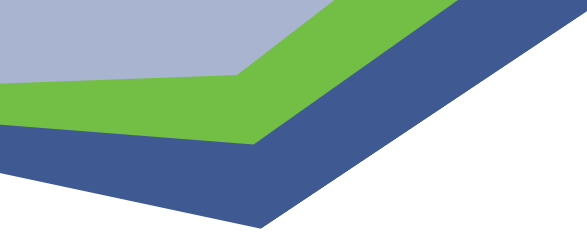




**DANSA
D'ARATA
SOUCIA** LLP

SOC REPORTING

How often should you have a report
issued?



TIMING OF YOUR NEXT SOC

Your auditor just sent you your first official SOC report and you can finally satisfy that one (or several) customer request to see it. What now?

Below are a few common questions we have received when discussing the timing and cadence for SOC compliance.

Does my SOC report expire?

Technically, no. A SOC report is not a traditional certification, but is rather an attestation, and the auditor's report does not expire. However, the user of the report may determine that the period covered by the auditor's report is no longer relevant. SOC reports are often considered stale or irrelevant by users after 12 months.

Additionally, when you initially receive your SOC report from your auditor, you're able to register with the AICPA and display their SOC logo on your website and other marketing materials. Per the AICPA's terms and conditions, a service organization may only display the logo for 12 months immediately following the date of the auditor's report.

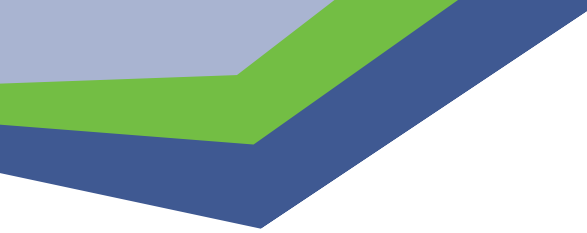
How often do other organizations go through SOC?

The most common and recommended cadence for SOC is a continuous cycle of compliance. For example, an organization who has never gone through SOC before will likely decide to go through an initial SOC Type 1, followed by an immediate 3 to 6-month SOC Type 2, and then follow that with 12-month Type 2's in perpetuity. Using dates for reference, SOC Type 1 as of January 1, 20XX, SOC Type 2 from January 1, 20XX to June 30, 20XX, then SOC Type 2 from July 1, 20XX to June 30, 20XX+1. This cadence would provide your organization with continuous, demonstrable compliance in perpetuity.

While the above sequence is typical it is not a requirement. We have had clients complete a SOC Type 2 covering 3 months, and then come back a year later and do another SOC Type 2 covering 3 months. Maybe this could work for your customers, but there are some risks to this approach. For instance, a vendor management department would likely be concerned that there was a 9 month period of time in between in which no independent third-party was attesting that your policies were being followed and your controls were operating effectively.

In summary, continuous compliance is the most conservative approach.





Are there any other disadvantages to putting off our next SOC until next year?

Another important consideration is efficiency. Constantly being engaged in an audit develops familiarity for both your team and the audit team. From the auditor's perspective, this familiarity may mitigate a number of questions that would otherwise have to be discussed in order to understand your organization and/or system. Likewise, your team would likely develop good habits regarding documenting and providing evidence to support the functioning of internal control on a regular basis. These efficiencies directly impact the price of the examination.

What if our organization and/or service has significantly changed since our last SOC report?

This is common for maturing companies and not a big deal. The AICPA thought of this when designing the Description Criteria® and established a specific criterion for organizations to disclose changes that occur within an auditable period in their next SOC. This section is a convenient way for users of your report to quickly identify those significant changes and evaluate how those changes may impact their organization (if at all). You do not have to put off a SOC examination due to changes you are experiencing.

Contact Us

Dansa D'Arata Soucia LLP is a public accounting and consulting firm focusing on information security attestation and consulting. We offer SOC 1, SOC 2, ISO 27001, GDPR, NIST CSF, HIPAA, and more.

☎ (716) 842-3900

🌐 www.darata.com

✉ tgavigan@darata.com

✉ dgarigen@darata.com

Author

Taylor Gavigan is an Audit Manager at Dansa D'Arata Soucia.

