SOC 1, 2 & 3

Sinds de ontwikkeling en ingebruikname van de ISAE 3402 heeft deze standaard jarenlang gegolden als de “best beschikbare optie” voor het verlenen van een redelijke mate van Assurance over uitbestede processen. Daarnaast is de afgelopen jaren ook verder ontwikkeld aan een product naast de ISAE 3402 door het American Institute of Certified Public Accountants (AICPA): de SOC-rapportagestandaard.

Deze rapportagestandaard is in het leven geroepen om uitbestede processen beter audit-baar te maken, zonder dat een auditor hierbij normenkaders als de SAS 70 of de ISAE 3402 gebruikt voor het verlenen van Assurance over uitbestede diensten.

SOC rapportages (met uitzondering van SOC 3) kunnen rapporteren over het opzet en bestaan, maar ook over de werking van geïmplementeerde beheersmaatregelen. SOC 3 is enkel verkrijgbaar als een rapportage welke het opzet, bestaan en werking van beheersmaatregelen toetst.

Wat is een SOC-rapport?

Een SOC-rapport is opgesteld volgens de SOC-rapportagenormen. Binnen SOC zijn meerdere typen te onderscheiden, respectievelijk SOC 1, 2 en 3. Elke SOC heeft een ander einddoel dan wel werkgebied om over te rapporteren. Per SOC wordt een rapport opgesteld wat voldoet aan de eisen van het AICPA met betrekking tot rapporteren over uitbestede diensten.

Voor uw organisatie betekent dit dat er accuraat kan worden getoetst hoe uw serviceorganisatie (uw) data beheert en/of bewaakt. Richting belanghebbenden kan zo inzichtelijk worden gemaakt waarom voor een bepaalde service organisatie wordt gekozen, bijvoorbeeld omdat het niveau van beveiliging voldoet aan de gestelde eisen.

Voor organisaties is een SOC-rapportage dé optie om volgens de nieuwste, internationaal geaccepteerde standaarden uitbestede diensten te laten auditen. Vooral voor organisaties met internationale aspiraties wordt de SOC rapportagestandaard gezien als een asset omdat de rapportagestandaard binnen Amerika al enkele jaren geldt.

Welke SOC-rapportage is voor wie geschikt?

De SOC rapportagestandaard kent drie typen: SOC 1, 2 en 3. Elke SOC heeft een andere rapportagedoel. De verschillende doelen zijn:

- SOC 1: rapporteert over beheersmaatregelen welke direct in relatie staan tot de financiële verslaglegging van een organisatie. SOC 1-rapporten zijn verkrijgbaar als rapport over het opzet en bestaan van beheersmaatregelen, maar ook de werking ervan. Een voorbeeld hiervan is het gebruik maken van data warehousing voor opslag van omzetregistratie of andere financiële gegevens welke relevant zijn voor o.a. jaarverslagen.
- SOC 2: rapporteert op basis van vastgestelde principes welke een relatie hebben met de opzet, bestaan en werking van operational IT-controls met betrekking tot uitbestede processen. SOC 2 toetst op basis van de TrustServicesPrincipales Sectie 100 welke het mogelijk maakt voor een organisatie zichzelf te laten toetsen op één of meer principes die de organisatie zelf kan bepalen op basis van deze lijst. Zodoende wordt een organisatie niet verplicht sterke punten te herkeuren en kan er specifiek geaudit worden naar wens van de organisatie. Voor een SOC 2-rapport kan worden gedacht aan het rapporteren over de

uitbesteding van de analyse van een Business Intelligence Proces aan een externe partij, dan wel het verkrijgen van zekerheid over het gebruik van een externe Clouddienst.

- SOC 3: is een verkorte versie van de SOC 2-rapportage. Deze rapportage mag vrij gepubliceerd worden en geeft aan belanghebbenden verkort weer hoe de service organisatie een SOC 2-engagement behaald heeft. Een SOC 3-rapport stelt de organisatie in staat een zegel te publiceren, verstrekt door het AICPA, over de kwaliteit van de uitbestede dienstverlening. SOC 3 is enkel te verkrijgen als rapportage welke betrekking heeft op het opzet, bestaan en de werking van beheersmaatregelen; doordat de zegel anders geen waarde zou vertegenwoordigen. SOC 2 is vereist voordat een SOC 3-engagement gestart kan worden om de waarde van het zegel te behouden.

Een SOC-rapportage is geldig totdat er wijzigingen plaatsvinden welke niet meer door de SOC-rapportage benoemd worden. Als er in het SOC-rapport aandacht is besteed aan aankomende changes en deze worden geïmplementeerd, dan is het voor het management van de organisatie toegestaan hun SOC-rapport als geldend aan te merken door middel van een bridge letter. Staan de changes niet aangegeven in het rapport, dan heeft dit als gevolg dat het SOC 2 rapport niet meer als geldig kan worden aangemerkt en de organisatie een nieuwe SOC 2 engagement moet starten.

Het kiezen van de juiste SOC-rapportage voor uw organisatie kan lastig zijn. 12secure-u helpt graag met het maken van de juiste keuze, zodat uw organisatie zekerheid heeft over uitbestede dienstverlening.