SOC 2: Update van de NOREA SOC Guide

17 december 2019

Carlijn Frins en Jeroen Francot

Onlangs is een update gepubliceerd van de NOREA SOC Guide, met enkele aanpassingen gemaakt rondom het gebruik van SOC 2- en SOC 3-rapportages. Wat betekenen deze wijzigingen voor ons, IT-auditors?

Aanleiding voor de update van de NOREA SOC Guide is dat de huidige guide nog uit 2016 stamt. Sindsdien heeft de AICPA de nodige aanpassingen gedaan aan de *Trust Services Criteria*, waaronder de update naar de versie van 2017. Deze aanpassingen en wijzigingen in regelgeving bieden nieuwe mogelijkheden, waaronder het uitbrengen van SOC 3- rapporten en het opnemen van de privacy-categorie. Doordat de privacy-categorie is toegevoegd, kan een serviceorganisatie laten zien dat ze de beheersing rondom privacy in de greep heeft. Gezien de groeiende aandacht voor privacy en gegevensbescherming is dat een belangrijke toevoeging.

SOC 2

Wat betekenen deze wijzigingen voor IT-auditors en voor serviceorganisaties? En vooral: gaan deze wijzigingen ervoor zorgen dat SOC 2 in Nederland een breder draagvlak krijgt? Vaak wordt de bekende ISAE 3402-standaard nog steeds gebruikt voor het rapporteren over IT-dienstverlening, maar deze rapporten passen niet altijd bij het doel van de rapportage. De ISAE 3402-standaard – in Amerika bekend als het SOC 1-rapport – richt zich namelijk specifiek op de verantwoording over financiële transactieverwerking. Het SOC 2-rapport richt zich echter juist op de maatregelen die in het bijzonder relevant zijn voor IT-dienstverleners. Deze maatregelen zijn onderverdeeld in vijf '*categories*':

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

Deze categorieën zijn op hun beurt weer onderverdeeld in een vast aantal beheersingsdoelstellingen, de 'criteria'. Binnen het SOC 2-rapport kan de IT-dienstverlener rapporteren over een of meerder categorieën, waarbij de security-categorie een verplicht

onderdeel is. De beheersingsdoelstellingen per categorie staan vast, wat de rapporten inhoudelijk meer uniform maakt. Dit vergroot het overzicht en maakt het geheel van de diverse maatregelen in de keten beter inzichtelijk. Hierdoor worden de rapporten en de beheersing bij verschillende organisaties eenvoudiger vergelijkbaar. Hoe een serviceorganisatie invulling geeft aan de doelstellingen, dus de inrichting van de diverse controlemaatregelen, is uiteraard aan de organisatie zelf.

De verschuiving naar een bredere toepassing van de SOC-standaard komt echter maar langzaam op gang. Dit terwijl SOC 2-rapporten een steeds praktischere oplossing worden voor serviceorganisaties met een focus op IT, onder meer doordat die specifiek gericht zijn op maatregelen die relevant zijn voor IT-dienstverleners. Denk bijvoorbeeld aan de PaaS- en SaaS-providers. Vaak verstrekken zij nog steeds een ISAE3402-rapport, terwijl dit niet altijd past bij het doel van het rapport. Immers, de inhoud van het rapport van IT-dienstverleners is in de meeste gevallen niet gericht op financiële transactieverwerking, maar op onderwerpen als beveiliging en beschikbaarheid. Voor deze organisaties is de specifiek voor deze doelgroep opgestelde SOC 2-standaard dan ook geschikter. In de praktijk wordt de SOC 2 echter nog niet veel gevraagd. Zonde, want SOC-rapporten brengen met hun uniforme en vergelijkbare inhoud een flink aantal voordelen met zich mee. Zo zijn deze rapporten bijvoorbeeld bij uitstek geschikt om te rapporteren over beveiligingsmaatregelen of het nakomen van service levels.

SOC 2 en SOC 3 in Nederland

SOC 2 is een door het American Institute of Certified Public Accountants (AICPA) uitgebrachte guide. Omdat deze gebaseerd is op Amerikaanse wet- en regelgeving is het niet zomaar mogelijk om deze in Nederland te gebruiken. Professioneel gezien wordt een SOC 2- of SOC 3-rapport in Nederland daarom afgeven onder de Richtlijn 3000A of de ISAE 3000. Dit voorkomt misverstanden over de vraag op welke wet- en regelgeving het rapport is gebaseerd. Het rapport betreft in Nederland dus een Richtlijn 3000A- of ISAE 3000-rapport, gebaseerd op de SOC 2 Trust Services Criteria.

In het kort: De wijzigingen in TSC 2017

De vernieuwde versie van de SOC 2 Trust Services Criteria is in 2017 uitgebracht. Alle SOC 2-rapporten die worden uitgebracht voor een periode die eindigt op of na 15 december 2018 moeten voldoen aan deze versie. De wijzigingen in de Trust Services Criteria zijn hieronder samengevat. In de update van de SOC guide van de NOREA zijn deze wijzigingen ook doorgevoerd.

Nieuwe naam: Trust Services Criteria

De oorspronkelijke naam 'Trust Services Principles and Criteria' is met de update gewijzigd in 'Trust Services Criteria'. De vijf categories ('principles' in de vorige versie) zijn hetzelfde gebleven, namelijk zoals gezegd:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

Nieuw framework: COSO 2013

Belangrijker dan de naamswijziging is dat het COSO 2013-framework in SOC 2 is geïntegreerd. COSO heeft net als SOC 2 betrekking op de interne beheersing van een organisatie, waardoor deze integratie goed past. Veel bedrijven gebruiken COSO al voor de inrichting van hun interne beheersing en ter ondersteuning van het interne beheersingssysteem. Deze integratie kan daarmee leiden tot schaalvoordelen en meer flexibiliteit in de toepassing van SOC 2. De integratie leidde tot een aantal wijzigingen in de security-categorie. Hierdoor verandert de invulling van controls voor de security-criteria ook. Voor serviceorganisaties betekent dit dat ze een mapping moeten maken van de bestaande controls naar de nieuwe criteria. Daarbij is vast te stellen of met de huidige set van controls aan alle criteria kan worden voldaan. In sommige gevallen betekent dit dat aanvullende controls nodig zijn om eventuele leemtes in te vullen.

Extra aandacht: Points of focus

Een ander nieuw element in de Trust Services Criteria zijn de *Points of Focus*. Voor het toepassen van de Trust Service Criteria is vaak professionele oordeelvorming nodig. Om daar extra richting aan te geven, zijn de criteria ingevuld met de Points of Focus. Dit zijn essentiële eigenschappen van de criteria, die kunnen helpen bij het ontwerpen, implementeren en beoordelen van beheersingsmaatregelen. Tevens hoopt de AICPA met de introductie van de Points of Focus meer consistentie op beheersingsmaatregel-niveau in de SOC 2-rapporten aan te brengen. Het is niet verplicht om alle Points of Focus in beheersingsmaatregelen te vatten. Ze zijn namelijk niet allemaal van toepassing op elke serviceorganisatie. De Points of Focus zijn bedoeld als niet meer dan een handvat bij het opstellen van een control framework.

SOC 2 in de praktijk

Zoals eerder aangegeven, vraagt de markt nog steeds veel om ISAE3402-rapporten. Ook daar waar het gaat om rapporten over IT-serviceproviders. De opgegeven reden is meestal

dat klanten van de serviceorganisaties specifiek vragen naar een ISAE3402-rapport. Zolang hun klanten niet om een SOC 2-rapport vragen, maken serviceorganisaties vaak de overstap liever nog niet omdat het SOC 2 nog relatief onbekend is in de markt. Het blijft in de praktijk daardoor een uitdaging om serviceorganisaties en hun klanten ervan te overtuigen dat een SOC 2-rapport passender is dan een ISAE3402-rapport. Wellicht bieden de twee hierna geschetste 'extra's' organisaties het laatste duwtje in de rug voor de overstap.

Selling point: SOC 3

Een van de belangrijkste reden voor serviceorganisaties om een assurancerapport uit te geven, is dat ze hiermee aan klanten kunnen aantonen dat ze hun bedrijfsprocessen beheersen. De verspreidingskring van het SOC 2-rapport is beperkt tot gebruikers van het systeem en hun accountants, terwijl de serviceorganisatie in veel gevallen ook zaken wil aantonen aan organisaties die buiten de verspreidingskring van het SOC 2-rapport vallen. Denk hierbij aan potentiële klanten of andere geïnteresseerden zoals security officers. Een SOC 3-rapport is dan de perfecte oplossing. Een SOC 3-rapport is een beknopte versie van een SOC 2-rapport, met één belangrijk verschil: het SOC 3- rapport kent een brede verspreidingskring.

Dit kan aantrekkelijk zijn voor serviceorganisaties, omdat hiermee eenvoudig aan potentiële klanten en andere geïnteresseerden aangetoond kan worden dat ze hun zaken op orde hebben. De vernieuwde SOC guide van de NOREA besteedt hier dan ook uitgebreid aandacht aan. In de SOC guide is nu ook uitgewerkt hoe in Nederland een SOC 3-rapport kan worden afgegeven. Belangrijkste voorwaarde: bij het uitvoeren van de audit mogen geen relevante uitzonderingen geconstateerd zijn. Zijn die er wel, dan is het niet mogelijk om een SOC 3-rapport uit te geven. Voor sommige organisaties is dit wellicht (nog) een struikelblok, maar voor organisaties waarvoor al een 'schone' verklaring wordt afgegeven een extra selling point. Het SOC 3-rapport mag op de website van de serviceorganisatie worden geplaatst, zodat (potentiële) klanten eenvoudig kunnen vaststellen dat de organisatie 'in control' is.

Hot topic: Privacy

Het tweede 'extra' voor de overstap naar SOC 2 is dat de SOC guide van de NOREA is uitgebreid met de privacy-categorie. In de Amerikaanse SOC 2-rapporten bestond al langer de mogelijkheid om te rapporteren over privacy. Eerder was het in Nederland niet eenvoudig mogelijk om de privacy-categorie op te nemen in de scope van de opdracht. De SOC guide verwees naar de omstandigheid dat de privacy-categorie gebaseerd is op Amerikaanse wet- en regelgeving (GAPP) en dat hiervoor in Nederland nog geen invulling bestond. Daarnaast werd de wetgeving rondom persoonsgegevens in Europa op het moment van schrijven nog herzien. Met de komst van de AVG is dat verleden tijd.

Op basis van de regels die binnen Europa gelden, kan nu prima invulling gegeven worden aan de privacy-categorie en de bijbehorende criteria. Deze hoeven dan niet per se op 'Amerikaanse' wijze ingevuld te worden. De vereisten uit de AVG sluiten namelijk ook aan op de criteria in de privacy-categorie. Punt van aandacht voor zowel de gebruiker van het rapport als de auditor is wel dat het toevoegen van de privacy-categorie aan het SOC 2-rapport *niet* betekent dat de organisatie AVG compliant is. Het betekent dat voldaan wordt aan de criteria uit de SOC 2 privacy-categorie, maar dat wil nog niet zeggen dat de organisatie daarmee ook aan alle vereisten uit de AVG voldoet.

Met het oog op de aandacht die privacy en gegevensbescherming op dit moment krijgen en vanuit de veronderstelling dat deze aandacht alleen maar toe zal nemen, is de toevoeging van de privacy-categorie een welkome aanvulling op de SOC-rapporten. De implementatie van de privacy-categorie brengt echter wel een aantal uitdagingen met zich mee. Als het goed is, is de klant als geen ander op de hoogte van de privacy-verplichtingen waaraan zij moeten voldoen en de risico's die daaruit voortvloeien. Maar hoe toets je als auditor of de klant deze allemaal geïdentificeerd heeft? En wanneer zijn er voldoende interne beheersingsmaatregelen ingericht om de risico's te beheersen? Op dit moment zijn dit nog open vragen. Of het eenvoudig mogelijk is om deze inschattingen te maken zal in de praktijk moeten blijken, want ook voor IT-auditors is deze categorie nieuw.

In het geval van een audit bij een verwerker zal de inschatting door de IT-auditor eenvoudiger zijn dan bij een verwerkingsverantwoordelijke. Neem een SaaS-provider. Deze zal in veel gevallen (sub)verwerker zijn, en is daarmee niet verantwoordelijk voor de data in de applicatie. Wel moet de SaaS-provider (technische) maatregelen treffen zodat de verantwoordelijke die de applicatie gebruikt, kan voldoen aan de AVG. Dit is eenvoudiger te controleren dan in het geval van een verwerkingsverantwoordelijke. Zeker als het gaat om de meer procedurele maatregelen en zaken als bewustzijn. Daarnaast is ook voor de serviceorganisatie zelf in een aantal gevallen een behoorlijke uitdaging om de privacy-categorie toe te voegen. De privacy-categorie en de criteria die daaronder vallen, overlappen vaak weinig met de andere categorieën. Dit kan er in de praktijk toe leiden dat een groot aantal beheersingsmaatregelen aan het raamwerk van de serviceorganisatie moet worden toegevoegd. Daarbij is het ook voor de serviceorganisatie niet eenvoudig om te bepalen wanneer men 'in control' is op het gebied van privacy, juist omdat dit nog een relatief nieuw onderwerp is in assurance rapportages.

Mapping met het Privacy Control Framework

Met het oog op de AVG heeft de Kennisgroep Privacy van de NOREA het privacy control framework (PCF) opgesteld. In samenwerking met de Kennisgroep Privacy van de NOREA hebben de opstellers van de NOREA SOC guide vervolgens een mapping gemaakt van het PCF naar de criteria van de SOC 2 privacy-categorie. Zo kunnen gebruikers van de guide eenvoudig bepalen welke interne beheersingsmaatregelen mogelijk invulling kunnen geven aan de doelstellingen uit de privacy-categorie. Uiteraard is het geen limitatieve lijst en kunnen gebruikers ook andere beheersingsmaatregelen inrichten. Het is geen 'one size fits all', maar wel een handig hulpmiddel. Ook deze mapping is opgenomen in de nieuwe SOC guide van de NOREA.

Tot slot

Al met al dus genoeg vernieuwingen die het draagvlak voor SOC 2 in Nederland kunnen vergroten. Met name het kunnen rapporteren over de privacy-categorie en het mogen uitbrengen van een SOC 3-rapport zal hieraan gaan bijdragen. De vernieuwde NOREA SOC guidance biedt handvatten voor het toepassen van deze toevoegingen. Nu is het de taak voor ons als IT-auditors om deze in de praktijk ook daadwerkelijk toe te passen.

Jeroen Francot MSc RE

Jeroen Francot werkt sinds 2015 als IT auditor bij BDO IT Risk Assurance. Daar is hij onder meer verantwoordelijk voor verschillende assurancerapportages, waaronder SOC 2, SOC 3, ISAE3402 en ISAE3000 voor een breed scala aan dienstverleners. Jeroen is daarnaast lid van de Commissie Beroepsregels van NOREA en is een van de samenstellers van de vernieuwde SOC guide.

Carlijn Frins MSc

Carlijn Frins werkt sinds 2014 als IT auditor bij BDO IT Risk Assurance, waar zij verantwoordelijk is voor diverse assuranceopdrachten zoals SOC 2, ISAE 3000 en ISAE 3402 bij verschillende typen dienstverleners. Binnen BDO is zij actief in de werkgroep Assurance en ze is tevens een van de samenstellers van de vernieuwde SOC guidance van NOREA.