WAT IS EEN ASSURANCE-OPDRACHT

Een onderzoek voor de Online Trust Coalitie

ONLINE TRUST
COALITIE

ASSURANCE-OPDRACHT

INHOUD

Samenvatting 4

Inleiding 5

Wat is de betekenis van het woord ‘assurance’ in ‘assurance-opdracht’? 6

Wat voegt een assurance-opdracht toe aan de constructie van certificeringen en toezicht? 8

Waarom richt de assurance-opdracht zich op het verleden en geeft het geen garanties voor de toekomst? 11

Waarom spelen ISAE- en SOC-rapportages een steeds grotere rol in IT-dienstverlening? 12

Samenvatting

Assurance-opdrachten spelen een steeds grotere rol in de samenleving, bijvoorbeeld bij het uitbesteden van essentiële organisatorische processen aan cloudproviders. Dit onderzoek gaat in op de vraag: wat is een assurance-opdracht en wat is de toegevoegde waarde is? Een assurance-opdracht is namelijk geen verzekering, het geeft geen zekerheid (zoals certificeringen en systemen voor kwaliteitsmanagement), maar het is ‘een verklaring die vertrouwen versterkt’. Wat is het belang van ‘vertrouwen versterken’? Hoe verhoudt een verklaring die ‘vertrouwen versterkt’ zich tot certificeringen, audits, accreditaties die zekerheid geven?

Een assurance-opdracht onderzoekt de waarde van de informatie over een onderzoeksobject (denk aan een dienst van een cloudprovider die getoetst is op allerlei aspecten, waarover informatie beschikbaar is en die allerlei certificeringen heeft) voor een specifieke belanghebbende (bijv. een eindgebruiker, een toezichthouder of een accountant) om een specifieke beslissing op te baseren (bijv. om een belangrijk proces binnen een organisatie uit te besteden en daarvoor de verantwoordelijkheid te nemen).

Een assurance-opdracht speelt een rol wanneer bij een beslissing verschillende, soms tegenstrijdige, belangen en doelen afgewogen moeten worden. De evaluaties en metingen die de beslisser voor zich heeft, zoals certificeringen en andere kwalificaties van een product of dienst, spelen natuurlijk een belangrijke rol bij de beslissing, maar het wegen van de belangen en doelen, zoals de risico’s verbonden aan een beslissing, blijft bij de beslisser. De cloud is niet meer uit onze samenleving weg te denken. De cloud speelt een belangrijke rol in onze dagelijkse activiteiten, in bedrijven, bij digitale innovaties en het beantwoorden van de grote maatschappelijke vraagstukken waar de samenleving voor staat.

Inleiding

Het doel van certificeringsschema's, audits, toezicht, vergunningen en alles wat in de samenleving is georganiseerd rondom kwaliteit van diensten en producten, is dat gebruikers deze diensten en producten kunnen vertrouwen. Ze bieden de zekerheid dat een dienst of product levert wat mag worden verwacht en dat de dienst of het product veilig en betrouwbaar is.

Het woord 'assurance' heeft in het vakgebied van certificeringen en standaarden veel verschillende betekenissen, allemaal bedoeld om zekerheid te geven aan afnemers van diensten en producten. Dit paper beoogt orde te scheppen in die betekenissen en laat zien hoe een specifieke vorm van assurance, de assurance-opdracht, het cruciale bouwblok is van een risk-based benadering van zekerheid.

Het paper legt het standpunt van de Online Trust Coalitie uit, dat de assurance-opdracht een essentieel instrument is voor bestuurders, toezichthouders en andere belanghebbenden. De assurance opdracht moet hen in staat te stellen verantwoordelijkheid te nemen, dat zij een online dienst gebruiken of toestaan en om gericht maatregelen te kunnen nemen of eisen om de bijbehorende risico's te beperken.

IFAC, de International Federation of Accountants, voegt aan dit complexe geheel het concept "assurance engagement" toe (in deze publicatie vertaald met 'assurance-opdracht'). Assurance-opdrachten worden veel gegeven wanneer organisaties voor hen belangrijke bedrijfsprocessen uitbesteden aan externe clouddienstverleners. Wat voegt dit concept 'assurance-opdracht' toe?

Bij het beantwoorden van deze vraag wordt de Nederlandse definitie van assurance-opdracht gevolgd, uit het *'Stramien voor assurance-opdrachten'* vastgesteld door de NOREA-ledenvergadering (14 december 2016).

"Een assurance-opdracht is een professionele dienst waarbij een IT-auditor voldoende en geschikte assurance-informatie wil verkrijgen om een conclusie tot uitdrukking te brengen om de mate van vertrouwen van de beoogde gebruikers, niet zijnde de verantwoordelijke partij, in de uitkomst van de meting of evaluatie van het onderzoeksobject ten opzichte van criteria te versterken."

In het "stramien" wordt ook het Engelse origineel gegeven (IFAC): "An assurance engagement is an engagement in which a practitioner aims to obtain sufficient appropriate evidence in order to express a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the measurement or evaluation of an underlying subject matter against criteria."

Het valt op dat de Nederlandse vertaling de Engelse tekst op de voet volgt. Maar dat het woord waar het om gaat in deze beschrijving, namelijk 'assurance', onvertaald blijft. In deze publicatie wordt daarom ook het woord 'assurance' onvertaald gebruikt. In de volgende paragraaf wordt ingegaan op de betekenis van het woord 'assurance'. Een tweede verschil tussen het Engelse origineel en de Nederlandse vertaling is dat het Engelse woord 'practitioner' is vertaald met 'IT-auditor'. Een vertaling die aansluit op de Nederlandse situatie waarin iemand die zich IT-auditor noemt is ingeschreven in het Beroepsregister van de NOREA en aan vaste eisen moet voldoen wat opleiding, ervaring en ethische normen.

In de volgende paragrafen wordt ingegaan op de elementen van de beschrijving van ‘assurance-opdracht’. Daarbij komen de volgende vragen aan de orde:

1. Wat is de betekenis van het woord ‘assurance’ in ‘assurance-opdracht’?
2. Wat voegt een assurance-opdracht toe aan de constructie van certificeringen en toezicht?
3. Waarom richt de assurance-opdracht zich zo nadrukkelijk op het verleden?
4. Waarom speelt assurance (in de vorm van ISAE- en SOC-rapportages) een steeds grotere rol in IT-dienstverlening?

Wat is de betekenis van het woord ‘assurance’ in ‘assurance-opdracht’?

Het woord assurance in ‘assurance-opdracht’ wordt door de beschrijving in het stramien voor assurance-opdrachten niet vertaald. De reden is dat het Engelse woord ‘assurance’ een betekenis heeft die het Nederlands niet kent. Namelijk: assurance in de betekenis van “een positieve verklaring met als doel vertrouwen te geven”[1].

Voorbeelden van ‘assurance’ in de betekenis van ‘een positieve verklaring om vertrouwen te geven’:

1. “Ga gerust op reis, want de gids is erg ervaren”.
   De zinsnede “want de gids is erg ervaren” is een ‘assurance’: een verklaring bedoeld om in vertrouwen de beslissing te nemen om op reis te gaan.

2. “Ik zou kiezen voor deze behandeling, want die is vrijwel altijd succesvol”.
   De zinsnede ‘want die is vrijwel altijd succesvol’ is een ‘assurance’: een uitspraak bedoeld om in vertrouwen de beslissing te nemen voor een behandeling.

De betekenis ‘een positieve verklaring met als doel vertrouwen te geven’ kent het Nederlands niet.

Het woord assurance heeft echter ook een aantal betekenissen, die we in het Nederlands wél kennen, en die ook nog eens een rol spelen in de wereld van kwaliteitsmanagement en certificering. Dat zorgt voor veel verwarring rond de betekenis van het woord ‘assurance’ in ‘assurance-opdracht’. Assurance heeft immers ook de betekenis ‘zekerheid geven’, ‘garanderen’. Kwaliteit assurance, een onderdeel van systemen voor kwaliteitsmanagement, is immers wél bedoeld om de afnemer zekerheid te geven. Assurance heeft dan de betekenis: ‘zekerheid geven dat een dienst of product de verwachte eigenschappen heeft’. Kwaliteit assurance speelt een belangrijke rol bij de productie van systemen en apparaten, maar wordt ook toegepast op diensten.

1 as·sur·ance / ə’shoŏrəns/
1. a positive declaration intended to give confidence; a promise:
2. confidence or certainty in one's own abilities.
3. chiefly Brit. insurance, specifically life insurance
(Oxford University Languages/ OUL.com).

Ook de *Common Criteria*, die zo'n belangrijke rol spelen in de internationale handel, gebruiken het woord 'assurance' in de samenstelling 'assurance-level' in de zin van 'geven van zekerheid'[2]. Echter, een assurance-opdracht zoals gedefinieerd door de NOREA, geeft geen zekerheid, maar versterkt vertrouwen.

Het woord assurance wordt tenslotte in het Engels ook nog gebruikt om een bepaald type 'verzekering' aan te duiden. Namelijk een verzekering voor gevallen dat een voorval zich zeker zal voordoen, maar het is niet bekend wanneer. Een overlijdensrisicoverzekering is een voorbeeld van een 'assurance'. Een brandverzekering (de verzekeraar weet niet of er ooit brand zal uitbreken) is een 'insurance'.

De vraag wat de assurance-opdracht bijdraagt aan certificeringen en toezicht (bedoeld om de afnemer zekerheid te geven) kan nu preciezer worden omschreven: wat is het belang van 'een onderzoeksopdracht om vertrouwen te versterken' als er ook systemen en methodieken bestaan die zekerheid en garantie geven bij het afnemen van producten en diensten?

Een 'intuïtief' antwoord op deze vraag wat een assurance-opdracht toevoegt aan de hand van de eerdere voorbeelden.

Een assurance-opdracht in het geval van het reisvoorbeeld ('ga gerust op reis want de gids is erg ervaren') zou kunnen zijn:

Een opdracht voor een onafhankelijke deskundige om te onderzoeken welke zekerheid u kunt ontlenen, bij het nemen van mijn beslissing om te reizen op basis van het feit dat de gids jaren ervaring heeft. Als ik wil gaan reizen en maar één been heb is de ervaring van de gids een relevant gegeven, maar misschien niet doorslaggevend. Het onderzoek van de onderzoeker die de assurance opdracht uitvoert zou kunnen zijn om te onderzoeken wat de waarde van de informatie (de ervaring van de gids) betekent voor mijn beslissing om te reizen, wetende dat ik maar één been heb.

In het tweede voorbeeld ('ik zou kiezen voor deze behandeling, want die is vrijwel altijd succesvol) zou een assurance-opdracht kunnen inhouden dat een onafhankelijk deskundige uitzoekt of er aanwijzingen zijn dat in mijn specifieke geval, die behandeling ook succesvol is. Het resultaat van de assurance-opdracht kan zijn dat de onderzoeker een conclusie formuleert dat het succespercentage ook in mijn geval van toepassing is.

---

2 Common Criteria (CC) spreekt van 'assurance' als "grounds for confidence that a Target Of Evaluation (TOE) meets the Security Functional Requirements (SFRs)" - bron: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 CCMB-2017-04-001 p.17. retrieved 12.09.2022 van *https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf*

De CC gebruiken het woord assurance in de samenstelling 'assurance level'. Een assurance level is 'a set of requirements … representing a point on the … predefined assurance scale, that form an assurance package'. Idem.P.17

Een 'assurance package' is:
'composed assurance package — assurance package consisting of requirements drawn from CC Part 3 (predominately from the ACO class), representing a point on the CC predefined composition assurance scale'. Een 'assurance package' is, in andere woorden, een set van eisen behorend bij een voorgedefinieerd 'assurance level' waar de beoordeling aan wil voldoen.

'Common Criteria' en 'Assurance Levels' hebben hetzelfde doel als assurance-opdrachten, namelijk redenen verschaffen om het vertrouwen te versterken in de uitkomst van een meting of evaluatie. Het grote verschil is dat CC zekerheid geeft, op een precies gedefinieerde manier. En een assurance-opdracht gaat over de vraag wat de relevantie van de informatie, die zekerheid geeft, bijvoorbeeld van de CC, voor de beslissing waar de beoogd gebruiker van de assurance-opdracht voor staat.

Wat voegt een assurance-opdracht toe aan de constructie van certificeringen en toezicht?

De NOREA omschrijft een assurance-opdracht als:

"Een assurance-opdracht is een professionele dienst waarbij een IT-auditor voldoende en geschikte assurance-informatie wil verkrijgen om een conclusie tot uitdrukking te brengen om de mate van vertrouwen van de beoogde gebruikers, niet zijnde de verantwoordelijke partij, in de uitkomst van de meting of evaluatie van het onderzoeksobject ten opzichte van criteria te versterken."

De belangrijkste verschillen tussen een assurance-opdracht en andere manieren om vertrouwen te geven (certificeringen of toezicht) komen naar voren in deze beschrijving.

1. **Een assurance-opdracht is een professionele dienst**
   een assurance-opdracht is een "professionele dienst waarbij een IT-auditor voldoende en geschikte assurance-informatie wil verkrijgen om een conclusie tot uitdrukking te brengen om…".

   Hierbij valt het volgende op:

   a.) In de omschrijving staat 'een assurance-opdracht is een professionele dienst'. Waarom wordt hier van 'dienst' gesproken en niet van bijvoorbeeld: 'een assurance opdracht is een onderzoeksopdracht voor een professional'?

   b.) In de omschrijving staat 'om een conclusie tot uitdrukking te brengen'. Waarom staat er niet iets als: een assurance-opdracht is een opdracht 'om een assurance verklaring op te stellen' of 'om assurance te geven'?

   c.) In de omschrijving staat dat de IT-auditor informatie 'wil verkrijgen'. Waarom staat er niet iets als 'verzamelt'

   Waarom is een assurance-opdracht een dienst?
   Een certificering wordt uitgevoerd om tot een certificaat te komen. Dat certificaat is een verklaring door een gekwalificeerde professional (die geaccrediteerd moet zijn en daarvoor aan allerlei eisen moet voldoen) dat een onderzoeksobject aan bepaalde gespecificeerde eisen voldoet.

   Een assurance-opdracht leidt echter niet tot een herhaalbare gedefinieerde reeks van handelingen, die in gelijke gevallen altijd tot dezelfde uitkomst leiden (zoals dat bij een certificering het geval is). Een assurance-opdracht is een dienst. De opdracht leidt tot een professioneel oordeel. In gelijke gevallen kan een assurance-opdracht tot verschillende uitkomsten leiden, bijvoorbeeld omdat de IT-auditor verschillende (vaak tegenstrijdige) belangen op een andere manier weegt.

   Een assurance opdracht is een "professionele dienst". De opdrachtgever kan gerust zijn dat een professional volgens professionele standaarden te werk zal gaan om tot het oordeel te komen en een conclusie te formuleren. En omdat die professional is aangesloten bij een beroepsorganisatie, kan de opdrachtgever die professional aanspreken wanneer de professional niet volgens deze standaarden te werk gaat of ondeskundig is.

Waarom is het belangrijk dat de IT-auditor iets 'wil verkrijgen' bij een assurance-opdracht?

Een opvallend woord in deze omschrijving, is het gebruik van het woord 'wil': 'de IT-auditor .... wil ... voldoende en geschikte informatie verkrijgen ... om ... een conclusie tot uitdrukking te brengen'.

Bij certificering of andere verklaringen speelt de "wil" van de onderzoeker geen enkele rol. Het certificeringsschema beschrijft welke informatie moet worden verzameld en er zijn spelregels hoe die informatie wordt gewogen. In een 'assurance-opdracht' staat echter de 'wil' van de onderzoeker centraal. De onderzoeker "wil een conclusie ... tot uitdrukking brengen...om".

Daarmee wordt de assurance-opdracht in een heel ander domein geplaatst dan die van certificering. Namelijk in domeinen waarin een beslissing niet genomen kan worden op basis van tevoren geformuleerde beslisregels (zoals een certificering). Het menselijk oordeel geeft de doorslag in de conclusie. In dat oordeel 'wil' de beoordelaar tegenstijdige en ongelijksoortige belangen afwegen op een zo objectiveerbare en transparante manier.

De IT-auditor wordt hiermee geplaatst in dezelfde situatie als andere professionals die zo goed mogelijk belangen wegen en bepaalde doelen realiseren (i.e. willen bereiken). Bijvoorbeeld artsen, rechters en advocaten, agenten, militairen, wetenschappers. Een arts wil tot een oordeel komen en daarin tegenstrijdige belangen wegen. Voorop staat echter het welzijn van de patiënt die de arts voor ogen heeft. De arts 'wil' het welzijn van deze individuele specifieke patiënt dienen. Ook als het belang van de individuele patiënt ingaat tegen het belang van de groep of van anderen (de publieke opinie, financiering etc.). Ook als er protocollen zijn, die precies beschrijven hoe een behandeling plaatsvindt, is het aan de arts om daarin, met het oog op het welzijn van de patiënt, eigen professionele en keuzes te maken, die de arts later kan verantwoorden. Een rechter weegt in het oordeel ook allerlei belangen. Die van de samenleving, de toepasselijke wetgeving en de individuele verdachte. De rechter 'wil' dat een oordeel de bedoeling van de wet respecteert, belangen van samenleving en slachtoffer meeweegt en ook nog eens goed is voor de verdachte. Die belangen worden gewogen en geen van de belangen geeft bij voorbaat de doorslag. Daar is geen beslisboom voor en de rechter neemt zelf de beslissing. De rechter kan die beslissing wel verantwoorden. Het is geen willekeurige keuze.

Een assurance-opdracht wordt uitgevoerd door een professional (de IT-auditor) om te komen tot een uitspraak over de waarde van informatie voor een beoogd gebruiker, zie de volgende paragraaf. Die uitspraak van de IT-auditor is een (feilbaar, onvolmaakt) menselijk oordeel. Door een professional met ethische standaarden en die voldoet aan strikte eisen wat betreft de opzet en de uitvoering van het onderzoek. En aan wie strenge eisen worden gesteld wat betreft kennis en ervaring. Ook de IT-auditor kan het oordeel verantwoorden.

Vaak is het veel wenselijker, als dat kan, om met beslisbomen en heldere besliscriteria te werken bij het nemen van een beslissing (zoals bij certificeringen). Een assurance-opdracht komt echter in beeld als dat niet mogelijk is. Een oordeel op basis van strikte eisen en criteria en meetprocedures, is om allerlei redenen (moreel, praktisch, cultureel) onwenselijk of onmogelijk.

Een belangrijk element, dat impliciet in de beschrijving staat, is dat de onderzoeker daarbij onder toezicht staat van een beroepsorganisatie: de onderzoeker is een 'IT-Auditor'. In Nederland staat een IT-auditor onder toezicht van de NOREA, de beroepsvereniging die toeziet op integriteit, de vakkundigheid en de kwaliteit van de onderzoeksmethodiek van de onderzoeker. Doel van de assurance-opdracht is dat degene voor wie de assurance-opdracht wordt uitgevoerd, in vertrouwen kan beslissen en beter verantwoordelijkheid kan nemen (en afleggen) voor die beslissing.

2. De beoogd gebruiker

Een tweede groot onderscheid tussen assurance-opdracht en andere manieren om zekerheid te geven over de kwaliteiten van een object van onderzoek, is dat een assurance-opdracht wordt uitgevoerd met het oog op “een beoogde gebruiker”. Dat wil zeggen een specifieke gebruiker in een specifieke rol en in een specifieke (beslis)situatie. Bijvoorbeeld de directeur van een bedrijf of organisatie die moet beslissen om een voor de organisatie cruciale dienst uit te besteden. Of een bestuurder die verantwoordelijkheid moet nemen over de veiligheid van een onlinedienst waar een organisatie van afhankelijk is. De beoogd gebruiker kan ook een (overheids-)toezichthouder of accountant zijn, die wil beslissen of de continuïteit van een organisatie voldoende is gewaarborgd als cruciale diensten zijn uitbesteed. Beoogd gebruikers kunnen financiers zijn, die zich afvragen of bij de uitbesteding van diensten aan derden hun belangen voldoende zijn gewaarborgd.

Certificeringen en andere vormen van zekerheid zijn generiek, ongeacht de partij die wil steunen op de uitkomst van de meting en de onderzoeker. Bij een assurance-opdracht is die beoogde gebruiker van invloed op het onderzoek en de onderzoeker is van invloed op de geformuleerde conclusie.

De omschrijving perkt het begrip ‘beoogde gebruiker’ in. De beoogde gebruiker is “niet zijnde de verantwoordelijke partij”. Niet degene die verantwoordelijk is voor het object dat onderzocht wordt.

De partij die verantwoordelijk is voor het object van onderzoek kan een assurance-opdracht geven, maar de beoogd gebruiker van de assurance-opdracht is nooit die verantwoordelijke partij, de partij verantwoordelijk voor het object van onderzoek.

Dit is een verschil tussen een certificering en een assurance-opdracht. Veel certificeringen worden immers uitgevoerd met als doel dat óók (of zelfs juist) de verantwoordelijke partij zelf de conclusie kan trekken alles op orde te hebben.

Als de verantwoordelijk partij de beoogd gebruiker is, dan is er geen sprake van een assurance-opdracht.

3. Vertrouwen versterken

De assurance-opdracht wordt gegeven met als doel “een conclusie tot uitdrukking te brengen om de mate van vertrouwen in de uitkomst van de meting of evaluatie van het onderzoeksobject… te versterken”.

Een assurance-opdracht geeft opdracht het onderzoek te doen, dat nodig is om het vertrouwen van een beoogd gebruiker in de beschikbare informatie (de meting of evaluatie) over het object van onderzoek (bijvoorbeeld een clouddienst) te versterken.

Het resultaat van een assurance-opdracht is dus geen ja-of-nee oordeel, zoals een certificering. Een certificering verklaart dat het object van onderzoek aan bepaalde eisen voldoet. Het resultaat van een assurance-opdracht is echter een uitspraak om vertrouwen in de uitkomst van zo’n evaluatie of meting te versterken.

Waarom richt de assurance-opdracht zich op het verleden en geeft het geen garanties voor de toekomst?

Een belangrijke bron van misverstanden rond assurance is dat een certificering over de toekomst gaat (of een product of dienst in de toekomst de verwachte eigenschappen zal hebben). Een assurance-opdracht zegt niets over de toekomst.

Een assurance-opdracht komt in beeld als er sprake is van een menselijk oordeel. Er is geen kant en klare certificering, beslisboom of onderzoek template die de ‘beoogd gebruiker’ voldoende zekerheid kan geven. De vraag achter een assurance-opdracht is: wat is de waarde van die beschikbare (misschien wel zekere) informatie bij het nemen van een beslissing in een situatie waarin geen volledige zekerheid kan zijn wat de juiste beslissing is?

Een assurance-opdracht wordt gegeven als de vraag luidt: wat betekent de informatie over het onderzoeksobject voor de beoogde gebruiker, voor een specifieke beslissing? Als er geen sprake kan zijn van zekerheid bij het nemen van een beslissing, maar er sprake is van ‘vertrouwen’.

Waarom spelen ISAE- en SOC-rapportages een steeds grotere rol in IT-dienstverlening?

'Assurance-opdrachten' spelen de laatste jaren een steeds grotere rol in het uitbesteden van organisatorische processen aan externe dienstverleners. En dat vaak boven op de certificeringen die de dienstverleners al hebben. Wat is de reden van die toegenomen populariteit?

Voordeel 1: Assurance helpt organisaties zelf verantwoordelijkheid nemen bij uitbesteden van processen

ISAE- en SOC-rapportages, de bekendste voorbeelden van assurance-opdrachten, verzamelen de informatie die nodig is voor een 'assurance-opdracht'. En die opdracht wil een beoogd gebruiker (zoals de bestuurder van een organisatie) in staat stellen een beslissing te nemen en beter verantwoordelijkheid te kunnen afleggen. Als de beslissing verkeerd uitpakt blijft de beoogd gebruiker verantwoordelijk, maar de beslisser kan met de resultaten van een assurance-opdracht wel beter onderbouwen waarom de beslissing genomen werd. Bijvoorbeeld bij calamiteiten als persoonsgegevens van klanten op straat komen te liggen of wanneer een organisatie schade lijdt omdat er iets fout gaat bij de externe dienstverlener.

Veel dienstverlening en producten komen in onze samenleving alleen op de markt, als ze aan strikte eisen voldoen. Dat is niet het geval bij clouddiensten. Bij het uitbesteden van processen aan externe dienstverleners maakt de bestuurder zelf de afweging of de risico's van 'zelf-doen' opwegen tegen de risico's van 'uitbesteden'.

Assurance-opdrachten helpen organisaties de risico's van het uitbesteden van processen te beoordelen. Certificeringen gaan over de vraag of de dien\st die de derde partij levert aan bepaalde eisen voldoet. Maar beantwoorden niet de vraag wat het vertrouwen is wat een beslisser aan die meting/evaluatie kan ontlenen.

Voordeel 2: Bij IT-dienstverlening zijn complexe constant veranderende ketens van dienstverleners betrokken.

Een tweede reden waarom ISAE- en SOC-rapportages een grotere rol spelen, is dat bij uitbesteding aan clouddienstverleners vaak een hele keten aan dienstverleners is betrokken. Die allen een kleine, in hoge mate gestandaardiseerde (deel)component aanbieden, en tezamen in interactie de dienst vormen. Steunen op certificeringen van die dienstverleners is een goed begin, maar welke zekerheid al die certificeringen bieden aan de gebruiker is niet duidelijk. De meeste certificeringen geven immers geen heldere beschrijving van de risico's van de deeldiensten. Dan moet de organisatie die een dienst afneemt zelf onderzoek doen naar de risico's bij alle dienstverleners. En dat betekent voor de dienstverlener dat er regelmatig auditors over de vloer komen, die allemaal ongeveer hetzelfde onderzoeken. Dat is niet efficiënt, kost veel inspanning en vergt veel kennis.

Het is daarom in meerdere opzichten efficiënter en doelmatiger als de partij die een deeldienst aanbiedt, eenmalig een audit laat uitvoeren en een assurance rapportage laat schrijven, waar vervolgens de IT-auditor van een afnemer van de dienst, van de klanten van die afnemer, van de toezichthouder of van een stelselautoriteit, op kan steunen.

Voordeel 3: Verantwoording - een extra check door een onafhankelijke, deskundige.

Een assurance-opdracht helpt een beslisser aan te tonen zorgvuldig te werk te zijn gegaan bij het nemen van een beslissing. Een onafhankelijke derde is ingeschakeld die onderzocht heeft welk vertrouwen de beslisser kan ontlenen aan de informatie beschikbaar over het object van onderzoek.

Voordeel 4: Assurance is risk-based en niet rule-based

Een vierde voordeel van assurance-opdrachten bij het uitbesteden van processen aan derden, is dat een assurance-opdracht de informatie geeft aan partijen om risico's te wegen. Een certificering is een binair oordeel: ja of nee. Assurance geeft een genuanceerd beeld van de aspecten van de dienstverlening, die relevant zijn voor de partij die deze dienst gebruikt. De technische kant, hoe zaken zijn georganiseerd, de mensen in de organisatie en organisatiecultuur, de processen en de praktijk. Veel certificeringsschema's eisen allerlei maatregelen en voorzieningen: ze zijn rule-based. Waarbij vaak niet duidelijk is of deze maatregelen en voorzieningen afdoende zijn wanneer een dienst wordt gebruikt voor een specifiek doel. Of juist veel te zwaar zijn voor bepaalde toepassingen. Assurance is risk-based en geeft inzage in de risico's.

WILT U CONTACT OF MEER INFORMATIE?
info@onlinetrustcoalitie.nl
www.onlinetrustcoalitie.nl