. Readiness assessments typically take a couple months to work through and can vary depending on where an organization starts its journey. Organizations with mature IT security and processes can expect shorter remediation paths while relatively immature organizations have longer remediation timeframes.

If the scoping exercise does not draw the system boundaries appropriately, customers may not be satisfied with the SOC 2 report and may request additional information, or even a separate audit. Getting the scope phase right is critical to the success of the SOC 2 process.

Readiness Assessments
Are you Prepared?

SOC 2 Readiness Assessment

High-Level Steps

Initial Assessment and Control Design

The next step is to evaluate management's control environment using the SOC 2 criteria and the relevant TSCs to identify gaps that require remediation. The assessment process can be broken out into the following high-level steps:

- Mapping of existing controls to the framework
- Documentation of gaps and future state" controls
- Identification of remediation plans and responsible individuals

The mapping process should start with a review of control documentation that may already exist, relevant to the scope and the control objectives identified in the SOC 2 standard. This could include sources such as Sarbanes-Oxley Section 404 compliance, internal audits, risk management, control self-assessments, past advisory assessments, or policies and procedures.

Walk-throughs of management's existing processes will provide a more complete view of the relevant processes and controls and gives the SOC 2 team information to understand where management's controls align to the standard and where gaps exist. It is critical to involve the correct stakeholders and process owners to ensure accurate and complete information. Inaccurate control information can lead to delays and testing exceptions later in the SOC 2 audit.

Mapping of processes and identification of gaps is a very collaborative process, as there is no single correct approach to addressing the requirements of the SOC 2 standard. It is important to involve a knowledgeable, experienced IT risk and control team in the process. The Service Auditor will likely take a very detailed approach to reviewing the final set of controls to ensure that SOC 2 objectives are met. While the specific technologies, processes and organizational roles established as part of the control environment are up to the discretion of management, achieving an appropriate level of control in light of the service provider's organizational size and complexity, data risk profile, volume of customer activity, and other related factors are all critical.

Remediation and Readiness

Remediation plans become the detailed road map toward the SOC 2 report. For every gap in the control environment, a remediation plan that includes the following should be articulated:

Remediation Plan Examples

- Detailed steps and deliverables to satisfy the control standard
- Timelines that are feasible, yet aggressive in meeting goals
- Remediation owners to track and motivate progress

There should be periodic meetings for all those involved in SOC 2 remediation processes. Since many TSCs affect the service provider as a whole, *not just IT* --it is critical to gather all relevant parties and solicit input on remediation feasibility and process improvements. These meetings can serve to foster a culture of SOC 2 compliance, which is imperative, especially for organizations completing the assessment for the first time. Some gaps are easily remedied. Others will require a more significant time and cost investment, as well as changes to established systems, processes, cultures and subject-matter expertise.

While organizations will always have an initial target date in mind for SOC 2 readiness, the results of the gap analysis and extent of remediation plans will dictate the feasibility of those initial targets. Depending on the drivers for the SOC 2 assessment and the importance of meeting a target date, management may need to augment its capabilities with the help of additional outside resources to implement the necessary control enhancements within a designated time frame. The most important goals coming out of the remediation phase are to maximize repeatability of processes and to achieve a stable, consistent control environment that addresses SOC 2 requirements.

No matter how ready a service organization may appear on paper, it is important to conduct readiness testing to ensure the organization's controls work as intended. Readiness testing reduces the risk of exceptions that could result in qualified opinions and serves to validate management's assertions made during the documentation and remediation phases. It also achieves alignment with the Service Auditor regarding how controls are designed and what control evidence will look like.

The SOC 2 Audit

Like most audits, SOC 2 success requires excellent communication. Expert auditors are excellent communicators frequent and transparent communication. Expectations for the audit, scope, audit timeline, staffing and delivery dates are all critical factors and should be discussed openly with the auditor from the start. An initial kickoff meeting with the auditor should be scheduled to discuss these items and other critical factors concerned with the audit.

Type of Test	Description of Test
Inquiry or corroborative inquiry	Inquiry of appropriate personnel to ascertain compliance with controls.
Observation	Observation of specific controls in operation.
Inspection	Obtain and review documents and reports indicating performance of the controls is effective.
Re-Performance	Re-performed application of the controls.

As tests progress, auditors will raise questions or concerns regarding the evidence Organizations should expect to receive feedback and status results. Should the auditor raise an observation or finding, clarification or further information may be needed.

SOC 2 Wrap-Up and Report

Once the audit fieldwork is concluded, organizations conduct a closing meeting with the auditor to review the results and confirm any outstanding items before they draft the report. A draft report for review lets organizations respond to any issues raised during the audit. Once finalized, the report will be issued to the organization to be distributed to customers.

Six Reasons Your Enterprise Needs a SOC 2 Report

Many service organizations have yet to develop the control frameworks and tools required to meet the rigorous SOC 2 audit standards.

Turning to a trusted advisor helps service organizations prepare for a favorable report. Conducting a readiness assessment before the audit helps service organizations identify gaps in current controls against the SOC 2 standard and remediate controls and processes that could sufficiently pass an examination.

Alternatively, the reputational and economic consequences of a negative report can be catastrophic for an organization.

1. **Customer and Contractual Demands:** Protecting customer data increasingly is a standard requirement for doing business and part vendor due diligence processes. Without a SOC 2 report, you could lose business.

2. **Competitive Advantage:** Showing a commitment to IT security, a SOC 2 report gives you an edge over competitors who don't have it.

3. **Cost Avoidance:** In 2019, a single data breach meant an average $3.92 million added expense to an enterprise, a figure that increases yearly. SOC 2 proactively helps establish strong internal controls to avoid costly security breaches.

4. **Regulatory Compliance:** SOC 2 dovetails with other frameworks, including HITRUST and ISO 27001, and can accelerate enterprise overall efforts overall.

5. **Valuable Insights:** A SOC 2 report delves into your risk and security posture, vendor management, internal controls governance, regulatory oversight, and more, for analysis, prioritization and action.

6. **Peace of Mind:** A SOC 2 report provides independent expert assurance of systems and network security for your enterprise ecosystem.

Conclusion

A SOC 2 report can be an ideal solution for many service providers looking for a more efficient way to satisfy customer inquiries about their control environment, but a structured readiness process is critical. Engaging a public accounting firm such as **Alchemi Advisory Group** as a trusted partner to a clarity to every step can simplify the process, shorten the overall timeline and achieving enterprise benefits more efficiently and effectively.

Get in Touch

ALCHEMI
ADVISORY GROUP

TheAlchemiGroup.com

4101 McEwen Road,
Suite 205
Dallas, TX 75244

(888) 590-1618

info@thealchemigroup.com