Welke vorm past het best?

Rapportages voor derden

17 december 2019

Han Boer

Het is niet altijd voor iedereen duidelijk wat en hoe een IT-auditor naar derde partijen moet rapporteren. Dat is niet alleen voor buitenstaanders een lastig punt, maar ook voor relatief onervaren auditors. De auditor mag niet in conflict komen met de regels en de daarop gebaseerde verwachtingen van de professionele buitenwereld. Een rapport en de onderliggende werkzaamheden voor derden moeten aan regels voldoen: de IT-auditor kan niet naar eigen goeddunken te werk gaan. Het begint met de keuze van de juiste richtlijn en daarbinnen de keuze van de juiste vorm van rapportage. Het doel van het rapport moet bepalend zijn voor de te volgen regels. Maar hier gaat het vaak fout. Waar ligt dit aan? Onbegrip of onbegrijpelijke regels? In elk geval leert de praktijk dat opdrachtgevers nogal eens vragen naar assurancerapporten die niet passen, respectievelijk dat de voorstelling die zij van het assurancerapport hebben anders is dan de geformuleerde vraag.

In dit artikel analyseer ik hoe wij als IT-auditors voor onszelf, en vooral ook voor de markt duidelijkheid kunnen scheppen. Voorwaarde om dat te kunnen doen, is natuurlijk dat we zelf goed in het hoofd hebben welke standaard voor welke situatie geschikt is. Daarom besteed ik hier uitgebreid aandacht aan. Verder pleit ik voor extra duidelijkheid door een onderscheidende benaming te gebruiken voor assurancerapporten over de beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening door IT-serviceorganisaties. De van ouds bekende '*Third Party* Mededeling' (TPM) vind ik daar een prima label voor.

Beoogde gebruiker

Allesbepalend voor de opzet van de rapportage over de uitgevoerde werkzaamheden is het beoogde gebruik. Bij het aanvaarden van de opdracht moet de IT-auditor zich verdiepen in het doel dat de opdrachtgever voor ogen heeft. Deze activiteit vormt een logische basis voor professionele dienstverlening in het algemeen. Dit is dan ook een vereiste, vastgelegd in de *NOREA Richtlijn 210 Opdrachtaanvaarding*. De IT-auditor moet hierbij niet alleen afgaan op de informatie die de opdrachtgever verstrekt, maar zich ook afvragen of het rapport een rationeel doel dient. Of, zoals in het *Reglement Gedragscode Register IT-Auditors* is verwoord, 'De IT-auditor evalueert omstandigheden of relaties waarmee hij

bekend is of in redelijkheid bekend behoort te zijn, die de naleving van de fundamentele beginselen in gevaar kan brengen'. In de praktijk zullen vooral het deskundigheids- en zorgvuldigheidsbeginsel in het geding zijn. De evaluatie moet voorkomen dat de IT-auditor in een later stadium in een lastige discussie terechtkomt over het gebruik van het rapport. Bijvoorbeeld doordat de uitgevoerde werkzaamheden die aan het rapport ten grondslag liggen niet aansluiten bij het gebruik van het rapport, of doordat het rapport op gespannen voet staat met de regelgeving.

> *"Richtlijn 3000-rapportage met uitsluitend oordelen per norm vraagt om misverstanden"*

Voor rapportages opgesteld door de IT-auditor onderscheid ik in dit artikel twee hoofdcategorieën, gebaseerd op het beoogde gebruik van het rapport. Ten eerste rapportages die uitsluitend bedoeld zijn voor gebruik *binnen* de organisatie zelf. Ten tweede rapportages die gericht zijn op gebruik *buiten* de organisatie waar deze betrekking op hebben – voor derden dus.

Rapportage voor gebruik binnen de organisatie zelf

De aanduiding voor rapportages die alleen worden gebruikt *binnen* de organisatie waar het rapport betrekking op heeft, is 'adviesrapport'. NOREA heeft hiervoor geen aanvullende specifieke richtlijnen uitgebracht. Voor deze opdrachten zijn dus alleen de algemene richtlijnen en reglementen van NOREA van kracht. De belangrijkste eisen komen voort uit de fundamentele beginselen uit het *Reglement Gedragscode Register IT-Auditors*. Vormfouten kunnen zich eigenlijk niet voordoen, zolang de IT-auditor maar weet te waarborgen dat het adviesrapport alleen binnen de organisatie wordt gebruikt en het rapport geen kenmerken vertoont van een assurancerapport, zie het *Stramien voor Assurance-opdrachten* van NOREA.

In dit artikel laat ik het bij deze opmerkingen, voor wat de eerste hoofdcategorie betreft, de rapportage voor de organisatie zelf. Wie meer houvast zoekt, kan het in 2012 uitgebrachte NOREA-studierapport *Adviesdiensten* erop na slaan.
Dit artikel gaat verder over de tweede hoofdcategorie, de rapportage voor derden.

Rapportage voor derden

De keuze van de juiste NOREA-richtlijn en de correcte toepassing van de richtlijn wordt een punt van attentie als het rapport bestemd is voor derden die geen verantwoordelijkheid dragen voor het onderwerp waar het rapport betrekking op heeft. Uitgaande van het Stramien voor Assurance-opdrachten krijgt dit rapport al snel het karakter van een assurancerapportage volgens de regels van Richtlijn 3000 of 3402. Dit komt door de brede werking van dat stramien. Hierbij geldt nog wel een 'tenzij'. Het is mogelijk dat alle betrokken partijen (auditee, gebruiker en auditor) expliciet afspreken dat zij het

rapport niet als assurancerapport kwalificeren. Voorbeelden hiervan zijn overeengekomen specifieke werkzaamheden (Richtlijn 4401), *due diligence*-rapporten en adviesrapporten waarbij de derde partij expliciet verklaart te begrijpen dat geen zekerheid aan het rapport kan worden ontleend.

Alvorens in te gaan op de te kiezen richtlijn, wil ik eerst stilstaan bij het beoogde gebruik van een rapport. Wie zijn de gebruikers? Is het er één of zijn het meerdere gebruikers? Zijn het bekende gebruikers of betreft het een rapport voor het algemeen maatschappelijk verkeer (het 'open verkeer')? Voor welk doel wordt het rapport gebruikt? Deze informatie over het beoogd gebruik is nodig voor verantwoorde afwegingen bij de invulling van de opdrachtbevestiging, de werkuitvoering en de rapportage. De kenmerken van de beoogde gebruikersgroep bepaalt de te gebruiken richtlijn, maar ook hoe binnen de grenzen van een richtlijn om te gaan met specifieke eisen vanuit de opdrachtgever.
Voor assurance en assurance-gerelateerde opdrachten gelden drie mogelijke NOREA-richtlijnen: 4401, 3402 en 3000 (deze laatste met twee varianten: A en D), zie de volgende paragrafen.

Richtlijn 4401

Redenerend vanuit het beoogd gebruik van de rapportage lijkt het eenvoudig als de gebruiker van het rapport niet om een oordeel vraagt, maar om het vaststellen van feitelijke bevindingen. Het meest geëigend hiervoor is *Richtlijn 4401 Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie*.
Zowel de verantwoordelijke voor het object van onderzoek als de gebruiker van het rapport bevestigen vooraf de reikwijdte en de beperkingen in het gebruik van de rapportage. De auditor voert de specifieke werkzaamheden uit en rapporteert de feitelijke bevindingen, maar geeft geen oordeel. Toepassing van deze richtlijn is per definitie alleen mogelijk als de gebruiker vooraf bekend is. Die is immers een van de betrokken partijen bij afspraken vooraf over het gebruik van de rapportage. Over het algemeen zal het om één specifieke gebruiker gaan. Omdat het rapport gebaseerd is op specifieke afspraken tussen alle betrokken partijen, kan het rapport alleen door deze partijen worden gebruikt.

Richtlijn 4401 valt niet onder de werking van het *Stramien voor Assurance-opdrachten*.
De auditors weten precies wat dit betekent: zij geven geen assurance en richten hun werkzaamheden dan ook niet op assurance. De IT-auditor voert enkel de afgesproken werkzaamheden uit. De implicaties hiervan zijn echter niet voor iedereen vanzelfsprekend. Van de niet als auditor geschoolde gebruiker van de rapportage valt niet te verwachten dat hij deze nuance kent en doorziet hoe een rapport van feitelijke bevindingen verschilt van een assurancerapport. Deze categorie gebruikers ziet een RE automatisch als een professional die oordelen afgeeft. Om te voorkomen dat het 4401-rapport ten onrechte als assurancerapport wordt gezien, zal de IT-auditor in extra zorgvuldige bewoordingen moeten rapporteren. Dit zal niet altijd toereikend zijn om te voorkomen dat een gebruiker het rapport als een assurancerapport interpreteert. Uit hoofde van risicomanagement zal

de IT-auditor de Richtlijn 4401 daarom alleen toepassen als de gebruiker van het rapport een professionele gebruiker is en er geen aanwijzingen zijn dat het rapport op een later moment mogelijk anders zal worden gebruikt dan bedoeld. In alle andere situaties zal de IT-auditor het zekere voor het onzekere nemen en kiezen voor het verstrekken van een assurance-rapport, om het risico van onbedoelde assurance in de kiem smoren.

Maar hiermee is het risico nog niet bezworen: er is nog een mogelijke oorzaak waardoor gebruikers de betekenis van een assurance-rapport volgens Richtlijn 4401 verkeerd kan begrijpen. Ook het geven van oordelen over onderdelen in plaats van het geven van een oordeel over het geheel kan namelijk leiden tot misinterpretatie. Bij de behandeling over de toepassing van de assurance-richtlijn 3000 ga ik hier verder op in.

Richtlijn 3402

Als de beoogd gebruiker van de rapportage de accountant is die het rapport nodig heeft voor het verkrijgen van inzicht en zekerheid over uitbestede processen, dan is Richtlijn 3402 de best passende richtlijn. Althans, hiervoor is deze richtlijn bedoeld. Artikel 3 van de richtlijn is wat ingewikkeld geformuleerd maar laat geen misverstand bestaan over de reikwijdte van de richtlijn. Die betreft de interne beheersingsmaatregelen van een serviceorganisatie die waarschijnlijk relevant zijn voor de interne beheersing van de gebruikersorganisaties in relatie tot de financiële verslaggeving.[1]

> *“IT-auditor, ken de beoogde gebruikers van je rapport”*

In de praktijk blijkt de vraag lang niet altijd van de accountant te komen. Door de populariteit wordt ISAE 3402[2] als algemene naam voor een assurance-rapport gebruikt, zonder oog te hebben voor de specifieke inhoud van de richtlijn. Als de serviceprovider hierin meegaat, vraagt de serviceprovider een rapport dat gezien de inhoud van de richtlijn onmogelijk is. Ook NOREA wijst hierop in haar audit alert[3]: ‘Misvatting publiciteit en scope 3402 assurance-rapporten’. Als u hier als IT-auditor tegenaan loopt, is de vraag hoe dit op te lossen. De opdrachtgever wil of kan niet altijd terug naar de gebruiker(s) van het rapport om tot een aanpassing van de vraag te komen. Naar mijn opvatting is de flexibiliteit die de auditor kan tonen afhankelijk van wie de gebruikers zijn. Om een afweging te maken onderscheid ik drie categorieën:

1. Een brede groep al dan niet bekende gebruikers.
2. Eén specifieke gebruiker.
3. Een groep bekende gebruikers.

Brede groep al dan niet bekende gebruikers. In dit geval wordt de vorm van de rapportage over het algemeen bepaald door de opdrachtgever. Denk bijvoorbeeld aan een leverancier van een SAAS-boekhoudapplicatie. De opdrachtgever heeft de regie volledig in handen en

kan eventueel in overleg met zijn auditor tot de juiste richtlijn komen. Hier speelt het issue van een opgedrongen richtlijn dus niet.

Eén specifieke gebruiker. Bij rapportages die een relatie met de financiële verslaggeving hebben is Richtlijn 3402 de aangewezen richtlijn; die is daar immers voor bedoeld. Is die relatie er niet, dan moet de IT-auditor in beschouwing nemen in welke mate de reikwijdte van het rapport afwijkt van het uitgangspunt van de richtlijn. Als de IT-auditor de reikwijdte van het gevraagde rapport afzet tegen de bedoeling van Richtlijn 3402, moet de IT-Auditor niet alleen de processen in scope maar ook de gevraagde kwaliteitsaspecten in de afweging meenemen. Een Richtlijn 3402-rapport is beperkt tot de kwaliteitsaspecten, gericht op het beheersen van betrouwbaarheidsrisico's (juistheid, volledigheid en tijdigheid). Een uitbreiding van de reikwijdte betreft meestal het meenemen van de kwaliteitsaspecten beschikbaarheid en vertrouwelijkheid.

Omvat de reikwijdte ook alle processen die relevant zijn voor de financiële verslaglegging van de gebruiker, dan kan de IT-auditor naar mijn mening coulant zijn. De IT-auditor kan dan meegaan in de vraag wanneer zowel de gebruiker als de serviceprovider aan de auditor bevestigen dat zij begrijpen dat voor de verkeerde richtlijn is gekozen. Dit, omdat het voor de gebruiker waarschijnlijk niet van belang is. Richtlijn 3402 is een nadere uitwerking van Richtlijn 3000 A. Ook al sluit de reikwijdte niet aan bij artikel 3 van Richtlijn 3402, het blijft een volwaardig assurance-rapport. De IT-auditor moet er zorg voor dragen dat de referentie naar de verkeerde richtlijn duidelijk uit het rapport blijkt. Dit kan een onderdeel van het oordeel zijn of expliciet zijn opgenomen in het rapport.

Bij het verkeerd toepassen van de Richtlijn 3402 in de situatie dat sprake is van een groep bekende gebruikers (de derde onderscheidde gebruikerscategorie) betekent dat de IT-auditor zal moeten afwegen in hoeverre deze groep de kennis heeft om het issue te begrijpen. De uitkomst van de afweging bepaalt zijn gedragslijn. De afweging bestaat uit twee elementen:

1. De professionaliteit van de gebruiker.
2. De mate waarin wordt afgeweken van de reikwijdte als bedoeld in de Richtlijn 3402 (aard van de processen en beoordeelde kwaliteitsaspecten).

Concludeert de IT-auditor dat de gebruikers geen audit-professionals zijn, of beoordeelt de IT-auditor de afwijking in de processen en kwaliteitsaspecten ten opzichte van de reikwijdte van de richtlijn als groot, dan zal de auditor minder coulant zijn over de afwijking van de richtlijn.

Richtlijn 3000

De minste knelpunten ten aanzien van de gebruikersgroep zijn er bij het uitbrengen van een assurance-rapport onder Richtlijn 3000. Belangrijk is dat de auditor hier vaststelt dat het rapport een rationeel doel dient, zie Richtlijn 3000 A/3000 D paragraaf 24, lid (vi),

en niet leidt tot misinterpretatie. Dus ook hier geldt weer: IT-auditor ken uw gebruikers. Richtlijn 3000 bevat in paragraaf 69 aanwijzingen om te bepalen welke onderwerpen de rapportage ten minste moet bevatten. De vorm van de rapportage is vrij, waarbij onder voorwaarden ook mogelijkheden zijn voor *short form*-rapportages, zie Richtlijn 3000 A en 3000 D, paragraaf A 160. Het mag misschien lijken dat deze vrijheden de toepassing van richtlijn 3000 makkelijk maken, maar de praktijk is anders. Gebruikers van assurance-rapporten willen geen verrassingen over de vorm van het assurance-rapport, maar willen herkenbaarheid. Dat is juist een van de redenen waarom gevraagd wordt om een Richtlijn 3402/ISAE 3402-rapportage. De herkenbaarheid van de rapportage komt voort uit een artikel in Richtlijn 3402, waar concreet in vastligt welke items in het rapport moeten worden opgenomen. Dit is in de richtlijn aangeduid met rapportagecriteria (Richtlijn 3402, paragraaf 15 t/m 18).

De vrijheid binnen richtlijn 3000 heeft ook grenzen. In situaties waarin het rapport bestemd is voor bekende professionele gebruikers, is een rapportagevorm ontstaan die volgens mij afwijkt van de bedoeling van Richtlijn 3000. Ik doel hiermee op het afgeven van een oordeel per norm in plaats van een oordeel over het gehele object van onderzoek, inclusief een oordeel over de toereikendheid van de gehanteerde norm. De toepassing van deze rapportagevorm kan bij minder professionele partijen aanleiding geven tot misinterpretatie. Als de individueel te beoordelen normen zijn opgesteld door de gebruikende partij, zal het een rationeel doel dienen en ligt misinterpretatie niet voor de hand. Maar als de gebruikende partij niet bij de normvaststelling betrokken is, wordt het voor de IT-auditor lastig om vast te stellen of het rapport een rationeel doel dient (Richtlijn 3000 A/3000 D, artikel 24). Het gebruik van het rapport met slechts een oordeel per norm is gevoeliger voor misinterpretatie, omdat de gebruiker zelf moet vaststellen of de gehanteerde normen toereikend zijn.

Sterker nog, vanuit een onethisch motief gezien geeft deze vorm van rapportage de opsteller van het rapport zelfs de mogelijkheid tot bewuste manipulatie van de volledigheid van de normenset. Normen met betrekking tot elementen die de auditee niet gerapporteerd wil zien, zou de auditor kunnen weggelaten. Ook hier geldt weer dat wanneer de auditor meegaat met de wens om per norm een oordeel af te geven, de auditor de beoogde gebruiker moet kennen. De auditor moet vaststellen dat de gebruiker de normenset heeft geaccordeerd en bovendien professioneel genoeg is om de beperkingen van het assurance-rapport te begrijpen. Goed beschouwd is het een niet gedocumenteerde tussenvorm van de rapportages onder de Richtlijnen 3000 en 4401. Vanuit deze laatste richtlijn gezien, wordt in plaats van een auditbevinding een oordeel per overeengekomen norm gegeven, al dan niet op basis van een verantwoording door de auditee (richtlijn 3000 A of 3000 D). Door het ontbreken van richtlijnen komen we hier in een grijs gebied.

Bij de recente herziening van Richtlijn 3000 zijn twee varianten[4] onderscheiden, te weten 'Attest' (3000 A) en 'Direct' (3000 D). In de praktijk zie ik dat deze nieuwe opzet van de

richtlijn goed heeft uitgepakt. De auditor moet analyseren hoe de verantwoordelijkheden voor de rapportage liggen, resulterend in keuzes over de structuur van het rapport en de formulering van het oordeel. Door deze duidelijke vastlegging in de richtlijn zie ik een bewuste keuze ontstaan: de attestvorm, waarbij de auditee ook zelf verantwoording aflegt op basis van de gehanteerde normen, wint duidelijk terrein. De vermelding[5] vanuit het management in een assurance-rapport in de attestvariant geeft duidelijk de verantwoordelijkheid van de auditee weer. Overigens, dit is de voorgeschreven rapportagevorm onder Richtlijn 3402, de standaard die de gebruikers al dan niet terecht hebben omarmd.

SOC 1 en SOC 2

In de VS hanteren auditors andere standaarden dan in Nederland. Een van die standaarden komt overeen met onze ISAE 3402/Richtlijn 3402. 'Dat is de standaard, tevens merknaam SOC 1.'[6] Ook hier werd geworsteld met het gebruik van deze aanduiding in situaties waar die standaard niet voor was bedoeld. Omdat de meeste rapporten die ten onrechte werden aangeduid als SOC 1 betrekking hebben op uitbestede IT-processen, is hiervoor onder de merknaam SOC 2 een rapport-format op de markt gezet. Qua vorm lijkt dat format op SOC 1 maar inhoudelijk heeft het betrekking op IT-omgevingen zonder dat er verband wordt gelegd met beheersingsmaatregelen die relevant zijn voor de financiële verslaglegging. SOC 2 is gebaseerd op guidance van het Amerikaanse accountsinstituut[7]. Voor de lezers die meer willen weten over de wijze waarop Nederlandse IT-auditors tegemoet kunnen komen aan de klantvraag voor een SOC 2–rapport, verwijs ik naar de hiervoor door NOREA uitgegeven handreiking[8].

Het roer moet om

ISAE 3402/Richtlijn 3402 heeft van alle assurance-rapporten de grootste naamsbekendheid. Dit betekent dat voor vele niet-auditors ISAE 3402 een bekende aanduiding is voor een assurance-rapport. ISAE 3402/Richtlijn 3402 is heel bruikbaar, maar kan niet altijd worden toegepast. Wanneer dat niet kan, is Richtlijn 3000 een prima alternatief. Alleen heeft Richtlijn 3000 geen duidelijk herkenbare merknaam. Deze richtlijn is ook niet te definiëren met één begrip. De flexibiliteit van de richtlijn leidt tot veel verschillende invullingen.

> *"Gebruik bij onbekende gebruikers de criteria van Richtlijn 3402 onder toepassing van Richtlijn 3000 A"*

De oplossing voor een brede assurance-vraag die niet kan worden afgedekt met gebruik van Richtlijn 3402 ligt voor de hand: hanteer voor assurance-rapporten voor een brede kring (onbekende) gebruikers met betrekking tot de beschikbaarheids-, integriteits- en

vertrouwelijkheidswaarborgen bij serviceorganisaties een rapport in de vorm van Richtlijn 3402 met toepassing van Richtlijn 3000 A. Een idee dat overigens ook is opgenomen in Richtlijn 3402. Richtlijn 3402 doet in de paragrafen 3 en A2 namelijk een suggestie voor situaties waarin de reikwijdte afwijkt van de vereisten die worden gesteld aan de toepassing van Richtlijn 3402. In die gevallen kunnen de vormvoorschriften uit Richtlijn 3402 worden gebruikt als kader voor de toepassing van richtlijn 3000 A.

Hoe krijgen we de markt zover om hiernaar te vragen? Ik denk dat dit alleen maar kan door deze rapportvorm met een onderscheidende naam op de markt te brengen. Die moet weinig introductie nodig hebben, omdat de markt nu eenmaal denkt termen van producten met duidelijk herkenbare productnamen. Dit is te zien bij de populaire ISAE 3402 / Richtlijn 3402 rapportages. Het heeft lang geduurd voordat de naam van de voorganger van Richtlijn 3402, SAS70, uit het dagelijkse spraakgebruik verdween. Ter illustratie, tegenwoordig zien we door de hang naar een eenvoudige productaanduiding, dat Richtlijn 3402 assurance-rapportages vaak worden aangeduid met de merknaam van de Amerikaanse ISAE 3402 / Richtlijn 3402 equivalent:
SOC 1.

TPM

Nederland kent een hardnekkig gebruik om een assurance-rapport aan te duiden met TPM (Third Party Mededeling). Wat hiermee wordt bedoeld kan van persoon tot persoon verschillen. Het begrip TPM is namelijk nergens gedefinieerd. Het komt oorspronkelijk voort uit studierapport 26 uit 1982 van het NIVRA[9] (nu NBA) over de teksten van verklaringen op basis van onderzoeken van ICT-omgevingen (toen 'EDP' genoemd: *Electronic Data Processing*). Het studierapport introduceert onder meer de *third party review*, waarbij de third party de accountant of IT-auditor is, die als derde onafhankelijke partij zijn oordeel geeft.

Sinds 1982 is er veel veranderd. Het merendeel van de assurance-rapporten heeft de vorm van een attestrapport. Meestal gebeurt dit in de vorm van assurance over een in het rapport opgenomen management bewering, die onder Richtlijn 3402 wordt aangeduid als 'vermelding van het management'.

Populair zijn assurance-rapporten over processen die zijn uitbesteed aan serviceorganisaties. Vanuit de gebruiker bezien is de serviceprovider de eerste die gezien wordt als een derde partij. De auditor bevestigt de bewering van de serviceorganisatie, door daar een oordeel aan toe te voegen. Door de opkomst van de attestrapportages klopt het oude spraakgebruik niet meer: het is niet langer de auditor die het inzicht geeft. De serviceorganisatie rapporteert als derde partij aan de gebruiker over de wijze waarop de processen worden geborgd op afgesproken kwaliteitsaspecten als beschikbaarheid, integriteit en vertrouwelijkheid. De beheersing van de kwaliteitsaspecten binnen de reikwijdte van het rapport wordt met het oordeel van de auditor bevestigd (Richtlijn 3000

A). Tijd dus, om ook in de definitie de rollen te wisselen en de serviceorganisatie als third party aan te duiden.

Third Party Mededeling door de serviceorganisatie

Ik wil ervoor pleiten als onderscheidende productnaam de aanduiding TPM te gaan gebruiken in overeenstemming met hoe deze aanduiding (nog steeds) in de praktijk wordt gebruikt. Een assurancerapport gebaseerd op Richtlijn 3000 A zoals als voorgeschreven in Richtlijn 3402 krijgt hiermee een naam waarmee de gebruiker met één kernachtige en herkenbare term kan aanduiden wat hij nodig heeft. De naam is er al en wordt in het dagelijkse spraakgebruik gehanteerd voor de groep assurancerapporten waar nu nog geen vastgestelde naam voor is. Het enige wat wij als IT-auditors concreet moeten afspreken is waar deze naam precies voor staat. Hiermee lossen wij twee problemen op. Ten eerste krijgen we een duidelijke naam voor assurancerapporten die geen relatie hebben met de financiële verslaglegging. Ten tweede krijgt de tot nu toe achteloos gebruikte term TPM een duidelijke definitie.

Net als bij de bestaande Richtlijn 3000, is het te kiezen *control framework* (de norm) in principe vrij. Voor verdere standaardisering is mijn advies: koppel het TPM-rapport in eerste instantie aan het NOREA/PviB studierapport Algemene beheersing van IT-diensten. Om de rapportagevorm breed toepasbaar te houden, mag deze koppeling niet hard zijn. Afhankelijk van de situatie moet de opsteller van het rapport ook kunnen kiezen voor een specifieke, beter passende normenset.

Samenvatting

Het artikel gaat uit van de door gebruikers en opdrachtgevers komende vraag naar assurancerapportages. Een vaak gesignaleerd probleem is dat de geformuleerde vraag niet aansluit op de verwachting van de gebruikers en bij de randvoorwaarden voor de assurance-richtlijnen 3000 en 3402. Hierop kan de IT-auditberoepsgroep op drie manieren reageren:

1. De gebruikers en opdrachtgevers beter voorlichten.
2. De rapportage erop aanpassen.
3. De producten aanpassen aan de vraag.

De eerste reactie, de markt onderrichten over wat auditors hebben bedacht, is een weg die de afgelopen jaren is gevolgd.
De tweede reactie bestaat eruit de rapportage langs de randen van wat mogelijk is aan te passen. Een voorbeeld is dat de IT-auditor in zijn rapportage opneemt op welke onderdelen de richtlijn niet goed zijn toegepast. De IT-auditor moet zich er altijd van overtuigen dat de partij(en) de assurance-rapportage begrijpen en er geen aanleiding is voor enige misinterpretatie.

De derde reactie, het aanpassen van het product, heeft mijn voorkeur. Laten we het roer omgooien en kiezen voor deze optie. Of beter gezegd, laten we tot een eenvoudige aanduiding komen waarbij eenieder eenzelfde product voor ogen heeft dat past binnen de NOREA assurance-richtlijnen. De kracht is dat we dan een aanduiding gebruiken die bekend klinkt: TPM (Third Party Mededeling). Een term die al wordt gebruikt om de vraag naar een assurancerapporten te duiden. De aanduiding TPM is tot nu toe niet gedefinieerd. Dit is opgelost als wij, als IT-audit professionals, vanaf nu de term TPM definiëren als een assurancerapport voor een brede kring (onbekende) gebruikers over de beschikbaarheids-, integriteits- en vertrouwelijkheidswaarborgen bij serviceorganisaties volgens de criteria van Richtlijn 3402 onder toepassing van Richtlijn 3000 A. Ideaal zou het zijn als NOREA deze definitie bekrachtigt.

Literatuur

NOREA Richtlijnen

NOREA Handreikingen

NOREA/PviB studierapport Algemene beheersing van IT-diensten

KPMG praktijkgids assurancerapport 3000, april 2019

Noten

1 Richtlijn 3402 artikel 3: Deze Richtlijn is alleen van toepassing wanneer de serviceorganisatie verantwoordelijk is voor, of anderszins in staat is om een vermelding te doen over de geschikte opzet van interne beheersingsmaatregelen. In deze Richtlijn worden niet de assurance-opdrachten behandeld:
(a) om uitsluitend te rapporteren over de vraag of interne beheersingsmaatregelen van een serviceorganisatie zo werken als staat beschreven; of
(b) om te rapporteren over interne beheersingsmaatregelen van een serviceorganisatie anders dan die beheersmaatregelen die verband houden met een dienst die waarschijnlijk relevant is voor de interne beheersing van de gebruikersorganisaties in relatie tot de financiële verslaggeving (bijvoorbeeld, interne beheersingsmaatregelen die de productie of kwaliteitsbeheersing van de gebruikersorganisaties beïnvloeden).

2 ISAE 3402 is uitgeven door IFAC IAASB ze vormen de bron voor NBA Standaard 3402 (onderdeel van de NV COS) en NOREA Richtlijn 3402. Materieel gezien zijn er geen verschillen en kunnen de aanduidingen ISAE, standaard en richtlijn door elkaar worden gebuikt. Dit artikel gebruikt de NOREA aanduiding Richtlijn 3402.

3 https://www.norea.nl/nieuws/3174/audit-alert-norea-misvatting-publiciteit-en-scope-3402

4 Bij een attestopdracht baseert de IT-auditor zich op een bewering door de verantwoordelijke partij (de auditee) of iemand anders steunend op een door deze partij uitgevoerde evaluatie;
bij een directe opdracht baseert de IT-auditor zich niet op een bewering en is tevens de evalueerder.
Zie bijlage 1 NOREA Richtlijn 3000: Assurance-opdrachten (Attest en Direct Reporting)

5 De vermelding vanuit het management is de in Richtlijn 3402 voorgeschreven vormgeving van de uitkomst van de door het management (de verantwoordelijke partij) uitgevoerde evaluatie.

[6] SOC 1® en SOC 2® zijn in de Verenigde Staten door de AICPA geregistreerde handelsmerken.

[7] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html / https://www.aicpastore.com/SOC/soc-2-sup–reg—sup–reporting-on-an-examination-/PRDOVR~PC-0128210/PC-0128210.jsp.

[8] Guidance to Richtlijn (ISAE) 3000 Service Organization Control Reports for IT Service Organizations Based on the AICPA SOC 2® report model and the Trust Services Principles and Criteria.

[9] Nivra geschrift 26 Automatisering en Controle, Deel IV Mededeling door de accountant met betrekking tot de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking, Kluwer februari 1982.

J.C. (Han) Boer RE CISM | zelfstandig werkend professional

Han Boer is zelfstandig professional die zich in het bijzonder richt op advisering bij de totstandkoming van assurancerapporten. Tevens is Han verbonden aan Executive Programme of Digital Auditing van de Amsterdam Business School (onderdeel van de UvA), waar hij het vak Professional Standards doceert.
LinkedIn: www.linkedin.com/in/hanboer