FACTSHEET

Service Organisation Control (SOC)-rapportages

Service Organisatie Control-rapportages (SOC-rapportages), zijn bedoeld om informatie en assurance te verschaffen over interne beheersingsmaatregelen van serviceorganisaties (zoals datacenters, applicatie service providers, clearing instituten, vastgoedbeheerders, etc.).

Met de toename van uitdagingen en risico's in de huidige markt kan de implementatie van een SOC-rapportage serviceorganisaties helpen:

- te voldoen aan klantverwachtingen en contractuele verplichtingen;
- zich te onderscheiden van concurrenten door middel van een proactieve opstelling met betrekking tot interne beheersingsmaatregelen, waardoor een concurrentievoordeel behaald kan worden;
- inherente risico's te verlagen door potentiële zwaktes in het systeem te identificeren en aan te pakken.

Audits op serviceorganisaties worden steeds belangrijker, echter de hiermee samenhangende complexe technologische terminologie en de strenge eisen die hieraan worden gesteld zorgen voor verwarring en vormen een uitdaging voor de implementatie. Deze publicatie dient als steun om SOC-rapportages te begrijpen en de behoeften van uw serviceorganisatie af te stemmen met de toepasselijke rapportage om uw doelstellingen te bereiken.

De toegevoegde waarde van een SOC-rapportage

SOC-rapportages worden onder andere gebruikt door de serviceorganisatie zelf en haar klanten of accountants van deze klanten om de interne beheersingsmaatregelen die bij de serviceorganisatie zijn geïmplementeerd te begrijpen.

1 Voor de serviceorganisatie zelf:

SOC-rapportages bieden meerdere voordelen, waaronder:

- het verminderen van de noodzaak om vragen van accountants van verschillende klanten te beantwoorden. Dit kan zeer indringend en tijdrovend zijn als meerdere accountants zijn betrokken;
- het verminderen van accountantskosten voor klanten door de inspanning te minimaliseren die externe accountants dienen te leveren om de interne beheersingsmaatregelen van de serviceorganisatie te beoordelen (kosten voor een dergelijk proces worden gewoonlijk doorberekend aan de klant als service fees);
- het helpen aantonen dat processen en procedures in werking zijn gesteld om te verzekeren dat uitbestede diensten naar behoren worden beheerd. Dit kan een essentiële factor zijn bij het binnenhalen van nieuwe business; veel requests for proposals vragen tegenwoordig om een SOC-rapportage van de serviceorganisatie;
- het identificeren van issues op het gebied van efficiëntie alsmede dubbele beheersingsmaatregelen op efficiënte en proactieve wijze.

2 Voor klanten, prospects, belanghebbenden en andere geïnteresseerde partijen:

SOC-rapportages helpen deze groepen vertrouwen te krijgen in de interne beheersing van de serviceorganisatie en deze te begrijpen.

3 Voor de accountants van de klanten:

Zij kunnen de rapportage gebruiken om inzicht te verkrijgen in de interne beheersingsmaatregelen die bij de serviceorganisatie in werking zijn gesteld. Afhankelijk van het type rapportage kan de accountant van de klant de interne beheersingsmaatregelen van de serviceorganisatie meenemen in de planning en uitvoering van de audits op financiële overzichten. Daarnaast helpt het om vertrouwen te verkrijgen in de beheersingsmaatregelen die zijn geïmplementeerd om gevoelige informatie te beschermen.

BDO's SOC-rapportages

BDO kan verschillende typen rapportages afgeven, welke verdeeld kunnen worden over twee basisgroepen:

1 Rapportages specifiek gericht op systemen betrokken bij de verwerking van financiële transacties (SOC 1);
2 Rapportages gericht op informatiebeveiliging, beschikbaarheid, integriteit, vertrouwelijkheid en privacy (SOC 2 en SOC 3).

1 Rapportages om te voldoen aan financiële vereisten

De ISAE 3402 (SOC 1)-rapportage focust op de interne beheersingsmaatregelen die verband houden met de verwerking van financiële transacties bij een serviceorganisatie. Deze wordt uitgevoerd conform de International Standard on Assurance Engagements 3402 (ISAE 3402) of Nederlandse vertalingen hiervan: Standaard 3402 zoals uitgegeven door de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) of Richtlijn 3402 als uitgegeven door de Nederlandse Beroepsorganisatie van IT-auditors (NOREA). Zowel de standaard als de richtlijn voldoen aan de internationale ISAE 3402-vereisten.

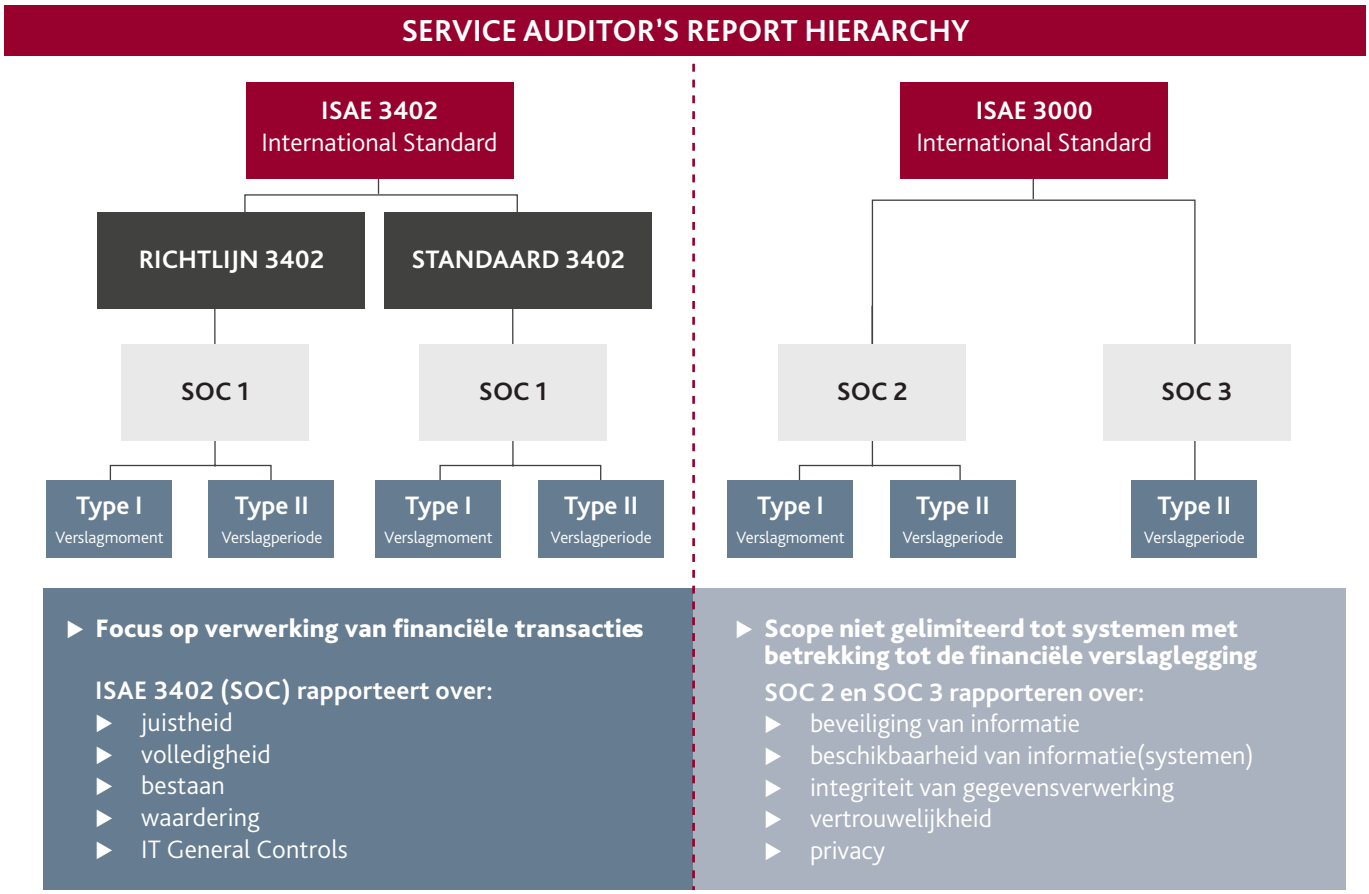
Dit type assurancerapportages heeft betrekking op de interne beheersingsdoelstellingen en interne beheersingsmaatregelen die zijn opgesteld door een serviceorganisatie en gerelateerd zijn aan financiële aspecten van hun bedrijfsvoering, waaronder:

- juistheid;
- volledigheid;
- bestaan;
- waardering;
- IT general controls (gebaseerd op het CobiT Model):
  - toegangsbeveiliging;
  - change management;
  - IT continuïteit.

Gebaseerd op de ISAE 3402-standaard en de door de NBA en NOREA uitgebrachte implementaties hiervan, bevat een 3402-rapportage de volgende elementen:

Beschrijving van het systeem: management dient een complete en accurate beschrijving van het systeem van de serviceorganisatie voor te bereiden en te presenteren, in plaats van alleen de interne beheersingsmaatregelen van de serviceorganisatie.

Risicoanalyse: management dient een formele risicoanalyse uit te voeren om risico's voor het bereiken van de interne beheersingsdoelstellingen te identificeren. Hoewel deze niet opgenomen hoeft te worden in de rapportage, dient de auditor van de serviceorganisatie het proces van de risicoanalyse en de basis van de conclusies van de serviceorganisatie te beoordelen.



Identificatie van interne beheersingsdoelstellingen: management dient interne beheersingsdoelstellingen te specificeren en deze te vermelden in de beschrijving van het systeem van de serviceorganisatie.

Interne beheersingsmaatregelen om risico's te mitigeren: interne beheersingsmaatregelen moeten zijn geïmplementeerd om in te spelen op de risico's die zijn geïdentificeerd in de risicoanalyse en deze te mitigeren. De serviceorganisatie dient interne beheersingsmaatregelen op te zetten, te implementeren en te onderhouden om een redelijke mate van zekerheid te verschaffen dat de interne beheersingsdoelstellingen worden behaald.

Bewering van het management: management dient een geschreven bewering op te leveren aangaande de compleetheid en het accuraat zijn van de verschafte informatie en aan te geven welke criteria zij hanteerde als basis voor deze bewering.

2 Rapportages om te voldoen aan niet-financiële vereisten

Bedrijven die de verwerking of bewaring van informatie uitbesteden (aan bijvoorbeeld datacenters) zoeken zekerheid dat deze data vertrouwelijk blijft, beschikbaar is als overeengekomen in overeenkomsten en/of beveiligd is tegen ongeautoriseerde toegang. De SOC 2- en SOC 3-rapportages zijn ontwikkeld om organisaties die het verzamelen, het bewaren of de overdracht van informatie hebben uitbesteed te voorzien van een mechanisme om toezicht en governance bij een serviceorganisatie te beoordelen. Dit kan met name van belang zijn als het onpraktisch is de fysieke locatie te inspecteren vanwege de geografische locatie, of omdat deze zich in 'de cloud' bevindt.

De SOC 2- en SOC 3-rapportages hebben een bredere scope en zijn gebaseerd op vijf categorieën:

- Beveiliging van informatie;
- Beschikbaarheid van informatie(systemen);
- Integriteit van gegevensverwerking;
- Vertrouwelijkheid;
- Privacy.

SOC 2- en SOC 3-rapportages bieden serviceorganisaties een methode om zich te onderscheiden. Ze tonen huidige, potentiële en toekomstige klanten dat ze adequate interne beheersingsmaatregelen en waarborgen met betrekking tot hosting of het verwerken van informatie hebben ingericht door een grondige audit te ondergaan. Serviceorganisaties kunnen de categorieën selecteren die aansluiten bij de doelstellingen van hun verslaggeving en bij de aard van hun bedrijfsvoering. Voor elk beginsel zijn er onderliggende criteria (interne beheersingsdoelstellingen) die vooraf gedefinieerd zijn waardoor rapportages gestandaardiseerd kunnen worden en makkelijker te interpreteren zijn.

BDO's auditproces en raamwerk

De algemene stappen voor het komen tot een SOC-rapportage volgen de reguliere auditaanpak. Zij

FASE 1		FASE 2	
A Planning	**B** Beoordeling beheersings-omgeving	**C** Toetsen beheersings-maatregelen	**D** Rappor-tage
Stem de scope van de opdracht af met het management Definieer alle van toe-passing zijnde beheer-singsdoelstellingen Bevestig de scope van de rapportage	Identificeer de huidige beheersingsomgeving inclusief de IT General Controls Evalueer procedures voor alle onderliggende beheersingsdoelstel-lingen en beoordeel de effectiviteit van de opzet Oplossen van tekort-komingen door het management	**Type I:** Voer testprocedures uit om het bestaan van elke beheersingsmaatregel vast te stellen op een bepaald moment **Type II:** Voer testprocedures uit om de werking van elke beheersingsmaatregel vast te stellen over een periode van 6 tot 12 maanden	Voer Quality Assurance procedures uit Breng het definitieve SOC-rapport uit

kunnen echter verschillen naar aanleiding van de huidige beheersingsomgeving van een serviceorganisatie. Een assuranceopdracht bestaat uit de volgende fases en activiteiten:

Ons raamwerk, dat ontwikkeld is om een effectieve aanpak voor het uitvoeren van audits te leveren, zal:

- minder tijd vergen van u gedurende het auditproces;
- een rapport leveren dat voldoet aan de vereisten van uw klanten, hun accountants en andere regelgevende instanties;
- leiden tot waarnemingen die uw interne beheersingsmaatregelen en operationele effectiviteit verbeteren.

Meer weten?

Voor meer informatie kunt u contact opnemen met onze specialisten via:

E ita@bdo.nl
T 088 – 236 48 222

03/2019 – FA1955