Link to article: https://discover.claromentis.com/knowledgebase/articles/567/understanding-ssae-18-soc-reports

Understanding SSAE 18 / SOC reports

Archived

Replaced with a simple explanation in the 'important information for sales' KB article. We also have an article on Codedev that explains how to view the SOC 2 report (Internally only).

Introduction

SSAE 18 contains the rules to check that a service organization's internal controls are as claimed. The process for following these rules results in a SOC report (see the definitions below). Service auditors (aka CPA Firm's) are required to follow these rules when conducting a SSAE 18 engagement.

Note: The auditing standard SSAE 18, replaced SSAE16 (May 1, 2017). SSAE 16 previously replaced SAS 70 (15 June 2011).

Can Claromentis provide a SOC II report?

Claromentis cannot provide a SOC report (1,2 or 3) as Claromentis Ltd has not been assesed by an SSAE 18 engagement. However, our hosting provider (and main sub-processor) Google is regularly audited under SSAE 18 rules and we review the controls on a yearly basis.

You can view more information about this at the following link: https://cloud.google.com/security/compliance/#/

Key points:

- Only the SOC 3 report is available to Claromentis Ltd customers. It is available publicly at the following link: https://services.google.com/fh/files/misc/gcp_soc3_report_2018.pdf
- Google's SOC 2 (Type 2) report is available to Claromentis Ltd, but only under NDA. We are unable to share this with our own customers, but we can assure you that we check this on a yearly basis to ensure we are aware of the controls that we have responsibility over. We have an internal policy that defines exactly how frequently this is checked and we update this each year to understand any changes to the responsibilites for either Claromentis or you, as the client.

Definitions

SSAE: Statement on Standards for Attestation Engagements

CPA Firm: A firm that contains at least one Certified Public Accountant

SOC: Service Organization Control.

SOC Reports: SOC reports are internal control reports that provide insight into the risks associated with the provision of a service by an external organisation. The reporting structure is put together and overseen by the American Institute of Certified Public Accountants (AICPA).

SOC 1: Reports on the controls put in place related to a service providers financial reporting.

SOC 2: The SOC 2 reports on the controls an organisation has set up to ensure the security, availability, integrity, confidentiality, and privacy of the data they control (aka Trust Services Principles). The SOC 2 report is only available to users/direct customers of a particular service and often only available under NDA. SOC 2 - Type 1 vs Type 2: For a Type 1 report, the auditor gives an opinion

based on the organisation management's description of the controls and after a review of the documentation (at that moment in time). For a Type 2 report, the auditor will spent a period (minimum of 6 months) reviewing and testing the controls in order to compare the organisation management's description *vs. the operational effectiveness* of the controls (as shown in the tests). Type 2 reports generally take a lot longer to be generated, due to the minimum time it takes to test these controls.

SOC 3: The SOC 3 is a freely distrbuted (often publicly available) version of the SOC 2 report. It will give an overview of whether an organisation is maintaining effective controls (Trust Service Principles), but it won't provide a description of the service providers systems/infrastructure.

Created on 13 May 2019 by Will Emmerson. Last modified on 19 August 2022
Tags: ssae 18, ssae 16, soc II, soc 2, sas 70, soc 3, soc I, soc III, report, controls