SOC Reports, Audit Periods, and Bridge Letters

May 1, 2023

LC 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@lenderscooperative.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?

LC is pursuing a SOC2® Type 2.

LC SOC2® Report

Many of LC'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. When LC was organized under Summit Technology Consulting Group, LLC (STG), these services were addressed under STG's SOC® reporting. Obtaining a SOC2® report for LC as an independent organization takes time; however, LC has engaged a certified public accounting firm to assess these criteria annually and to report on their results. This means that an independent third-party auditor will review LC's control environment this year (and every year thereafter) and draw 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 will be summarized in an annual SOC2® Type2 report.

This report will assess the design, effectiveness, and reliability of LC's internal processes and control environment. By undergoing an annual SOC®2 audit, LC will obtain 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. LC plans to participate in the Security Criteria. During our annual test period, which this year runs from January 1 through September 30, our independent third-party auditor will collect 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 will draft a SOC2® Type2 report that outlines their conclusions on whether LC's controls were in place and operating effectively during the testing period. This report takes time to produce. We expect to receive a draft of this report to review for completeness and accuracy in the beginning of October. The auditors expect to provide a final report near the end of October, which we will 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.

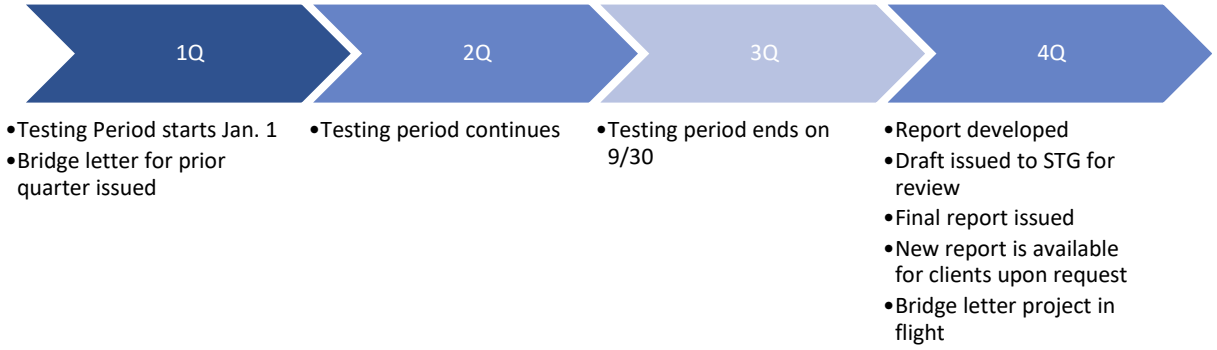
Bridge Letters

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 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 LC can cause a reliance gap. LC will issue a *bridge letter,* also known as a *gap letter*, to provide our clients with continuity during those periods. LC expects to issue its bridge letter for its SOC2® report 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 clients send out of cycle, or even get urgent same-day requests, for bridge letters. This puts us in a difficult position, as a LC's bridge letter has to attest that:

- There are no material changes in the control environment outlined in most recent 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.