Beheersing van de digitale informatieverwerking;

wat dragen IT-assurance-rapporten hieraan bij?

Han Boer

SAMENVATTING Bij uitbesteding van bedrijfsprocessen wordt gebruik gemaakt van assurance-rapporten om zekerheid en inzicht te krijgen in de kwaliteit van de beheersing van de uitbestede processen. Indien het processen betreft die betrekking hebben op de financiële verslaglegging van de uitbestedende organisatie is de meest bekende vorm het ISAE 3000- en 3402-assurance-rapport. De aanleiding voor dit artikel is de door het Amerikaanse instituut van accountants ontwikkelde SOC 2-handreiking voor assurance-rapporten met betrekking tot IT-serviceorganisaties. Het is een waardevolle uitbreiding aan het pallet van assurance-rapporten.

RELEVANTIE VOOR DE PRAKTIJK Een relativering is op zijn plaats. Vanuit het operationeel perspectief komt assurance-rapportage te laat beschikbaar om tijdig maatregelen te kunnen nemen bij afwijkingen van het normale verwerkingspatroon. Informatie-uitwisseling tussen serviceorganisatie en gebruikers op operationeel niveau is de basis voor de operationele beheersing. De auditor kan in zijn rol als adviseur een belangrijke bijdrage leveren om deze operationele beheersing van de keten serviceorganisatie - gebruikersorganisatie te realiseren. Afhankelijk van de situatie kan een assurance-rapport een betekenisvol sluitstuk van de beheersingsketen zijn.

1 Inleiding

In de huidige digitale wereld maken particulieren maar ook organisaties veelvuldig gebruik van door derden aangeboden IT-diensten. Vaak is de dienst zo vanzelfsprekend dat de gebruiker zich helemaal niet realiseert dat gebruik wordt gemaakt van een door derden aangeboden IT-service. Uitbesteding die leidt tot afhankelijkheden die duidelijk worden op het moment dat er incidenten plaatsvinden. Voor de particulier wellicht minder ingrijpend, maar bij bedrijfsmatig gebruik kan het desastreus zijn. Om te weten waar afhankelijkheden ontstaan, moet een organisatie een actueel beeld hebben van de IT-diensten die van derden worden afgenomen. In het verleden was dit beperkt tot de leverancier van de hardware en de op deze hardware geïnstalleerde software. Dit is echter sluipend uitgebreid met de beschikking over software, verwerkingsplatformen of servers van derden. Een uitbreiding die lang niet altijd onder regie van de bedrijfsfunctie verantwoordelijk voor de IT-infrastructuur plaatsvindt.

Het gebruik van computercapaciteit van derden respectievelijk het beheer van computers door derden is niet nieuw. Dit wordt vaak aangeduid als het gebruik maken van een computerservicebureau, IT-housing of IT-cloud service. Doordat het beheer geen onderdeel uitmaakt van de eigen organisatie is direct toezicht niet meer mogelijk, terwijl de verantwoordelijkheid voor het proces blijft. Overigens geldt dit niet alleen voor uitbestede IT-operaties maar voor alle vormen van uitbesteding. De uitbesteding van IT was door zijn complexiteit en kapitaalintensiteit echter een terrein waar uitbesteding vanaf het begin van de digitalisering grote opgang maakte.
In theorie zijn er drie mogelijkheden om de verantwoordelijkheid voor het proces te kunnen blijven dragen:

- het houden van directe betrokkenheid bij de opzet en uitvoering van de operatie;
- van de serviceverlener verlangen dat hij informatie oplevert over de werking van de beheersing van de door hem uitgevoerde (IT-)verwerkingen;
- het opvragen van een door een vertrouwde deskundige geverifieerd rapport, waarin deze aangeeft in hoeverre de beheersing toereikend is geweest.

In de praktijk zie ik nog een vierde punt: vertrouwen op de goede naam van de serviceorganisatie. Hoewel dit veelvuldig voorkomt zult u met mij eens zijn dat dit een ongewenste situatie is, die niet past binnen een professionele omgeving.

De eerst genoemde oplossing staat haaks op de motieven om tot uitbesteding over te gaan. De uitvoering van het (IT-)proces wordt juist afgestoten om er geen directe operationele bemoeienis meer mee te hebben. Het niet loslaten van de bemoeienis bij de uitvoering betekent dat de beoogde efficiencyvoordelen niet gerealiseerd worden.

De tweede oplossing om de verantwoordelijkheid te kunnen blijven dragen betekent dat de informatie-uitwisseling over de procesbeheersing moet worden ingericht. De uitbestedende organisatie moet definiëren welke informatie nodig is, maar ook een proces inrichten om de beheersing uit te voeren. De serviceorganisatie moet in de informatieverstrekking aan de gebruiker kunnen voorzien. Systeemtechnisch is dit een extra functionaliteit; een metafunctionaliteit naast de operationele functionaliteit van het in opdracht uitgevoerde proces. Deze benadering wordt ook wel aangeduid met monitoring approach. In de praktijk constateer ik dat de invulling van deze monitoring van de service organisatie slechts ten dele is ingevuld; onvoldoende om hiermee de verantwoordelijkheid voor het uitbestede proces aantoonbaar te kunnen dragen.

De als derde genoemde oplossing is de meest gevolgde en inmiddels redelijk ontwikkeld. Een assurance-rapport geeft achteraf de bevestiging dat de processen in scope voldoen aan gestelde normen. Kritisch geformuleerd: vertrouwen vooraf met achteraf een bevestiging in hoeverre het vertrouwen niet is geschonden. Een veel voorkomende invulling is, dat op verzoek van serviceorganisaties of op verzoek van gebruikers van diensten, auditors van serviceorganisaties certificaten en assurance-rapporten met betrekking tot de kwaliteitsbeheersing uitbrengen. De standaarden die hiervoor gebruikt kunnen worden ontwikkelen zich steeds verder. Zo is ISO 27001: 2005 vervangen door ISO 27001: 2013 (NEN, 2013), en Standaard 3000 doorontwikkeld naar Standaard 3402 “Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie” (NBA, 2015). Specifiek voor IT-serviceorganisatie is door het Amerikaanse instituut van accountants (American Institute of Certified Public Accountants; AICPA) het SOC 2-assurance-rapport ontwikkeld (AICPA, 2012). Een veelbelovende rapportagevorm, die orde kan brengen in de vele verschijningsvormen van IT-gerelateerde assurance-rapporten onder standaard 3000. In paragraaf 3 zal hier nader op worden ingegaan.

Naar mijn waarneming is de inhoud en de vorm van assurance-rapportages sterk bepaald vanuit de audit-professie; de aanbieder van het assurance-product. De verstrekkers van assurance-rapporten hebben hun rapporten ontwikkeld vanuit hun bekende frameworks voor het uitvoeren van reviews en het afgeven van oordelen. Dit geldt voor de gehele beroepsgroep van auditors, zoals financial auditors (accountants), IT-auditors en ISO-auditors. Wat ontbreekt is het neerzetten van een op beheersing gericht operationeel monitoring-proces dat leidt tot vertrouwen in de uitbesteding op elk niveau van de uitbestedende organisatie en op ieder moment. Het monitoring-proces beweegt zich over de keten; de serviceorganisatie moet zijn processen zodanig inrichten dat het de uitbesteder van monitoring-informatie voorziet; de uitbesteder (gebruiker) moet processen hebben om de monitoring uit te voeren en in te kunnen grijpen als zaken anders lopen dan verwacht. Waarbij in mijn beeld het assurance-rapport een sluitstuk kan zijn. De woorden “kan zijn” zijn bewust gekozen, zoals uit de paragraaf over de inpassing van assurance-rapporten (paragraaf 5) zal blijken. Het is lang niet altijd noodzakelijk voor de beheersing van uitbestede processen dat de serviceorganisatie een assurance-rapport overlegt. Ook het omgekeerde komt voor. Dit zijn de situaties waar een assurance-rapport comfort zou kunnen geven maar een passend assurance-rapport niet te verkrijgen is.

Alvorens in de paragrafen 4 en 5 op deze praktische implicaties ten aanzien van assurance-rapporten in te gaan belicht ik in de paragrafen 2 en 3 eerst de kenmerken van assurance-rapporten. Afsluitend wordt in paragraaf 6 op basis van de kenmerken en de praktische beperkingen een conclusie getrokken ten aanzien van de toegevoegde waarde van assurance-rapporten.

2 Assurance-rapporten

Nederlandse accountants en register-IT-auditors werken voor de uitvoering van assurance-werkzaamheden op basis van door de International Auditing and Assurance Board (IAASB) vastgestelde standaarden. De uitgangspunten van de assurance-standaarden zijn vastgelegd in het “international framework for assurance engagements” (IAASB, 2005). Door de Nederlandse Beroepsorganisatie van Accountants (NBA) in de Handleiding Regelgeving Accountancy (HRA) opgenomen met de titel “Stramien voor assurance-opdrachten”. Het stramien geldt in principe voor alle werkzaamheden waarbij de accountant zekerheid geeft, zowel met betrekking tot historische financiële informatie als andere oordelen, waaronder assurance-rapporten inzake controls bij serviceorganisaties. Om het scherp te stellen, overeengekomen specifieke werkzaamheden, samenstellen van financiële ver-

antwoordingen en advieswerkzaamheden vallen buiten het stramien.

Het uitvoeren van wettelijk verplicht onderzoek van de jaarrekening is het domein dat door de wetgever in BW 2, artikel 393 exclusief is toegewezen aan de accountant (RA of AA met certificerende bevoegdheid). De overige assurance-producten, anders dan de accountantsverklaring, kennen deze wettelijk verankerde bescherming niet. Het is aan de gebruiker van de assurance-rapportage om te bepalen of hij de auditor voldoende gekwalificeerd vindt om het oordeel voor hem van betekenis te laten zijn. Dat de assurance-verstrekker werkt volgens bewaakte kwaliteitsnormen ten aanzien van opleiding, ervaring, professionaliteit en toezicht is voor de gebruiker van het oordeel van belangrijke toegevoegde waarde. Accountant RA / AA, Register-IT-auditor (RE), ISO-auditor en ISACA CISA-auditor zijn beroepskwalificaties waar de gebruiker van de rapportage op basis van de onderliggende accreditaties en beroepsregels waarde aan toekent.

De genoemde professionals werken binnen verschillende regelgevende kaders. Wij concentreren ons eerst op de accountant en IT-auditor RE. Zij werken op basis van beroepsregels en standaarden die zijn gebaseerd op de IFAC IAASB-standaarden. Waarbij Register-IT-auditors (RE's) door de NBA zijn erkend als een andere professional op wiens werkzaamheden binnen hun vakgebied door een RA gesteund mag worden gelijk als was het uitgevoerd door een accountant (RA / AA met certificerende bevoegdheid). De hierna volgende paragraaf (3) betreft specifiek op IT gerichte assurance-rapporten, waarbij ook wordt stilgestaan bij assurance afgegeven door professionals die niet werken onder de IFAC IAASB-standaarden.

Voor de uitvoering van assurance-opdrachten niet betrekking hebbend op historische financiële informatie heeft de IAASB ISAE 3000 vastgesteld: "Assurance engagements other than audits or reviews of historical financial information". De International Auditing and Assurance Standards board (IAASB) is een onafhankelijke commissie die zich bezighoudt met het ontwikkelen en vaststellen van standaarden voor leden van de International Federation of Accountants (IFAC). NBA (beroepsorganisatie van accountants) en NOREA (beroepsorganisatie van Register-IT-auditors) zijn respectievelijk lid en associated lid van IFAC. De NBA[1] heeft deze standaard in de HRA opgenomen onder de nadere voorschriften controle- en overige standaarden (NV COS) 3000: Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie. Standaard 3000 is gebaseerd op het eerder genoemde stramien voor assurance-opdrachten. De standaard geeft de vereisten waaraan de opdracht (waaronder scope / reikwijdte), de opdrachtuitvoering en de rapportage moeten voldoen. Inhoudelijk gezien is de standaard leeg, scope/reikwijdte en gehanteerde norm worden bepaald door de opdrachtgever, waarbij de auditor moet vaststellen of deze aan de in de standaard gestelde algemene eisen voldoen. De standaard kan worden toegepast voor het beoordelen van producten en processen. Een voorbeeld van een op een product gericht assurance-onderzoek in de digitale wereld is software-certificering. Deze toepassing van standaard 3000 is relatief beperkt. De assurance-standaard wordt door IT-auditors het meest toegepast voor oordelen over "opzet en bestaan" of "opzet, bestaan en werking" van processen. In de digitale omgeving is dit dan een oordeel over procedures binnen IT-serviceorganisaties, in het verleden ook wel aangeduid met het begrip TPM (Third Party Mededelingen). Een nog af en toe gebruikte naam, die lijkt te refereren aan een standaard-assurance-product. Echter, een dergelijk standaard-assurance-product bestaat niet. De term is in de praktijk ontstaan en betreft op verschillende wijze ingevulde en vormgegeven standaard 3000-assurance-rapporten.

Als genoemd bevat standaard 3000 alleen de randvoorwaarden voor de opdrachtdefinitie, de uitvoering en rapportage. Afhankelijk van de vraagstelling door de opdrachtgever en de invulling door de auditor kan het rapport veel verschijningsvormen hebben. Ik zie dat de markt hiermee worstelt. De markt zoekt een eenduidig product, waar met een relatief simpele vraagstelling duidelijk is wat wordt bedoeld. Accountants zijn zowel leverancier als gebruiker van assurance-rapporten. Deze laatste rol doet zich voor in situaties waar de accountant bij de uitvoering van de werkzaamheden in het kader van jaarrekeningcontrole geconfronteerd wordt met voor de controle belangrijke processen die door uitbesteding buiten de directe invloedssfeer van de gecontroleerde organisatie liggen. In plaats van zijn werkzaamheden uit te breiden tot de serviceorganisatie kan de accountant ook een door een collega opgesteld assurance-rapport opvragen. Om er zeker van te zijn dat het gevraagde assurance-rapport bruikbaar is, is een specifieke invulling van standaard 3000 ontwikkeld, de standaard 3402: Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie. De oorsprong van deze standaard was het Amerikaanse SAS 70-rapport. SAS 70 werd internationaal bekend in het kielzog van de Amerikaanse Sarbanes Oxley-wetge-

ving. Waarvan, door internationale verwevenheid, de werking niet beperkt bleef tot Amerika. De voorspelbaarheid van de reikwijdte en het formaat van het SAS 70-rapport leidde er toe dat, ook bij uitbestedingen in omgevingen zonder raakvlakken met de Sarbanes Oxley-wetgeving, om SAS 70-assurance-rapporten werd gevraagd. Gelijktijdig met de publicatie van standaard ISAE 3402 is in Amerika SAS 70 vervangen door de AT 801-standaard. AT 801 is geheel in lijn met ISAE 3402 en daarmee de oorsprong van de oude SAS 70. In Amerika is de wijziging geannonceerd onder SSEA[2] 16, een aanduiding die nog af en toe wordt gebruikt. Echter, het Amerikaanse instituut van accountants (AICPA) heeft het rapport de merknaam SOC[3] 1 gegeven.
Voor wie het spoor bijster is kort samengevat:
SSEA 16, AT 801 en SOC 1 zijn verschillende aanduidingen voor hetzelfde rapport en het is een implementatie van ISAE 3402; gelijkend Nederland waar NBA-standaard 3402/NOREA-richtlijn 3402 implementaties van ISAE 3402 zijn.

Het standaard 3402-assurance-rapport is bedoeld voor het gebruik door accountants van organisaties waarbij processen die van invloed zijn op de financiële verslaglegging zijn uitbesteed. Deze randvoorwaarde genoemd in artikel 3 van de standaard betekent dat de aanduiding 3402 aangeeft dat het rapport betrekking heeft op financiële, of daaraan ondersteunende, processen en dat de reikwijdte beperkt is tot het kwaliteitscriterium betrouwbaarheid. Het rapport is ontworpen voor gebruik door de accountant van de uitbestedende organisatie. De duidelijke vastlegging van het formaat van een standaard 3402-rapport spreekt ook bestuurders en hun toezichthouders aan. Het gebruik van de standaard 3402-rapporten door andere betrokkenen knelt niet met de standaard zolang het rapport betrekking heeft op processen die een (indirecte) invloed hebben op de betrouwbaarheid van de financiële verantwoording. Voorbeelden van rapporten die vaak van meer betekenis zijn voor de bestuurders van uitbestedende organisatie en hun toezichthouders zijn rapporten met betrekking tot uitbesteed vermogensbeheer, de uitvoering van de pensioenadministratie voor een pensioenfonds, of een IT-serviceorganisatie die bijvoorbeeld het door de organisatie gebruikte SAP-systeem exploiteert.

Het 3402-assurance-rapport heeft betrekking op financieel gerelateerde processen, die overeenkomstig het laatste voorbeeld in de vorige alinea, al of niet (gedeeltelijk) digitaal kunnen zijn. Hierbij onderscheiden wij de applicatie met daarin de geprogrammeerde controles en de IT-infrastructuur waar de applicatie gebruik van maakt. De specifieke elementen met betrekking tot de IT-infrastructuur zijn ondersteunend aan de betrouwbaarheid van de functionaliteit van de geprogrammeerde controles en daarmee de uitbestede bedrijfsprocessen. De complexiteit en daarmee de verwarring slaat toe als uitsluitend het element van de digitale verwerking is uitbesteed en daarover een 3402-assurance-rapport wordt opgesteld. Oppervlakkig gezien lijkt dit een assurance-rapport met betrekking tot uitbestede digitale verwerking in volle breedte. Zowel met betrekking tot de scope als de gehanteerde kwaliteitsaspecten, denk hierbij naast betrouwbaarheid ook aan beschikbaarheid en vertrouwelijkheid. Echter, op basis van de gehanteerde standaard betreft de reikwijdte uitsluitend het kwaliteitsaspect betrouwbaarheid van de omgeving die betrekking heeft op de digitale verwerking van applicaties die een raakvlak hebben met de financiële verslaglegging. Omdat dit impliciet is aan de gevolgde standaard wordt de scope-afbakening en de beperking in de reikwijdte over het algemeen niet in het rapport genoemd.

Als de 3402-standaard consequent is toegepast, hetgeen van een professionele auditor mag worden verwacht, gaat het assurance-rapport over de IT-infrastructuur niet verder dan de general IT-controls[4] met betrekking tot de applicaties in scope. De beoordeling van de general IT-controls heeft betrekking op de betrouwbare werking van de application controls voor zover deze betrekking hebben op de processen die mogelijk van invloed zijn op de financiële verslaglegging van de gebruiker. Dit geldt ook indien alleen de IT-infrastructuur in scope is, ook wel aangeduid met de “computer bureau approach”. Als de uitbesteding alleen betrekking heeft op de IT-operations begint de scope op basis van Standaard 3402 te wringen! Gebruikers, anders dan accountants die het assurance-rapport gebruiken bij hun op financiële verantwoording gerichte controle, verwachten een bredere scope (ook niet-financiële processen) en een bredere reikwijdte (naast betrouwbaarheid ook beschikbaarheid en vertrouwelijkheid).

Een assurance-rapport op basis van standaard 3402 heeft betrekking op uitbestede processen die mogelijk van invloed zijn op beweringen in de financiële verslaglegging van de uitbestedende organisatie. Deze processen kunnen geautomatiseerd zijn en voor hun betrouwbaarheid afhankelijk zijn van general IT-controls in de digitale verwerkingsomgeving. Het komt voor dat de general IT-controls met betrekking tot deze digitale verweking in een afzonderlijk rapport zijn opgenomen. Bijvoorbeeld in situaties waar de serviceorganisatie de digitale ver-

werking heeft uitbesteed aan een computerservicebureau (IT-housing). Dit IT-gerelateerde rapport kan onder standaard 3402 worden uitgebracht, wat in de 3402-praktijk wordt aangeduid met computerservicebureau-approach. Echter, de hiervoor beschreven impliciete scope-beperkingen van een standaard 3402-rapport zijn voor een buitenstaander maar ook voor een professional die niet dagelijks met assurance-rapporten te maken heeft onbegrijpelijk en een bron van misverstanden.

3 Assurance-rapporten met betrekking tot IT-processen

Het formuleren van oordelen over IT is in Nederland in 1982 voor het eerst vormgeven in NIVRA-geschrift 26, Automatisering en controle deel IV; Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking. Als al eerder genoemd, in de volksmond bekend onder een TPM[5]-rapport. In de kern gericht op betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Vertrouwelijkheid / privacy waren nog geen topic. Het internet bestond nog niet in de vorm zoals we het nu kennen waardoor het aantal externe koppelingen eenvoudig te overzien en te beheersen was. Het NIVRA-geschrift had in de bijlage een aanzet voor een normkader in zich; deze was echter door de technische ontwikkeling snel achterhaald. Echter, het idee achter de mededeling door de accountant met betrekking tot de geautomatiseerde gegevensverwerking heeft in de praktijk vorm gekregen in assurance-rapporten onder standaard 3000. Het probleem in de praktijk was het gebrek aan standaardisatie. Bij wijze van spreken hanteerde iedere auditor zijn eigen normenset en rapportagevorm. Buiten Nederland werd het rapport niet herkend en daardoor slecht bruikbaar voor internationaal opererende organisaties.

Standaardisatie met betrekking tot beheersingsinformatieverwerking heeft ook vorm gekregen in de code van informatiebeveiliging, die thans vastligt in de ISO/NEN-norm 27002:2013. Deze norm is breed en dekt alle thans actuele aspecten van informatiebeveiliging. In aansluiting op ISO 27002 is een certificering ontwikkeld, bekend onder ISO 27001. Certificering moet van kaders uitgaan om het implementeerbaar te maken. Voor de ISO 27001 certificering is dit het Information Security Management Systeem (ISMS), dat zorg moet dragen voor de implementatie en werking van de relevante informatiebeveiligingsmaatregelen (ISO 27002 of een verglijkbare normenset). Hier ligt de eerste bron van misverstand; de certificering geeft een oordeel over de implementatie van het ISMS en zegt niets over het realiseren van de beheersingsdoestelling middels de werking van de beheersingsmaatregelen. Als de door de ISO-auditor uitgevoerde beoordelingswerkzaamheden worden afgezet tegen de werkwijze van onder de IFAC-standaarden werkende auditors, kan de uitkomst van de werkzaamheden van de ISO-auditor niet verder reiken dan opzet en bestaan van het ISMS overeenkomstig ISO 27001. Een onmiskenbaar positief element van ISO 27001-certificering is de uniformiteit en de relatieve laagdrempeligheid. Naar mijn mening zou elke organisatie die serieus met IT omgaat op informatiebeveiliging gerichte managementprocessen geïmplementeerd moeten hebben. Het is een vorm van digitale bedrijfshygiëne. Met een ISO 27001-certificaat kan dit eenvoudig aantoonbaar worden gemaakt. Het kunnen overleggen van een ISO 27001-certificaat mag worden verwacht bij iedere IT-serviceprovider. Maar let op, vanwege de begrenzing tot het ISMS en de door ISO-auditor uitgevoerde beperkte beoordeling is het niet toereikend om er op te kunnen vertrouwen dat de beheersingsdoelstellingen doorlopend (in werking) zijn gerealiseerd. Hiermee is het niet geschikt om aan te tonen dat de informatieverwerking heeft voldaan aan de in ISO 27002 gestelde beveiligingsdoestellingen.

ISACA is een Amerikaanse beroepsorganisatie voor IT-governance, IT-security en IT-auditors met chapters over de gehele wereld. Naast de publicatie van ondersteunend materiaal als bijvoorbeeld COBIT voor IT-governance, kunnen professionals certificaten verkrijgen op basis van een afgelegd examen en overlegde praktijkervaring. De bekendste certificeringen zijn CISA (IT-audit) en CISM (IT-security management). Deze certificering heeft betrekking op de beroepsuitoefenaar en niet op de door hem of haar volgens de beroepsstandaarden opgestelde rapportages zoals bij ISO en IFAC. Het betreft deskundigheid ten aanzien van de beheersing van de digitale omgeving. ISACA biedt geen universele assurance-producten / -diensten.

Het pluspunt van het ISO 27001-certificaat is de uniformiteit en verwijzing naar ISO 27002 als concrete set van te realiseren informatiebeveiligingsdoelstellingen; het nadeel is de beperkte diepgang. Het voordeel van standaard 3000 assurance-rapporten is de diepgang van de review en de flexibiliteit waardoor het precies passend op de assurance-behoefte kan worden gemaakt; het nadeel is de beperkte voorspelbaarheid van vorm en inhoud en het risico van de mogelijke misinterpretatie door het niet juist interpreteren van de inhoud van het assurance-rapport. Als beschreven in het slot van

de vorige paragraaf is standaard 3402 naar de aard van de standaard ongeschikt voor assurance-rapporten die specifiek gericht zijn op de beheersing van de IT-infrastructuur in brede zin; het sterke punt van standaard 3402 is de gestandaardiseerde opbouw van het rapport. Op zich hoeven de beperkingen in de toepassing van standaard 3402 geen echte beperkingen te zijn. In het slot van artikel 3 van standaard 3402 staat vermeld dat als de scope anders is alle aanwijzingen uit standaard 3402 gevolgd kunnen worden voor het uitbrengen van een rapportage onder de algemene assurance-standaard 3000. Dit kan zo ook gesteld worden omdat, welbeschouwd, standaard 3402 een nadere invulling is van standaard 3000. De vorm van een assurance-rapportage onder standaard 3402 en een gestandaardiseerde op de IT-infrastructuur gerichte normenset leidt tot een herkenbaar en goed te benoemen assurance-rapport.

Het Amerikaans instituut van accountants (AICPA) heeft dit herkend. De al eerder ontwikkelde "trustservices principles and criteria" en een rapportformaat gelijk aan standaard 3402 (in de VS geïmplementeerd onder de merknaam SOC 1) zijn samengebracht en uitgewerkt in een guidance om tot een op de IT-infrastructuur gericht assurance-rapport te komen. In aansluiting op de naam van SOC 1 heeft dit assurance-rapport de merknaam SOC 2 gekregen. Een SOC 2-rapport kan betrekking hebben op de principles security, availability, processing integrity, confidentiality en privacy. Zowel naar opzet, bestaan (type 1) als naar opzet, bestaan en werking (type 2). Waarbij security de basis is en de andere principles een toevoeging naar keuze zijn. Qua vorm lijkt het rapport op het ons bekende standaard 3402-assurance-rapport waarbij de beheersingsdoelstellingen (bij standaard 3402 bepaald door de serviceorganisatie) vervangen zijn door de beheersingsdoelstellingen (criteria) die bij de betreffende trust services principles horen. De verspreidingskring en het toegestaan gebruik is, gelijk standaard 3402, gereguleerd tot de gebruikers van de betreffende IT-infrastructuur. De trust services criteria en principles kunnen betrekking hebben op: security, optioneel gecombineerd met availability, processing integrity, confidentiality en privacy. Met betrekking tot privacy principles wordt gebruik gemaakt van de Amerikaanse generally accepted privacy principles. Deze laatste zijn niet bruikbaar voor reviews die betrekking hebben op de Europese markt en zullen voor Europees gebruik moeten worden heroverwogen.

Naast SOC 2- is er ook een SOC 3-rapportage ontwikkeld. De review-werkzaamheden die aan een SOC 3-rapportage ten grondslag liggen zijn gelijk aan die van een SOC 2-review. De rapportage is beperkter, er zijn geen opgelegde beperkingen in het gebruik en de verspreiding van de rapportage[6].

De vraag naar SOC 2-rapportages komt in eerste instantie over naar Nederland vanuit serviceorganisaties die voor Amerikaanse bedrijven werken. Ook zien wij in Nederland de rapporten beschikbaar komen vanuit Amerikaanse serviceorganisaties die SOC 2-rapporten beschikbaar stellen aan hun klanten. Gelijk als bij de popularisering van de SAS 70-rapportage is de tendens dat de SOC 2-rapportage ook gebruikt wordt bij uitbestedingsrelaties die geen raakvlakken hebben met de VS.

De SOC 2-rapportage is gebaseerd op de algemene Amerikaanse attestation-standaard AT 101. (Amerikaanse standaarden gebruiken de term "attestation" waar ISAE spreekt van "assurance"). De door de AICPA uitgegeven professional standard AT 101 (Attest Engagements) is naar zijn aard gelijk aan standaard 3000. Ook veronderstelt het volgen van de AICPA SOC 2 guidance dat in volle breedte door de auditor gewerkt is onder de AICPA code of professional conduct en de Amerikaanse auditing standards (GAAS). Om SOC 2-rapportage onder de in Nederland gebruikte standaarden te positioneren, werkt op het moment van de publicatie van dit artikelNOREA in samenwerking met NBA aan een handreiking over de vorm waarin de Nederlandse beroepspraktijk een, aan een SOC 2 gelijkwaardige rapportage, onder standaard 3000 uit kan brengen.

Als eerder opgemerkt wordt de beperkte toepasbaarheid van standaard 3402 niet begrepen en worden in de praktijk de beperkingen genegeerd. Hetgeen bij de gebruikers van het rapport tot verwarring leidt en tot discussies onder professionals. In een omgeving waar regels zwaar wegen en het toezicht streng is, zal de accountant bij twijfel aan de formele juistheid van het standaard 3402-rapport al snel besluiten wel kennis te nemen van het rapport maar er niet op te steunen. Hetgeen overeenkomstig de audit-standaarden (in Nederland standaard 402) tot extra audit-werkzaamheden of in de zwaarste situatie tot beperkingen in accountantsverklaringen kan leiden.

De SOC 2-guideline biedt duidelijkheid over het rapport lay-out en de te hanteren normen met betrekking tot beheersing van uitbestede IT-infrastructuur. Met de beschikbaarheid van deze guideline is het niet meer nodig om rapporten met betrekking tot de serviceverlening in een digitale omgeving, geforceerd onder standaard 3402 te brengen. Zoals dit

vaak eerder gebeurde door het gebrek aan gestandaardiseerde alternatieven.

SOC 2 betreft alleen digitale verwerking, dit komt door de directe relatie met de IT-gerichte "trust services principles and criteria". Het vormt geen oplossing voor andere terreinen waar, bij gebrek aan een alternatief, standaard 3402 wordt toegepast voor assurance over processen waar het mogelijke verband ontbreekt met de financiële verslaglegging van de uitbestedende organisatie. Hoe bijvoorbeeld om te gaan met door een pensioenfonds aan een pensioenuitvoerder uitbestede processen met betrekking tot de bestuursondersteuning of bijvoorbeeld de uitbesteding van de postverzending aan een extern mailing house? Dit is belangrijk voor het management van de uitbestedende organisatie maar de uitgangspunten van een standaard 3402-rapport of een SOC 2-rapport bieden hiervoor geen ruimte. Als eerder aangehaald staat in artikel 3 van standaard 3402 dat indien de scope niet past, het in standaard 3402 uitgewerkte rapportageformaat gebruikt kan worden onder standaard 3000. Voor auditors duidelijke taal, maar voor buitenstaanders niet herkenbaar. Van de afnemers van assurance-diensten mag niet worden verwacht dat zij in hun assurance-vraag refereren aan details in de standaard. Ik zie het als een communicatieprobleem, vaktechnisch is het geen issue. Een uitdagende job voor de beroepsorganisaties om naast het nu ontwikkelde SOC 2-rapport met betrekking tot IT-serviceorganisaties te komen tot voor de markt herkenbare / benoembare assurance-producten. Ik zou er een lans voor willen breken om handreikingen te ontwikkelen voor direct toepasbare assurance-rapport-formaten, met een aanduiding die aansluit met de situatie waar het rapport voor is ontwikkeld. Ter illustratie en ideevorming: assurance-rapport inzake softwarepakketten, assurance-rapport inzake bedrijfsprocessen. Vaktechnisch gericht op de auditor, maar veel belangrijker vooral een duidelijke uiteenzetting voor de gebruikers van assurance-producten zowel gericht op de service- / product-verantwoordelijke entiteit als op de gebruiker. Geen nieuwe standaard maar een invulling van standaard 3000 voor concrete situaties.

4 Hoe bruikbaar is nu een assurance-rapport voor de praktijk?

Vanuit de audit-professie wordt veel effort gestoken in de ontwikkeling en marketing van assurance-rapporten. Wat we zien is dat de oplossing voor beheersing van uitbestede processen wordt gezocht vanuit de toolbox van de auditor. Dit is naar mijn mening te eenzijdig. Immers als je alleen een hamer hebt lijkt alles op een spijker. Assurance voegt waarde toe aan het uitbestede proces maar staat los van dit proces. Het komt niet vanuit het gereviewde proces maar is meta-informatie over het proces. Voor relatieve buitenstaanders als bestuurders, toezichthouders en accountants is dit effectief omdat kennisname van de assurance-rapporten de gezochte informatie over beheersing van het uitbestede proces geeft. Ook kunnen assurance-rapporten aan derden worden overlegd om te verantwoorden hoe toezicht is uitgeoefend respectievelijk de controle is uitgevoerd. Dit geeft bestuurders en accountants een comfortabel gevoel, ook al hebben zij maar beperkt op de inhoud van de rapporten gesteund. Voor de beheersing van het proces zelf is het van beperkte waarde. Natuurlijk, om goed door de review heen te komen moeten de beheersingsmaatregelen op orde zijn. Ter ondersteuning van de dagelijkse operatie komt het assurance-rapport te laat, waardoor het direct treffen van correctieve maatregelen niet mogelijk is.

Is een organisatie nu echt in control over haar uitbestedingen als zij assurance-rapporten kan overleggen? Bedoeld wordt met nadruk actief in control. Naast het functioneren van beheersingsmaatregelen gaat het erom dat afwijkingen van het normale patroon niet alleen zijn herkend, maar dat hier situatie-afhankelijk adequaat op is gereageerd. Het gaat om de uitkomst van het proces, niet om de beheersingsmaatregelen. Er zijn situaties waar voor de effectieve reactie de gebruiker direct moet worden ingeschakeld om schade van ongewenste situaties in te dammen. Denk aan data leakage; een serviceorganisatie is niet in staat vast te stellen in hoeverre het om privacygevoelige informatie gaat. Hier is directe interactie met de uitbestedende organisatie vereist. Alleen de constatering dat de preventieve beheersingsmaatregel niet heeft gewerkt en een repressieve beheersingsmaatregel het lek heeft gesignaleerd is voor de operatie ontoereikend. De interactie met de gebruiker moet tot een tijdige correctieve actie hebben geleid. Dit gaat over de grenzen van het assurance-rapport heen.

In de praktijk zijn situaties bekend waar er door de organisaties grote fouten in de uitvoering is gemaakt, die tot schade hebben geleid. De preventieve beheersingsmaatregelen (die qua diepgang optimaal waren geïmplementeerd gegeven de aard van het proces en de economisch verantwoorde uitvoeringsinspanning) hebben de fout niet kunnen voorkomen. De repressieve controles hebben de fout gedetecteerd, de opvolging is adequaat geweest en de schade is verantwoord. Een procesgericht assurance-rapport zal tot de conclusie komen dat het controlesysteem adequaat heeft gefunctio-

neerd. De uitbestedende organisatie wordt achteraf geconfronteerd met een "schoon" assurance-rapport en een forse schade in de uitvoering. Leg dat maar eens uit.

Een assurance-rapportage, maar ook een certificaat (bijvoorbeeld ISO) heeft de beperking in zich dat het een verantwoording van toetsing in het verleden is en dat het afgrenzingen kent die anders of beperkter kunnen liggen dan het uitbestede proces. De afgrenzing is een element dat een actieve bijdrage van een assurance-rapportage voor de beheersing beperkt. Assurance-rapporten en certificaten geven inzicht binnen de kaders van de scope. Een open deur, echter de praktijk leert dat de gebruikers hier niet bij stilstaan. Een beperkte scope kan betekenen dat processen die van betekenis zijn niet in de scope zijn opgenomen. Of zoals bij ISO 27001 het accent op het Information Security Management Systeem (ISMS) ligt en niet op de informatiebeveiligingsmaatregelen. Een ruime scope betekent over het algemeen dat het gegeven inzicht van hoog abstractieniveau is. Bij assurance-rapporten met betrekking tot de grote cloud-serviceproviders lopen gebruikers hier tegenaan. Formeel is er zekerheid, maar praktisch heeft dit voor de proactieve beheersing weinig betekenis. De afnemers-leveranciersrelatie met de grote cloud-providers heeft de kenmerken van een consumentenrelatie. Bij het niet-aanvaarden van de condities kan de dienst niet worden afgenomen, er is geen onderhandelingsruimte. Als er in dergelijke situaties assurance-rapporten zijn, is de kans groot dat deze zo algemeen zijn dat het niet aansluit op de behoefte van de afnemer.

Concluderend kan worden gesteld dat assurance-rapporten ontoereikend zijn voor de operationele procesbeheersing. De kern hiervan ligt in het retrospectieve karakter van het rapport, niet aansluitende scope en diepgang en het geeft geen real time inzicht in de situaties die correctieve maatregelen behoeven.

5 Inpassing assurance-rapporten in relatie tot operationele beheersing

Als de voorgaande conclusie wordt doorgetrokken resulteert dit in de constatering dat een assurance-rapport van weinig toegevoegde waarde is voor het operationeel management; het is te laat, scope past niet, geeft geen informatie over de uitkomst van het proces. Voor de operationele beheersing van uitbestede processen is meer nodig dan een assurance-rapport.

De praktijk wijst uit dat functionarissen en verantwoordelijk operationeel management zich hun verantwoordelijkheden realiseren en naar beste kunnen maatregelen treffen om de uitbesteding te coördineren. De voor het operationeel management beschikbare middelen om de uitbesteding te beheersen zijn meestal een gegeven. De uitbesteding is gebaseerd op commerciële gronden en daarna juridisch uitgewerkt. Om het zwart-wit te stellen: de uitvoerders moeten het doen met de gemaakte afspraken. Dit is een terrein waar auditors van grote waarde kunnen zijn, niet door te hameren op assurance-rapporten maar door te adviseren hoe het operationeel beheersingssysteem van de uitbestedende organisatie en de serviceorganisatie meer één kunnen worden. Denk aan het integreren van incident en problem management, change procedures en performance monitoring. In de praktische uitwerking hiervan moet onderscheid worden gemaakt tussen enerzijds de serviceorganisaties die maatwerk voor hun klanten leveren en anderzijds public cloud providers waar de service min of meer een consumer good is. Deze laatste situatie zien we veel terug in het MKB dat gebruik maakt van boekhoudservices in de cloud.

Met serviceproviders die in staat zijn om maatwerk aan te bieden is het zaak dat de uitbestedende organisatie afspraken maakt over de informatie-uitwisseling ten behoeve van de procesbeheersing en gezamenlijk te investeren in portals voor informatie-uitwisseling. Directe informatie-uitwisseling over de uitkomsten van beheersingsmaatregelen maakt het de uitbestedende organisatie mogelijk direct te reageren op situaties die afwijken van het normale patroon. Investeren in informatie-uitwisseling heeft op operationeel niveau een veel grotere toegevoegde waarde dan het verder verfijnen van beheersingsprocedures, de vastlegging van de uitvoering van de beheersingsprocedures en het achteraf testen op de uitvoering van de beheersingsprocedures. De auditor kan hierbij in zijn adviserende rol van grote toegevoegde waarde zijn. Mijn ervaring leert dat de organisatie primair denkt aan het operationele proces en zich pas achteraf realiseert dat er ook nog functionaliteit en procedures met betrekking tot beheersing moeten worden ingericht.

Indien sprake is van IT-service met karakter van een consumer good (ook wel aangeduid met pubic cloud-services) dan is het zaak om op zoek te gaan naar de middelen die al voorhanden zijn. Wat er beschikbaar is aan real time-inzicht is afhankelijk van de aard van de clouddienst. Bij infrastructuurdiensten (bijvoorbeeld een web server/data base server) is dit andere beheersingsinformatie dan bij het afnemen van applicatieservices, als een online boekhoudprogramma. U zult verbaasd zijn wat u allemaal kunt regelen en monitoren als u gebruik maakt van Amazon Elastic Compute Cloud (Amazon EC2). Met als enig echt onderscheid dat de server niet

onder het eigen bureau staat, maar op afstand en dat de interface via een browser loopt. Betreft het een cloud-oplossing op het niveau van applicatieservices dan is er een scala aan beheersingsinformatie beschikbaar op functioneel niveau. Denk hierbij aan de uitkomsten van in de applicatie opgenomen controls maar ook aan het inzicht in verleende autorisaties en incidenten. Informatie die niet technisch is, maar door een ieder die operationeel te maken heeft met het uitbestede proces kan worden geïnterpreteerd.

Assurance-rapporten die bruikbaar zijn voor het operationeel management zouden zich kunnen beperken tot opzet en bestaan van procedures bij de serviceorganisatie gericht op de beheersingsmaatregelen die ten grondslag liggen aan het leveren van beheersingsinformatie. Waarbij gewaarborgde afspraken zijn gemaakt dat het rapport ververst wordt bij significante wijziging in opzet en/of implementatie (bestaan). Assurance over de werking is niet nodig. De organisatie die uitbesteedt, is namelijk zelf in staat op real time-basis de werking vast te stellen. De vaststelling zou de organisatie overigens ook weer kunnen uitbesteden; gekscherend wordt dit dan assurance as a service (AAAS) genoemd.

Twee risico's blijven bestaan, maar die worden eigenlijk ook niet door assurance-rapporten afgedekt. Dat is het risico van de vendor-lock-in en de door juridische gronden optredende discontinuïteit van de serviceprovider (denk aan faillissement of beslaglegging). Het eerste, de vendor-lock-in, betreft de verbondenheid met de serviceprovider. De in de loop van de tijd opgebouwde bestanden met (historische) informatie en het gebruik van specifieke datastructuren belemmeren een snelle en niet al te kostbare overgang naar een andere serviceprovider. Bij een discontinuïteit van de provider door financiële problemen zullen alle technisch getroffen continuïteitsmaatregelen onder de regie van de serviceprovider door zijn bankroet niet langer beschikbaar zijn. De gevolgen van een discontinuïteit van de provider kunnen zich door de aanwezige vendor-lock-in verergeren. Voor het goede begrip: overdraagbaarheid (portabililty) en continuïteit vallen buiten de scope van een standaard 3402-assurance-rapportage en een ISO 27001-certificaat. Het leveren van een assurance-product voegt niets toe. Hier is vooral de auditor als adviseur van belangrijke toegevoegde waarde voor de uitbestedende organisatie. Om deze risico's te vermijden is er eigenlijk maar één oplossing die voldoende zekerheid geeft: het opslaan van de cruciale informatie in een omgeving buiten de economische invloed van de serviceprovider in een universele, niet applicatiegebonden, datastructuur.

6 Samenvatting en conclusie

Het is te kort door de bocht om na de beschouwingen in de paragrafen 4 en 5 over situaties waar assurance-rapporten minder goed passen te concluderen dat assurance-rapporten geen waarde hebben. Wat ik in de laatste paragrafen van dit artikel aan heb willen geven is dat assurance-rapporten geen panacee zijn voor alle assurance-behoeften. Het is een stukje van de puzzel en wel het sluitstuk. Assurance-rapporten, in het bijzonder op basis van standaard 3000 / 3402, zijn van toegevoegde waarde in situaties waar bestuurders en toezichthouders op afstand staan en niet in staat zijn middels eigen waarnemingen zich ervan te overtuigen dat de processen binnen de organisatie in control zijn. Het assurance-rapport is een sluitstuk waarmee de uitvoering van beheersingsmaatregelen wordt bevestigd door een auditor. Als instrument van governance is het één van de repressieve maatregelen gericht op de werking van de beheersingsmaatregelen binnen uitbestede processen. Waarbij een standaard 3402-assurance-rapport zich richt op de financiële aspecten, is een SOC 2-rapport gericht op beveiligingsmaatregelen binnen de IT-infrastructuur en geeft een ISO 27001-certificaat enige zekerheid of aan de basisuitgangspunten met betrekking tot IT-informatiebeveiligingsmanagement is voldaan. Al met al is het een aardig palet aan mogelijke assurance-rapporten met betrekking tot IT-uitbesteding. Een zorgvuldige afstemming met de gebruiker blijft van belang om er zeker van te zijn dat wordt gekozen voor de meest doeltreffende assurance-vorm. Hierbij mag niet uit het oog worden verloren dat de meest effectieve investering ligt in afspraken met de uitbestedende organisatie over de informatie-uitwisseling ten behoeve van de procesbeheersing. De uitwerking ligt in het ontwikkelen van portals voor de informatie-uitwisseling. De betrouwbaarheid van deze portals is cruciaal en kan inzichtelijk worden gemaakt middels reviews gericht op opzet en bestaan van de op betrouwbaarheid gerichte maatregelen. Bij de beoordeling van de opzet is een belangrijk element de toereikendheid van de informatie waarmee de gebruiker de betrouwbare werking van de portal kan vaststellen. ■

J.C. (Han) Boer RA RE CISM (www.linkedin.com/in/han-boer), adviseert en ondersteunt als zelfstandig professional ondernemingen en accountants bij vraagstukken met betrekking tot (IT) assurance. Han is als freelance docent verbonden aan de IT audit opleiding aan de Universiteit van Amsterdam en de Vrije Universiteit. Hij is actief betrokken bij NOREA, de beroepsorganisatie van IT-Auditors.

Noten

1 NOREA, beroepsorganisatie van de IT auditors RE, heeft de standaard overgenomen onder de aanduiding Richtlijn 3000.
2 Statement on Standards for Attestation Engagements (SSAE).
3 Service Organisation Control (SOC)-report.
4 Access management, change management en processing.
5 Third Party (accountants) Mededeling.
6 Wie verdergaand geïnteresseerd is in deze rapportages vindt meer informatie in Boer en Van Beek (2013).

Literatuur

- AICPA (American Institute of Certified Public Accountants) (2015). *Reporting on controls at a service organisation relevant to security, availability, processing integrity, confidentiality, or privacy (SOC 2®)*. Geraadpleegd op http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/IndustryspecificGuidance/PRDOVR~PC-0128210/PC-0128210.jsp (1 oktober 2015).
- AICPA (American Institute of Certified Public Accountants) (2014). *Trust services principles, criteria and illustrations*. Geraadpleegd op http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCGuidesandPublications.aspx. (1 oktober 2015).
- Boer, J.C., & Beek, J.J. van (2013). Nieuwe ontwikkelingen IT-gerelateerde Service Organisation Control-rapportages, SOC 2 en SOC 3. *Compact* (2013) 13/2. Geraadpleegd op http://www.compact.nl/artikelen/C-2013-2-Boer.htm?zoom_highlight=boer+beek. (1 oktober 2015).
- IAASB (International Auditing and Assurance Standards Board). ISAE 3000: Assurance Engagements Other than Audits or Reviews of Historical Financial Information. Geraadpleegd op http://www.ifac.org/system/files/downloads/b012-2010-iaasb-handbook-isae-3000.pdf. (1 oktober 2015).
- IAASB (International Auditing and Assurance Standards Board) (2005). International framework for assurance engagements. IAASB Handbook. Geraadpleegd op http://www.ifac.org/system/files/downloads/b003-2010-iaasb-handbook-framework.pdf. (1 oktober 2015).
- ISACA (Information Systems Audit and Control Association) (2012), SOC 2 User Guide. Geraadpleegd op ISACA member portal 1 oktober 2015 www.isaca.org.
- KPMG (september 2014). Praktijkgids 5 Assurancerapporten voor IT-serviceorganisaties SOC 2. Geraadpleegd op http://www.kpmg.com/nl/nl/issuesandinsights/articlespublications/pages/praktijkgids-5.aspx. (1 oktober 2015).
- NBA (Nederlandse Beroepsorganisatie van Accountants) (2015), Handreiking Regelgeving Accountancy (HRA), NV COS 3000 en NV COS 3402. Geraadpleegd op http://www.nba.nl/wet-en-regelgeving/beroepsregels/hra (1 oktober 2015).
- NEN (Nederlands Normalisatie-instituut)(2013). NEN-ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – requirements. Geraadpleegd op http://www.iso.org/iso/catalogue_detail?csnumber=54534 (1 oktober 2015).
- NIVRA (Nederlands Instituut van Registeraccountants) (1982). Automatisering en controle, Deel IV Mededelingen door de accountant met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Deventer, Kluwer.
- NOREA (Nederlandse Organisatie voor Register EDP Auditor) (2014). Audit Alert NOREA: misvattingen publiciteit en scope 3402 assurance-rapporten. 12 november 2014. Geraadpleegd op http://www.norea.nl/Norea/Actueel/Nieuws/Audit+alert+3402.aspx. (1 oktober 2015).