



A SERVICE ORGANIZATION'S GUIDE

SOC 1, 2, & 3 REPORTS



Introduction

If you're a growing service organization, whether a technology provider, financial services corporation, healthcare company, or professional services firm, chances are you need a System and Organization Controls (SOC) report.

After all, many of today's Requests for Proposals (RFPs) are now requiring them, a result of increased scrutiny over third-party controls and legislative requirements such as the Sarbanes-Oxley Act of 2002 (SOX).

SOC reports have also become a competitive necessity in many industries, essential to gaining client trust in your processes and controls.

However, the type of SOC report needed—as well as the benefits, components, and requirements of each—are not always clear. Furthermore, the nature and professional standards associated with SOC 1, SOC 2, and SOC 3 reports are continually evolving, leading to confusion on the part of not only service organizations, but also user entities (clients).

We're here to help.

In this guide, we break down the functions and evolution of service related SOC reports. We discuss their differences and recent changes, as well as the value of information provided by each.

And most importantly, we help you determine which report is right for your organization, preparing you for greater long-term efficiency, consistency, and success.





Table of Contents

The Evolution of SOC Reporting	1
SOC 1 Reports: Focusing on Controls Related to Financial Reporting	5
SOC 2 Reports: Meeting the Needs of a Broader User Range	7
SOC 3 Reports: Capitalizing on a Valuable Marketing Tool	9
SOC 1, 2, and 3 Report Comparison	10
SOC Reports: Common Questions and Confusions	11
More Change Is Coming	13
Conclusion: Choosing the Right Report for Your Organization	14

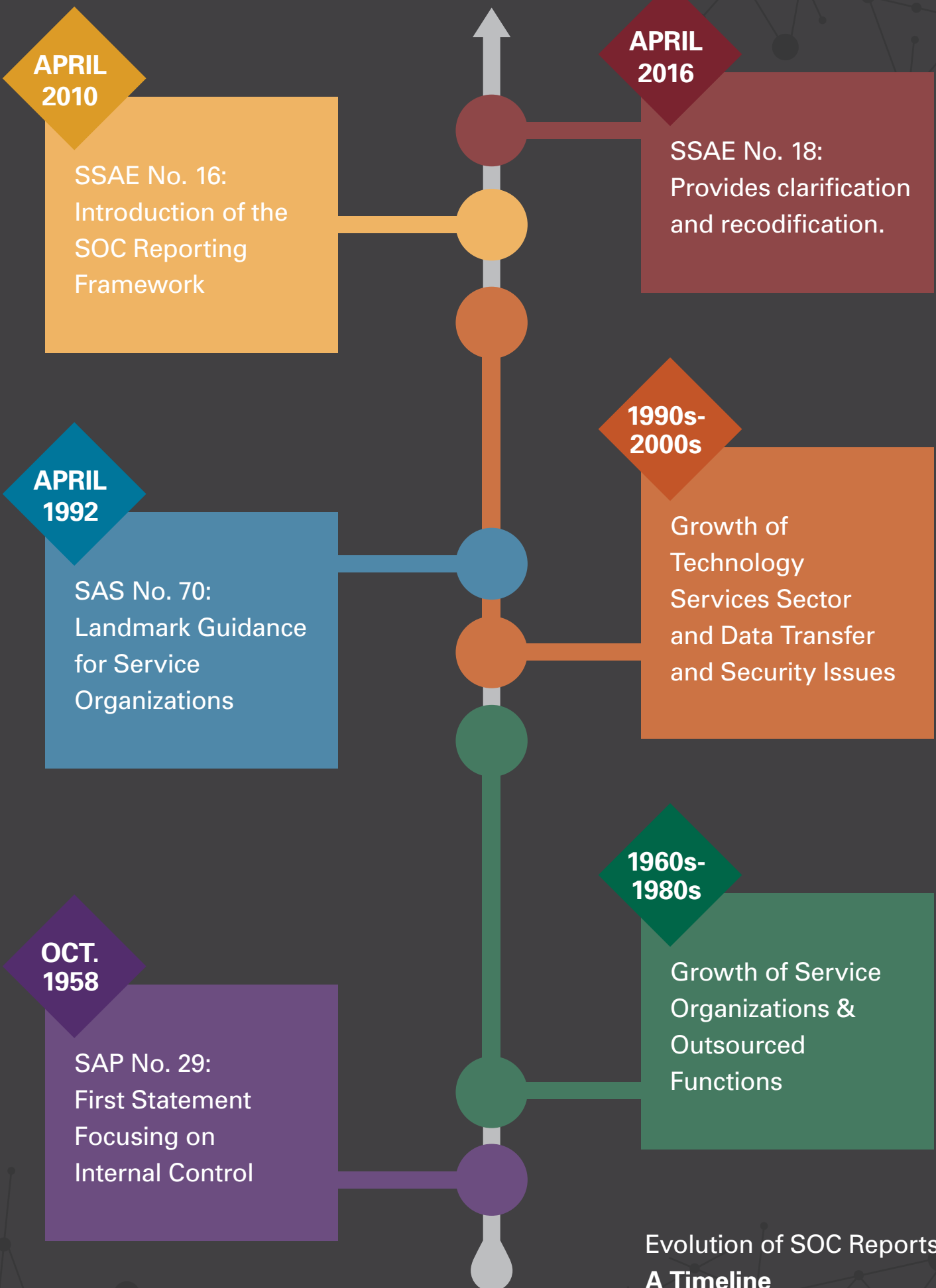
The Evolution of SOC Reporting

Before we dive into the requirements and uses of SOC 1, SOC 2, and SOC 3 reports, it is important to first understand their history and development.

The origins of SOC reports can be traced back to the October 1958 issuance of Statement on Auditing Procedure (SAP) No. 29, *Scope of the Independent Auditor's Review of Internal Control*, which was among the first Statements to focus on internal control and the impact of service organizations on an entity's control environment.

Over the next 30 years, service organizations took on a greater role and importance in the business world. User entities began shifting from large, integrated companies that directly controlled assets to diversified corporate bases.

In conjunction, the American Institute of Certified Public Accountants ([AICPA](#)) issued a series of Statements during this time, each addressing topics relative to internal control and service organizations.



**APRIL
2010**

SSAE No. 16:
Introduction of the
SOC Reporting
Framework

**APRIL
2016**

SSAE No. 18:
Provides clarification
and recodification.

**APRIL
1992**

SAS No. 70:
Landmark Guidance
for Service
Organizations

**1990s-
2000s**

Growth of
Technology
Services Sector
and Data Transfer
and Security Issues

**OCT.
1958**

SAP No. 29:
First Statement
Focusing on
Internal Control

**1960s-
1980s**

Growth of Service
Organizations &
Outsourced
Functions

Evolution of SOC Reports:
A Timeline

SAS 70

By the 1990s, a large portion of companies were outsourcing key ancillary functions and IT support services. While good news for service providers, this trend led to concern over how provider controls were affecting companies' financial statements.

The AICPA issued Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, in April 1992. For nearly two decades, SAS 70 served as the authoritative guidance for examinations of a service organization's control objectives and activities.

SAS 70 simplified auditing requirements, enabling auditors to review and test third-party controls, then issue an opinion via a uniform reporting format (Service Auditor's Examination).

SSAE 16 and the SOC Reporting Format

As time progressed and new technologies emerged, companies continued to increase their reliance on third-party service providers—thus requiring a greater assurance of sufficient controls over financial reporting and other key subject matters.

In April 2010, the AICPA issued the Statement on Standards for Attestation Engagements ([SSAE No. 16](#), *Reporting on Controls at a Service Organization*).

SSAE 16 updated and clarified reporting processes regarding controls around financial reporting. Further, it replaced SAS 70's Service Auditor's Examination with a SOC report.

With the introduction of the SOC reporting format, the AICPA also established three SOC report types (SOC 1, SOC 2, and SOC 3), each designed to meet a specific user need. AICPA's goal was to build user confidence through more appropriate, comprehensive reporting on service organization controls.

SSAE 18

Effective May 1, 2017, SSAE 18 updated SSAE 16 in several significant ways, thereby impacting SOC reporting. For example, [SSAE No. 18](#) requires more intensive vendor management controls for subservice organizations. These are companies that your organization uses to provide certain services to user entities (e.g., third-party data centers). This Standard requires additional controls related to the ongoing monitoring, selection, and management of vendors.

SSAE 18 also requires performance and documentation of formal risk assessments specific to potential material misstatements, as well as allows for reporting on a wide range of additional subject matter. This change results in additional services and product types falling under a SOC 2 examination.

SOC 2 Plus

In addition, the AICPA recently expanded the use of SOC 2 to align with other IT security regulations, allowing organizations to report on additional subject matter beyond the scope of AT-C 205. This change is especially useful for user entities in quickly developing regulatory landscapes.

For instance, SOC 2 Plus gives healthcare entities the ability to report on the HITRUST Common Security Framework control requirements used as the basis of their cybersecurity and information protection program. Also, it gives entities the ability to report on security at a service organization based on additional industry group criteria, such as the Cloud Security Alliance's Cloud Control Matrix.

More information on the requirements and benefits of these developments, as well as other forthcoming guidance, will be included in upcoming SC&H Group publications.

SOC 1 Reports: Focusing on Controls Related to Financial Reporting

SOC 1 reports focus only on your organization's controls relevant to a user entity's financial reporting. SOC 1 examinations are performed in accordance with SSAE 18, resulting in clearer, more detailed information regarding your control environment.

Given their limited scope, SOC 1 reports are best suited for organizations that must instill confidence in their controls and safeguards over their customers' financial data. Such organizations include providers of financial transaction services and various technology services, such as:

- Data center services
- Cloud computing and network monitoring services
- Software as a service (SaaS)
- Payroll and medical claims processing
- Lending services

Further, SOC 1 reports are often necessary when the user entity is publicly traded and must comply with SOX 404 or similar regulations.

SOC 1: QUICK FACTS

Controls relevant to a user entity's financial reporting

A Good Fit for Your Organization If:

You provide services that can materially affect your clients' financial data

Your clients will use the report to perform an audit of their financial statements

Your clients will use the report to comply with the SOX Act or similar regulations

Applicable Professional Standard
SSAE 18

Type 1 or Type 2?

When electing to perform a SOC reporting examination, there may be confusion regarding the two types of SOC 1 reports: Type 1 and Type 2.

The difference between Type 1 and Type 2 reports lies in the time period upon which they focus. Type 1 reports address the suitability of your control design and implementation at a *specific point in time*.


In contrast, a Type 2 report concentrates on control design and operating effectiveness over a *period of time*. A Type 2 report therefore enables the user auditor to assess the risk of material misstatement of financial statement assertions affected by your services criteria:

Report Contents and Variations

SOC 1 reports—which are intended for your management and the user entity’s financial statement auditors, CFO, CIO, controllers, and compliance officers—include a description of your system and the auditor’s opinion regarding:

- If your description of controls is fairly presented
- If your controls are effectively designed

Type 2 reports also contain a description of the tests performed, their results, and an opinion on whether your controls are effectively operating over a specified period.



SOC 2 Reports: Meeting the Needs of a Broader User Range

In transitioning from SAS 70 to SOC reporting, the AICPA introduced SOC 2 reports to provide a means for organizations to report on controls unrelated to financial reporting. SOC 2 reporting allows service providers to meet the needs of a broader range of users.

Specifically, SOC 2 examinations report on the effectiveness of your organization's controls as they relate to five AICPA-defined trust services criteria:

- *Common Criteria (Security)*: The system is protected against unauthorized access. (Per AICPA's [January 2014 guidance](#), Common Criteria is the minimum requirement for all SOC 2 examinations. The four other principles serve as add-ons to Common Criteria, not entirely separate requirements.)
- *Availability*: The system is available for operation and use as committed or agreed.
- *Processing Integrity*: System processing is complete, valid, accurate, timely, and authorized.
- *Confidentiality*: Information designated as confidential is protected as committed or agreed.
- *Privacy*: Personal information is collected, used, retained, disclosed, and disposed in conformity with commitments in the service organization's privacy notice and criteria set forth in the Generally Accepted Privacy Principles issued by the AICPA.

Performed in accordance with [AT-C 205, Examination Engagements](#), a SOC 2 examination focuses on how client data is stored and protected. It is a more technical, security-focused examination than SOC 1, but since the criteria required are predefined by the AICPA, it is easier to determine what compliance needs are required.

A Growing Demand for SOC 2 Reports

With increases in outsourcing—from ancillary tasks to entire corporate functions—the demand for SOC 2 reports continues to rise. In fact, many organizations are proactively performing SOC 2 examinations to not only improve process efficiency and consistency, but also highlight their commitment to securing client data.

In addition, with the growth in various technology sectors that process both financial and non-financial related data, many organizations are reporting on both SOC 1 *and* SOC 2 standards. Such organizations include certain SaaS, co-location, and data center service providers.

Similarities and Subtle Differences between SOC 1 and SOC 2 Reports

Much like SOC 1, SOC 2 reports can be Type 1 (addresses control design and implementation at a point in time) or Type 2 (addresses control effectiveness over a period of time). Also, both reports contain a description of your system, the auditor’s opinion in relation to your control description and design, and, for Type 2 reports, details of tests performed, their results, and an opinion on control effectiveness.

Finally, while SOC 1 and SOC 2 reports both have limited audiences, SOC 2 reports may be given to other parties with insight into the internal controls and nature of the service provided, such as prospective customers, vendor management professionals, regulators, and other key business partners.

SOC 2: QUICK FACTS

Controls relevant to security, availability, processing integrity, confidentiality, and/or privacy

A Good Fit for Your Organization If:

You provide services that require the storage and protection of your clients’ non-financial data

Your clients will use the report to gain confidence in your organization’s systems and controls

Your clients want a detailed understanding of processing and controls, as well as service auditor tests and results

Applicable Professional Standard

AT-C 205

SOC 3 Reports: Capitalizing on a Valuable Marketing Tool

Similar to SOC 2, SOC 3 reports are performed in accordance with AT-C 205 and also focus on controls relevant to the AICPA's five trust services criteria.

However, unlike SOC 2, SOC 3 reports are certified and can be made publicly available—making them valuable tools for marketing the effectiveness of your control environment.

Should you desire a SOC 3 examination, your organization must first complete a SOC 2, Type 2 audit. SOC 2 and SOC 3 examinations can be performed on one or more of the trust services criteria.

SOC 3 reports contain much of the same information as a SOC 2 report, except with a less detailed description of your controls related to compliance and operations. They also do not include detailed testing procedures, results, or an opinion on the system description.

SOC 3: QUICK FACTS

Controls relevant to security, availability, processing integrity, confidentiality, and/or privacy

A Good Fit for Your Organization If:

Your clients want to make the report generally available (e.g., for marketing purposes)


Your clients will use the report to gain confidence in your organization's systems and controls

Your clients don't need details regarding your controls or auditor tests and results

Applicable Professional Standard
AT-C 205

SOC 1, 2, and 3 Report Comparison

	SOC 1 Report	SOC 2 Report	SOC 3 Report
Purpose	Report on your controls relevant to the user entity's financial reporting	Report on your controls relevant to security, availability, processing integrity, confidentiality, and/or privacy	Same as SOC 2
A Good Fit for Your Organization If:	<ul style="list-style-type: none"> You provide services that can materially affect your clients' financial reporting Your clients will use the report to support an audit of their financial statements Your clients will use the report to comply with SOX 404 or similar regulations 	<ul style="list-style-type: none"> You provide services that require the storage and protection of your clients' data Your clients will use the report to gain confidence in your organization's systems and controls Your clients want a detailed understanding of your processing and controls, as well as service auditor tests and results 	<ul style="list-style-type: none"> Your clients want to make the report generally available (e.g., for marketing purposes) Your clients will use the report to gain confidence in your organization's systems and controls Your clients don't need details regarding your controls or auditor tests and results
Applicable Professional Standard	SSAE No. 18, <i>Attestation Standards: Clarification and Recodification</i>	AT-C 205, <i>Examination Engagements</i>	Same as SOC 2
Certification? (Yes/No)	No	No	Yes
Types 1 and 2? (Yes/No)	Yes	Yes	No
Audience Restricted?	Yes	Yes	No
Audience	Your management, as well as the user entity's financial statement auditors, CFO, CIO, controllers, and compliance officers	Your management, as well as the user entity's CFO, CIO, controllers, compliance officers, vendor management, regulators, other appropriate parties	Any interested party



SOC Reports: Common Questions and Confusions

What is the difference between SOC 1 / SOC 2 and Type 1 / Type 2?

The most important distinction between SOC 1 and SOC 2 is that SOC 1 reports focus on controls relevant to a user entity's financial reporting, while SOC 2 reports focus on non-financial reporting controls. Both SOC 1 and SOC 2 each have Type 1 and Type 2 report options. Type 1 addresses control design at a point in time, while Type 2 addresses control effectiveness over a period of time.

What if a client requests a SOC report that differs from what we think is needed?

This is a more common occurrence than many executives realize. We regularly consult with service organizations and user entities to evaluate the client needs and determine the appropriate SOC report. Ultimately, a SOC 2 report is needed in most of these circumstances, even when the client initially requests a SOC 1 report.

Does a SOC 2 examination require significantly more effort than a SOC 1 examination?

Given the in-depth technical and security-focused nature of SOC 2 examinations, they are typically more time consuming than SOC 1 examinations. However, SOC 1 examinations require more upfront time to determine scope, since SOC 2 criteria is predefined. Also, for organizations with complex financial processes and controls (e.g., certain mortgage lenders and healthcare claims processors), SOC 1 reports can exceed the time requirements of some SOC 2 reports.

Can I be SOC certified?

There is no such thing as a SOC 1 or SOC 2 certification. SOC 3 examinations are the only engagements that yield a certification and report that is freely distributed for marketing purposes. Completed SOC 3 reports also allow for a corresponding seal to be placed on your organization's website. However, please note that a SOC 2 examination must be performed prior to the completion of a SOC 3 report.

Do SOC reports provide any substantial benefits beyond satisfying client requirements?

Absolutely. Both user entities and service organizations can benefit greatly from SOC examinations. Besides ensuring that client data is housed and processed in a secure manner, SOC reports help ensure that your internal control processes are efficient, consistent, and documented—thus yielding improved operational performance.

What can my organization do to best prepare for a SOC 1, SOC 2, or SOC 3 examination?

When entering your first SOC examination, it is beneficial to work with your auditor to perform an initial readiness assessment, allowing you to remediate any gaps prior to the start of the SOC reporting process. Taking this step yields a more efficient examination, and much of the initial assessment can be leveraged for the SOC report.



More Change Is Coming

As in previous years and decades, guidance is continuously evolving to keep pace with industry progress. This evolution is reflected within the changes to the Trust Services Criteria and their impact on SOC 2 reporting requirements.

TSC Section 100

In April 2017, the AICPA updated the Trust Services Criteria impacting the controls required for inclusion within SOC 2 reports. The new criteria restructures and aligns the Trust Services Criteria with COSO 2013 framework and will be required for reports with periods ending after December 15, 2018. The updates to the Trust Services Criteria add additional points of focus to better address cybersecurity risk, specifically related to governance, risk management, and third party management. The changes are expected to impact the level of effort required for SOC 2 reporting, however we believe the changes will better position organizations to meet the needs of their clients and to provide greater transparency within the marketplace.



Conclusion: Choosing the Right Report for Your Organization

Navigating the world of SOC reporting can be a discouraging experience, fraught with unclear requirements, shifting guidance, and confusing terminology.

By partnering with an auditor that understands your organizational goals, industry regulations, and internal control environment, you can satisfy client requirements and instill confidence in your ability to protect and store client data. Further, a high-quality SOC examination can deliver value-added benefits, including more efficient, effective control processes and procedures.

Ultimately, working with a trusted auditor to overcome SOC challenges will help to ensure ongoing compliance and a solid foundation for long-term business success.

For More Information

To learn more about SOC requirements and considerations—and discuss which report is right for your organization — click [here](#) to contact SC&H Group.

About SC&H Group

SC&H Group is an audit, tax, and business consulting firm dedicated to minimizing risk and maximizing value. SC&H Group's practices advise leading companies from emerging businesses to the Fortune 500 on accounting, tax, profitability, and business process solutions. Clients in all states and worldwide benefit from SC&H Group's commitment to delivering powerful minds, passionate teams, and proven results on each and every engagement. www.schgroup.com.

This document is property of SC&H Group. No replication of its content is permitted without express permission from SC&H Group.