Successfully Navigating the SOC Examination Process

OVERVIEW OF PROCESS STAGES AND RESOURCE REQUIREMENTS

SC&H GROUP

TABLE OF CONTENTS

A System and Organization Controls (SOC) examination is performed by an experienced, reliable audit partner that provides independent third-party assurance over an organization's control environment. The initial process is typically comprised of seven main stages that result in a detailed, comprehensive audit report—a SOC report. SOC reports are a way for stakeholders to verify that an organization they plan on working with has internal controls that are appropriately designed, formally documented, and effectively operating.

Understanding what the process entails for your organization and staff, specifically the key stages and the responsibilities and requirements of each, is critical to business success. This knowledge, combined with the right internal team and audit partner, can maximize efficiency, clarity, and, most importantly, value throughout the SOC examination process and beyond.

WHAT ?

Examination Stages and Responsibilities

While each SOC report has different requirements and objectives, each is generally performed following seven main stages:

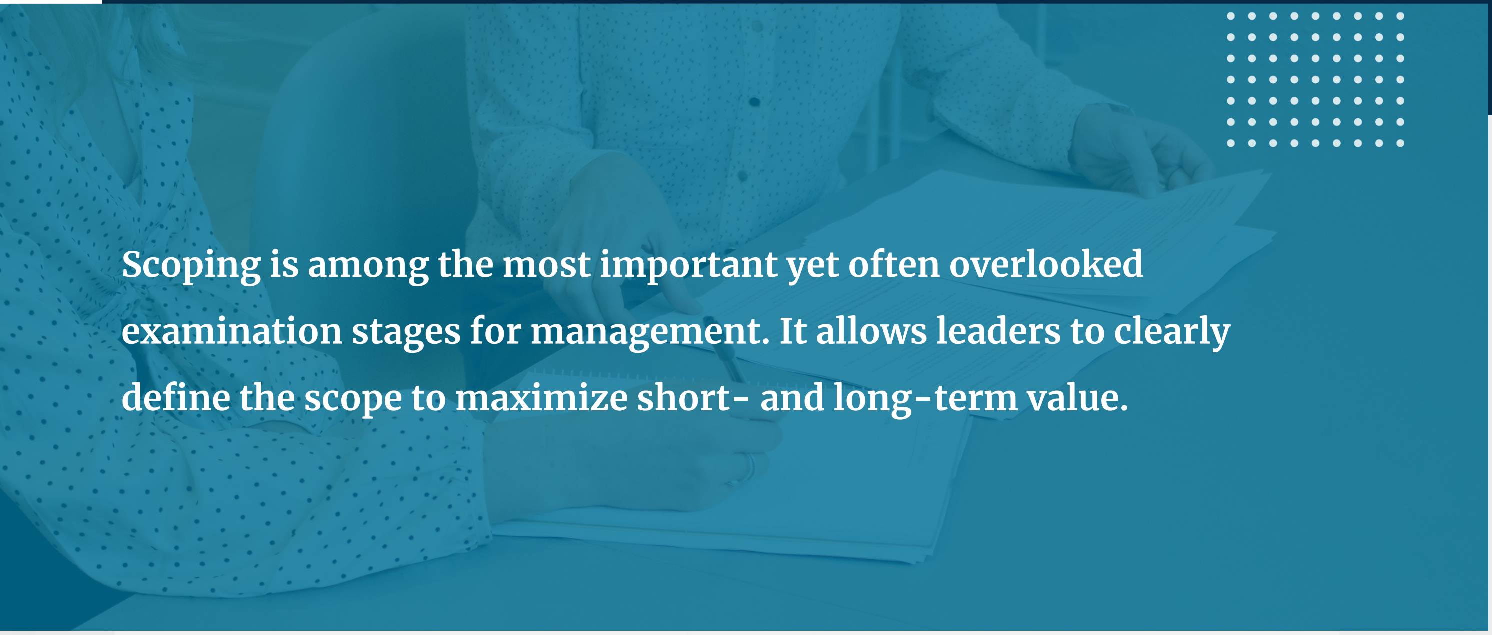
PROCESS STAGE	KEY PARTICIPANTS	KEY MATERIALS
1 **Scoping**	Management Auditors	Background on organizational needs and customer requirements
2 **Walkthrough and Control Design**	Auditors Process and Control Owners	Existing policies and procedures, materials from time spent with each process owner
3 **Gap Assessment**	Auditors Process and Control Owners	Preliminary documentation to support remediation roadmap
4 **Remediation**	Project Manager Process and Control Owners	Documentation for validation of the control environment
5 **Examination/ Testing**	Auditors Project Manager Process and Control Owners	Process documentation, examination evidence
6 **Report**	Management Auditors	Policies and procedures, draft feedback, response to feedback and exceptions
7 **Issuance**	Auditors	SOC report

STAGE 1: SCOPING

While organizations often view scoping as an effort driven by auditors, the most important components of this stage are led by your organization’s management team. It is an opportunity to clearly define the scope of the examination—systems, locations, and objectives—in a way that benefits your organization and its customers.

Your organization should examine what is driving the need for a SOC report (e.g., strategic goals, customer needs, regulatory requirements, etc.), to help better identify the systems and locations most relevant to those drivers.

Successful scoping sets the foundation for a well-organized examination with minimal disruption to business operations. For this reason, effective management-auditor collaboration is essential during this stage. All parties key to the process, including points of contact, should be identified and introduced. Auditors should work with key participants to review the purpose and content of SOC reports, as well as expectations throughout the remaining process stages.



Scoping is among the most important yet often overlooked examination stages for management. It allows leaders to clearly define the scope to maximize short- and long-term value.

STAGE 2: WALKTHROUGH AND CONTROL DESIGN

2

One of the keys to a successful walkthrough is making sure that the appropriate process and control owners are available during, and fully involved in, auditor discussions. This will ensure that auditors have access to the most complete and accurate information so they can minimize potential delays and challenges throughout the process.

Auditors will review formalized documentation and perform initial walkthroughs with each process and control owner to understand the extent and maturity of your current internal control environment to:

- Develop a comprehensive understanding of the control environment
- Map existing control activities
- Create a preliminary control matrix outlining controls necessary to meet the respective SOC requirements

Your auditor will aim to identify and unlock potential efficiencies during this stage by leveraging other compliance efforts and materials, where applicable. For instance, control documentation may already exist because of the Sarbanes-Oxley Act of 2002 Section 4040 (SOX 404) compliance, industry-specific control requirements (e.g., HITRUST Common Security Framework), internal audits, risk management efforts, and other advisory assessments.

STAGE 3: GAP ASSESSMENT

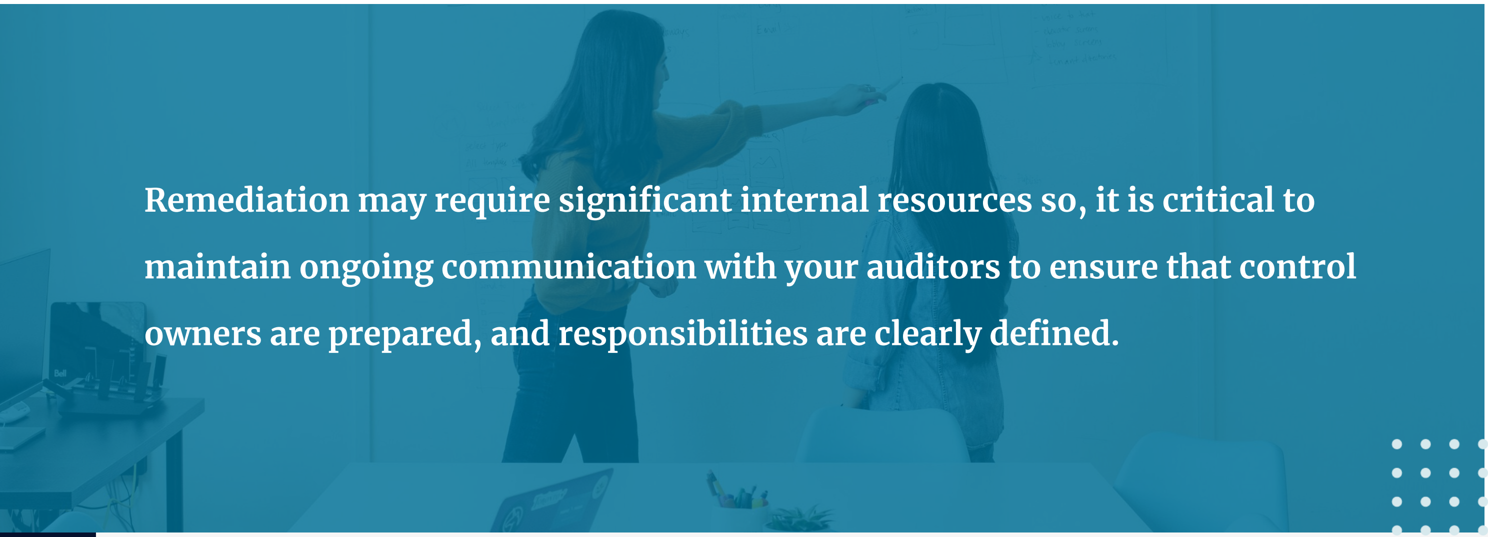
The gap assessment is an evaluation of existing control activities identified during the walkthrough stage. Performed by your auditors, this stage will determine if your organization has the proper controls designed and implemented and is maintaining sufficient audit evidence necessary to meet the respective American Institute of Certified Public Accountants (AICPA) requirements and/or management defined criteria.

Once the gap assessment is complete, a SOC focused control matrix will be created, which includes any findings and/or recommendations for SOC compliance. This deliverable is a remediation roadmap to guide the immediate next steps. The roadmap is discussed in detail prior to a Type 1 or Type 2 examination to ensure your organization is prepared to meet the respective SOC requirements.

STAGE 4: REMEDIATION

With oversight from your auditors, process and control owners will complete each step of the remediation roadmap to address control areas that are insufficient for examination. To maintain independence, service auditors may not act as management (e.g. physically implement controls during remediation). Therefore, it is vital that management's commitment to the necessary modifications remains consistent throughout this period.

Your service auditor should provide valuable, ongoing knowledge with process and control owners throughout remediation process. This will ensure that your team understand all the controls and are prepared to follow newly implemented policies and procedures. Additionally, auditors should be involved in periodic status meetings to discuss project updates and milestones and help address any concerns or challenges.



Remediation may require significant internal resources so, it is critical to maintain ongoing communication with your auditors to ensure that control owners are prepared, and responsibilities are clearly defined.

STAGE 5: EXAMINATION/TESTING

Following remediation, auditors will work directly with process owners to obtain sufficient evidence necessary for policy and procedure review and the detailed testing of all relevant control activities. Testing typically includes inspection of documents, system configurations, etc., observation of personnel in performance of their assigned duties, and inquiry.

TEST PROCEDURE	DESCRIPTION
Inspection	Inspected documents and records indicating performance of the control activities. This includes, among other things: • Examination of source documentation and authorizations • Examination of documents or records for evidence of performance and authorization (e.g., existence of initials or signatures) • Examination of system configuration and settings • Examination of user listings • Inspection of system documentation, such as operation manuals, policies and procedures documentation, system flowcharts, and system audit logs.
Observation	Observed the application or existence of specific control structure policies and procedures as represented. This includes: • Observations of personnel in performance of their assigned duties • Observations of control activity existence • Observance of various system tasks performed by personnel
Inquiry	Inquired of appropriate personnel. Inquiries seeking relevant information or representation from personnel were performed to obtain, among other things: • Knowledge and additional information regarding the control activity • Review of organizational structure, including segregation of functional responsibilities, policy statements, processing manuals; and • Corroborating evidence of the policy or procedure.

All SOC reports (except for SOC 3) can be either Type 1 or Type 2. The difference is based on the time period in scope.

TYPE 1 EXAMINATION

This will validate the design and implementation of controls at a specific point in time. The auditor will complete a test of one occurrence per control activity.

TYPE 2 EXAMINATION

This will validate the control design and operating effectiveness over a defined period of time. For non-automated controls, the auditor will obtain a population (or understand the specific frequency – e.g., quarterly) and select a sample of occurrences for testing.

The Type I report provides assurance over only the design of controls and therefore requires less time and effort when compared to the Type II, however testing the operating effectiveness in a Type II report gives the reader of the report greater assurance around whether an organization's control environment is functioning properly.

STAGE 6: REPORTING

Auditors will review your system description, as defined during the scoping stage, to verify completeness and accuracy and produce a draft SOC report. Much of the system description is derived from a compilation of relevant policies and procedures as documented and reviewed throughout the engagement and includes but is not limited to:

- The services covered
- Period or date to which a description relates
- Control objectives (SOC 1 – controls related to financial reporting, or SOC 2 – trust services criteria)
- Party specifying the control objectives (if not you)
- Related controls

Reporting should be a shared effort between the service organization and service auditor to ensure that the report accurately captures the environment as it exists throughout the audit period. The report will include four primary sections:

1. **Auditor's Opinion:** The service auditor's opinion on the system description, design, and operating effectiveness of identified control activities.
2. **Management Assertion:** Statements from the service organization's management regarding the system(s) audited, including specifics on scope.
3. **Description of the System:** Details about the system(s) reported including controls, subservice organizations, and complementary user entity controls.
4. **Results of Testing:** The control environment, including specific control activities in place and the auditor-performed tests.

STAGE 7: ISSUANCE

Lastly, auditors will issue the SOC report and conduct a closing meeting to discuss the contents and highlight the best practice for maintaining compliance with new policies and procedures. This transfer of knowledge will be critical to meeting your examination objectives and ensuring that process and control owners sustain an effective control environment, including management's commitment to:

- Upholding a culture of process and consistency to sustain the necessary control environment
- Emphasizing compliance and continual improvement
- Engaging auditors to perform subsequent testing to issue an annual recurring SOC report

WHEN ?

Timing and Setting Expectations

The first three stages (scoping, walkthrough, and gap assessment) can typically be accomplished in a defined time period. The fourth stage, remediation, is where that timeline is likely to vary based on the outcomes of the gap assessment and the organizational resources available to address them. Sometimes, the gaps surfaced are straightforward and easily addressed; other times, they may require more significant modifications to processes and systems that affect internal teams.

SOC 1 examinations may require more upfront time to determine scope, this is especially true for industries like mortgage servicing, healthcare, and others with complex financial processes and controls.

SOC 2 examinations, though the criteria are predefined, can be more time consuming due to the highly technical and security-focused nature.

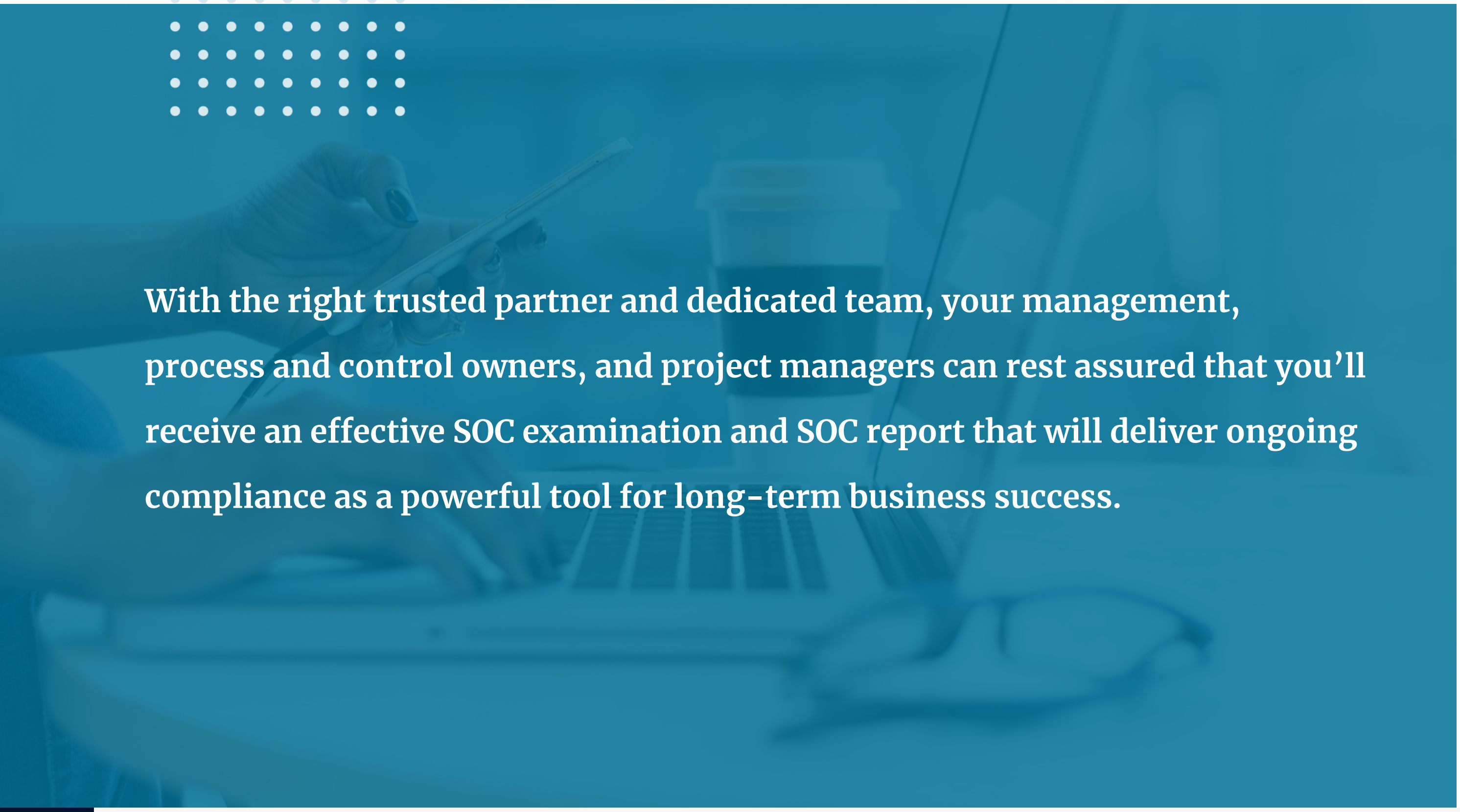
WHO ?

Selecting the Right Partner

A successful, dependable examination process is largely contingent on partnering with auditors you can trust. It’s important to do your due diligence and meticulously identify and select an experienced, insightful, and collaborative examination partner.

The right auditor will:

- Supply dedicated SOC examination specialists
- Possess a detailed understanding of your industry regulations, organizational goals, and internal control environment
- Provide reliable guidance and service throughout each process stage



With the right trusted partner and dedicated team, your management, process and control owners, and project managers can rest assured that you’ll receive an effective SOC examination and SOC report that will deliver ongoing compliance as a powerful tool for long-term business success.

Additional SOC Resources at Your Fingertips

BLOG

Two Key Components That Drive a Successful SOC Examination: Process and People

These are the keys you need to unlock peak operational performance for both you and your auditor. Gain an in-depth understanding of how the right dynamic team and a formalized process can lead to a faster, more efficient, and more helpful SOC examination for your company.

READ NOW »

BLOG

Marketing a SOC Report to Gain a Competitive Advantage

A SOC report is a valuable tool that can help your company harness future relationships with clients, business partners, and even investors. In this blog, we share the best practices, tips, and tactics that will ensure you leverage a SOC report to your advantage.

READ NOW »

ABOUT

SC&H SOC Audit Services

Our experienced SOC audit team advises service organizations on AICPA SOC reporting requirements. We provide valuable information that customers, prospects, and auditors require to assess the risks and internal controls associated with an outsourced service provider.

As a qualified firm in this space, we have had innumerable conversations around education, value, and efficiencies. We take pride in working with organizations who have specific needs, competing priorities, time constraints, and other unique objectives. We understand the value of time, appropriate planning, and education that ensure an examination seamlessly progresses.

YOUR SOC AUDIT TEAM

Paul Shifrin
Director

pshifrin@schgroup.com
410-403-1621

Jodi Harris
Principal

jharris@schgroup.com
410-403-1560

TELL US ABOUT YOUR SOC NEEDS

About SC&H Group

SC&H Group is a nationally recognized audit, tax, and management consulting firm serving rapidly growing private sector businesses to Fortune 500 companies. With more than 300 employees, SC&H Group has a strong foothold along the east coast, a client base representative of global brands, and a client approval rating nearly five-times the industry average (Net Promoter Score = 84.4). We've advised over 1,800 organizations, spanning numerous industries, on accounting, tax, profitability, and business process solutions.