SOC Reports, Audit Periods, and Bridge Letters

December 14, 2023

STG invests a great deal of time and effort into our SOC® audit process, as well as supporting processes that exist outside of the audit period (e.g., preparing bridge letters). We hope that the following addresses frequent questions we receive about STG's SOC® reports, the timing and length of the testing period, the assessment criteria, the annual reports issued, and accompanying bridge letters.

If you have additional questions after reading this, please reach out to us at CR@thesummitgrp.com.

What are SOC® reports?

The American Institute of Certified Public Accountants (AICPA) developed System and Organization Controls (SOC®) reporting as a way for a company to 1) show their customers and other key stakeholders that the internal controls on which the company relies are working and 2) provide an independent third-party validation of that assurance from a certified public accounting firm. SOC® reports are used to communicate that information.

Are there different kinds of SOC® reports?

There are several kinds of SOC® reports. SOC 1®, SOC 2®, SOC 3®, SOC for Cybersecurity and SOC for Supply Chain. Each has its own purpose and guidelines for use. There are also several types of SOC® reports. A Type 1 report covers the design of controls at a specified point in time in the past. A Type 2 report confirms that the controls were in place and operating effectively and as designed over a defined period of time in the past.

What kind of SOC® reports does STG provide to customers?

STG currently provides a SOC1® Type 2 and a SOC2® Type 2.

STG SOC1® Report

A SOC1® Report reports on the controls of the service organization that are relevant to the user organization's internal controls over financial reporting. Some clients use certain STG products or services that process or manage information that has the potential to impact these clients' financial results. This report is relevant only to customers who depend on STG for certain products or services that could impact the customer's own financial reporting.

Organizations like STG that provide products and services of this nature often provide clients with SOC1® Type 2. Examples of enterprises that produce SOC1® reports for clients include payroll processors, trust departments, employee benefit or retirement plan operators, registered investment advisors, loan servicers, payment processors and others. STG engages a certified public accounting firm to assess our control environment annually and report on their results.

STG's SOC1® includes general information about the organization, as well as the period covered by the report. An independent third-party auditor reviews STG's control environment every year. The report documents STG's current control objectives and the controls we use that are designed to meet those objectives. The report also includes the tests conducted by the independent auditor, as well as the results of those tests and the auditor's overall opinion on the design and effectiveness of our controls over time.

STG SOC2® Report

Many of STG's clients rely on us to maintain certain controls known as "Trust Services Criteria" that protect various areas of our business and those of our affiliate or subsidiary organizations. STG engages a certified public accounting firm to assess these criteria annually and to report on their results. This means that an independent third-party auditor reviews STG's control environment every year and draws a conclusion as to the existence and effectiveness of these controls over a period of time. This conclusion, the control environment description, and the testing results are summarized in an annual SOC2® Type2 report.

Our SOC® 2 Report assesses the design, effectiveness, and reliability of STG's internal processes and control environment. The report indicates the organization has undergone a rigorous, in-depth audit of its internal control activities by an independent accounting and auditing firm. By undergoing an annual SOC®2 audit, STG obtains a comprehensive audit report disclosing the controls and processes in place that provides the independent auditor's opinion regarding the operational effectiveness of the processes and procedures applied to the business activities that are subject to the described internal controls.

Trust Services Criteria

The AICPA maintains a set of criteria (Trust Services Criteria) designed for its members to use in evaluating the design, suitability, and operating effectiveness of a client's control environment. When this evaluation occurs for a point in time, that is reviewed in a SOC2 ® Type 1 report. When the evaluation is based on observations and testing over a period of that, that is reviewed in a SOC2® Type 2 report.

The primary categories of Trust Services Criteria are:

- **Security** – Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- **Availability** – Information and systems are available for operation and use to meet the entity's objectives.
- **Processing Integrity** – System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality** – Information designated as confidential is protected to meet the entity's objectives.
- **Privacy** – Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

The Security Criteria are required as part of a SOC2® evaluation. A participating organization also has the opportunity to select the other Trust Services Criteria that apply to it. At STG, currently we participate in the Security Criteria. During our annual test period, which typically runs from January 1 through September 30 each year, our independent third-party auditor collects information, reports, screen shots, and log files related to our Security Criteria controls. Once all of the evidence is gathered and tests have been performed, the auditor drafts a SOC2® Type2 report that outlines their conclusions on whether STG's

controls were in place and operating effectively during the testing period. This report takes time to produce, and we are given a draft to review for completeness and accuracy. We usually receive this at the beginning of October. The auditors typically provide a final report near the end of October, which we make available to our clients upon request.

Audit Period

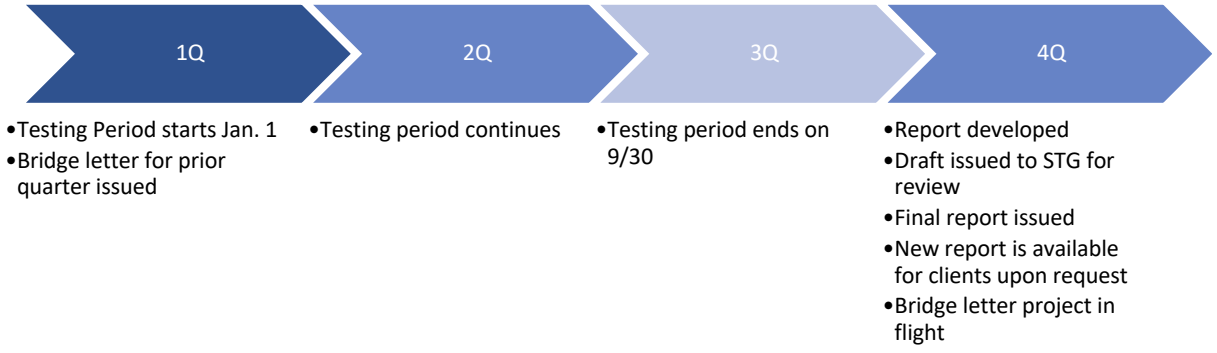
A SOC® review is performed as a "look-back." This means our independent third-party auditors examine evidence for activities that occurred previously during the nine months of our testing period to determine whether all stated controls were in place and operating effectively during that period. Clients sometimes ask for a report that covers the current year or quarter, or even one that is valid into the future. Unfortunately, that is not how the SOC® review process works, as we are only audited on whether the controls were in place and effectively operating during the audit period.

Bridge Letters

STG's audit period is based upon a fiscal year that starts on January 1 and ends on December 31. The testing period covered for our SOC®1 Type 2 and SOC2® Type 2 reports is January 1 through September 30 (the first nine months of the year). Some clients' vendor management cycles end in different periods, and the variation in fiscal years between client organizations and STG can cause a reliance gap. STG issues a *bridge letter,* also known as a *gap letter*, to provide our clients with continuity during those periods. STG typically issues its bridge letter for both its SOC1® and SOC2® reports in January or February of each year to cover the 4Q of the prior year (the period of time between the end of our report test period and our year-end).

Sometimes we get out of cycle, or even get urgent same-day requests, for bridge letters. This puts us in a difficult position, as STG's bridge letter has to attest that:

- There are no material changes in the control environment outlined in most recent SOC2® report;
- The description of the controls outlined in that report are still in place; and
- There have been no significant control deficiencies with the controls described in the report.



The effort required to officially validate these statements is substantial and takes time and effort from a number of associates and departments across the enterprise.

We understand the urgency and importance of these requests from our customers, but we want to ensure that all parties understand that a bridge letter is more than a simple email or document created

spontaneously to satisfy a particular client's request. Should an urgent and unplanned situation arise, please let us know as early as possible and we will do our best to work with you to help you meet your organization's timelines or find another mutually satisfactory solution in the interim.

What is the difference between a service organization, service auditor, user organization and user auditor?

- Service organization – the organization under examination (i.e., STG)
- Service auditor – the organization performing the examination (i.e., STG's auditors)
- User organization – Customers who receive your SOC report (i.e., your company)
- User auditors – Customers' auditors who may ask to see the SOC report (i.e., your auditors)

What are Complementary User Entity Controls (CUEC)?

CUEC internal controls describe responsibilities of a user organization. The user organization must implement these controls themselves within their own organization in order to the process to work end-to-end.