Compliance Today - June 2024

Renee Steffen (renee.steffen@vgm.com, linkedin.com/in/renee-steffen-b366336/) is a Compliance Analyst at VGM Group Inc.

David C. Harberts (dave.harberts@vgm.com, linkedin.com/in/dave-harberts/) is the Vice President, Compliance & Accreditation at VGM Group Inc.

Madison Kuester (madison.kuester@vgm.com, linkedin.com/in/madison-kuester-416b30145/) is a Compliance Analyst at VGM Group Inc.

SOC it to me: Adding to your foundation of compliance

by Renee Steffen, CHC; David C. Harberts, MSN, RN; and Madison Kuester, M.J., CRM

Over the past several years, System and Organization Controls (SOC) reports have been gaining popularity among service organizations within the healthcare industry, especially as service organizations' healthcare clients seek ways to verify that there are proper internal controls in place to protect their finances and data. More and more, healthcare clients are requiring these service organizations to provide SOC reports before signing on to do business. If you haven't heard about it, you likely will soon.

The compliance team at VGM Group was in a similar situation several years ago. We'd heard about SOC, but it wasn't until current healthcare clients and prospects started asking the various VGM Group business units about it that we finally took the necessary steps to complete a report.

When the request first comes, SOC can seem like a daunting undertaking. However, the process doesn't have to be scary. In fact, if you approach SOC the right way, it can be far more than a checkbox your clients have to mark. SOC can be the key to unlocking several benefits and opportunities to take your organization to the next level.

What Is SOC?

SOC is a set of attestation reports developed by the American Institute of Certified Public Accountants (AICPA). They are designed to evaluate whether a service organization has the proper internal controls in place, as well as their effectiveness.

An independent auditor produces the reports. The auditor will review your controls and documentation to determine whether your controls will meet their objectives and whether those controls are being followed over time within the organization. Following the audit, the service organization receives a report that can then be provided to current and prospective clients.

There are several versions of SOC reports to suit the specific needs of the organization and its clients:

- **SOC 1**: This report focuses primarily on financial controls. A successful SOC 1 report assures clients that the financial information they receive from the service organization is accurate.

- **SOC 2**: This report assesses a service organization based on the trust service criteria (TSC) developed by the AICPA. There are five categories of the TSC that the organization can pick to be assessed against. The five categories include security (required), availability, processing integrity, confidentiality, and/or privacy. In general, a successful SOC 2 report indicates that a service organization has effective controls in place to ensure client data is kept secure..

- **SOC 3**: This report is essentially a less detailed version of the SOC 2 report. It is designed for general use and applies to a wider audience. Organizations might display a SOC 3 achievement on their website, but they may also have a SOC 2 report that can be provided to a specific client.

- **SOC for cybersecurity**: This report examines the effectiveness of an organization's cybersecurity risk management programs.

- **SOC for supply chain**: This report assesses an organization's ability to mitigate these risks.

SOC assessments also have two different types of reports available:

- **Type 1**: During this assessment, the auditor will review the controls you have in place and ensure your design and implementation are effective as of a certain date.

- **Type 2**: During this assessment, the auditor will not only review your controls' design and implementation but also determine their operating effectiveness over a period of time (typically nine to 12 months).

This document is only available to members. Please log in or become a member.

Become a Member Login