Column

# Ervaringen uitvoering assuranceopdrachten

16 juni 2020

René Ewals

**OK, we hebben allerlei richtlijnen en guidance, en daar staat heel veel in over de wijze waarop wij assuranceopdrachten behoren uit te voeren. Echter, niet alles staat in onze richtlijnen en guidance. Dit artikel gaat in op enkele vraagstukken die in de praktijk vaak lastig zijn gebleken en waarover in Richtlijn 3402-trainingen veel vragen worden gesteld.**

Sinds de invoering van Richtlijn 3402 in 2011 zien we dat IT-auditors steeds meer assuranceopdrachten uitvoeren. In deze periode is veel ervaring opgebouwd met de bijzonderheden van dit type opdrachten. Ze worden uitgevoerd in een samenleving die sterk aan verandering onderhevig is en waarbij het accountantsberoep vaak onderwerp van discussie is, wat weer heeft geleid tot aanvullende regelgeving. Binnen deze kaders behandelt dit artikel enkele specifieke elementen uit assuranceopdrachten, die vanuit de regelgeving niet altijd (geheel) zijn ingevuld, en onderwerpen waarover in trainingen veel vragen worden gesteld.

## Inleiding Assurancestandaarden

Vanuit NOREA beschikken de IT-auditors over drie assurancestandaarden: de Richtlijnen 3000A, 3000D en 3402. Deze richtlijnen komen inhoudelijk geheel overeen met de gelijkluidende standaarden van de NBA. Daarnaast onderkent NOREA nog specifieke opdrachten, aangeduid als 'DigiD', 'SOC2' en 'SOC3', die formeel binnen de Richtlijnen 3000D of 3000A vallen.
Vanuit IFAC is ISAE 3000 ontwikkeld. Deze internationale standaard maakt geen onderscheid tussen '*attest*-opdrachten' en '*direct reporting*-opdrachten'. De standaard is opgesteld als een attest-standaard (vandaar de 'A' bij onze Richtlijn 3000A) en hierin is specifiek opgenomen dat de inhoud van deze standaard als uitgangspunt kan dienen bij opdrachten die leiden tot direct reporting. Binnen NOREA en NBA was wél behoefte om een aanvullende richtlijn te ontwikkelen (3000D) specifiek gericht op de direct reporting-opdrachten, waaronder DigiD.

# Formulering van doelstellingen en maatregelen

Veel assurancerapporten vermelden beheersingsdoelstellingen plus de bijbehorende beheersingsmaatregelen die ervoor moeten zorgen dat de doelstellingen worden behaald. De richtlijnen zelf maken niet duidelijk aan welke eisen deze doelstellingen en maatregelen moeten voldoen. Ook andere regelgeving, binnen of buiten NOREA, bevatten geen duidelijke criteria. Wel zijn *sound practices* in gebruik. Deze sluiten aan bij de wijze van werken binnen de jaarrekeningcontrole. Bij de jaarrekeningcontrole wordt gebruik gemaakt van *assertions* zoals 'volledigheid van de opbrengsten' en 'juistheid van de kosten'.
Een assurancerapport op basis van Richtlijn 3402 wordt altijd gebruikt ten behoeve van de jaarrekeningcontrole. De gebruikte doelstellingen zouden dan ook zo goed mogelijk moeten aansluiten bij deze assertions.

## Doelstellingen

Voor de formulering van doelstellingen in het kader van een 3402-assurancerapport bestaan de volgende sound practice-eisen. Ze zijn:

- **Specifiek**: de doelstelling moet de lezer in staat stellen om precies te begrijpen wat de reikwijdte van de doelstelling is. Bijvoorbeeld een doelstelling als 'beheersingsmaatregelen bieden redelijke zekerheid dat de afdrachten inkomstenbelasting aan de belastingdienst tijdig, juist en volledig plaatsvinden' is voldoende specifiek, terwijl een formulering als 'beheersingsmaatregelen bieden redelijke zekerheid dat alle transacties met de belastingdienst goed zijn' te algemeen is omdat de omschrijving 'alle transacties' te vaag is.
- **Meetbaar**: kwantitatieve evaluatie moet mogelijk zijn. Dit betekent dat doelstellingen veelal worden verwoord met termen als:
  - volledigheid;
  - juistheid/nauwkeurigheid;
  - tijdigheid.
- **Haalbaar en auditable**: een doelstelling moet haalbaar zijn en de auditor moet in staat zijn voldoende bewijsmateriaal te verzamelen om te kunnen concluderen of de doelstelling is behaald.
  Bijvoorbeeld: de doelstelling 'klanten zijn tevreden' is alleen auditable als specifiek wordt benoemd wat 'tevreden' inhoudt. De service-auditor zal anders geen oordeel kunnen uitspreken over de vraag of de beheersdoelstelling is behaald.
- **Relevant en realistisch**: de doelstelling moet relevant zijn voor de lezer van het rapport en moet voor de auditee realistisch zijn.

Hoewel lang niet alle 3000-rapporten worden gebruikt in het kader van de controle voor de externe verslaggeving, is het wel verstandig om bovenstaande eisen aan doelstellingen (en de eisen aan maatregelen in de volgende paragraaf) te betrekken bij de formulering van de doelstellingen en maatregelen. Zeker als een 3000-rapport wordt gebruikt in het kader van de externe verslaggeving.

Hierboven is aangegeven dat doelstellingen specifiek moeten zijn. Bepaalde woorden kunnen dat echter aantasten. Enkele voorbeelden zijn de woorden 'toepasselijk' (*appropriate* in het Engels), toereikend en/of adequaat. Deze woorden hebben een ruime betekenis en zijn daarom vaak niet specifiek genoeg. Ook in Engelse standaarden komt dit terug. Bijvoorbeeld in de AAF 01/06 (Engelse versie van de ISAE 3000 voor de financiële sector) [AAF0106] staan voorgedefinieerde doelstellingen opgenomen om bij voorkeur te hanteren bij rapporten die onder deze standaard worden opgesteld. Enkele van deze doelstellingen gebruiken het woord 'appropriate'. Gezien de ruime betekenis van dit woord vinden wij dit minder tot niet geschikt voor assurancerapporten.

## Maatregelen

Ook voor de formulering van maatregelen bevatten de richtlijnen geen eisen. Als sound practice worden de volgende elementen veel gebruikt:

- **Wie** (voert de maatregelen uit); oftewel wie is de verantwoordelijke partij voor de risico-mitigerende activiteit?
- **Wanneer** (hoe vaak, frequentie) wordt de maatregel uitgevoerd (meer dan dagelijks, dagelijks, wekelijks, maandelijks, per kwartaal, jaarlijks)?
- **Wat**: een omschrijving van de inhoudelijke activiteit van de beheersingsmaatregel.
- **Waar(uit)**: wat is de bron van de maatregel (indien van toepassing).
- **Waarmee**: de hulpmiddelen (informatie) waarmee de beheersingsmaatregel wordt uitgevoerd.
- **Resultaat en vervolgactie**: een omschrijving van het resultaat van de actie en eventuele daaruit voortvloeiende acties. Hierbij wordt specifiek gedoeld op de vervolgstappen als de uitvoering van de controle niet positief is: wat is dan het vervolg?

Deze eisen maken het niet altijd eenvoudig om een goede beschrijving van beheersingsmaatregelen op te stellen. Ook is het niet altijd mogelijk om bij de formulering van iedere maatregel aan alle eisen te voldoen. Vooral bij geautomatiseerde maatregelen is dat lastig, omdat hier geen mensen bij zijn betrokken.

Bij de beoordeling van de opzet van de interne beheersing zoals weergegeven in de beschrijving door het management, zowel als de beoordeling van de doelstellingen en maatregelen zelf, is het wel verstandig om deze meetlat te gebruiken en eventuele tekortkomingen terug te leggen bij de opdrachtgever en aan te dringen op verbetering. Overigens, als de opdrachtgever geen aanpassingen wil doorvoeren heeft de auditor altijd de mogelijkheid om over de opzet van de beschrijving een beperking in de mededeling op te nemen of, alleen in zeer ernstige gevallen, de opdracht terug te geven.

# Gebruik subserviceorganisaties en leveranciersmanagement

De IAASB gaf bij de publicatie van de toen net nieuwe ISAE 3402 weinig toelichting over het gebruik van subserviceorganisaties.1 De belangrijkste overweging was dat het inherent moeilijk zou zijn om ook de subserviceorganisaties in de scope te betrekken, omdat de auditor van de serviceorganisatie niet vaak ook de auditor van de subserviceorganisatie is. Een andere overweging was de vereiste dat je ook een beschrijving van de beheersingsomgeving moet opnemen als je een subserviceorganisatie in de reikwijdte opneemt. Zeg maar sectie II van het rapport, dan wel sectie III als de vermelding van het management als sectie I wordt opgenomen in het rapport. Dat leidt dan al snel tot hele dikke en onleesbare rapporten. Bovendien moest ook een aparte bewering van het management van de subserviceorganisatie worden opgenomen in het rapport. Dit vraagt op zijn beurt om een aparte opdrachtbrief en een door het management van de subserviceorganisatie ondertekende representatiebrief, ook wel bevestigingsbrief of *letter of representation* genoemd. Dit betekent dus dat het management van de subserviceorganisatie volledig moet meewerken. Tot slot moet de auditor ook onafhankelijk zijn van de subserviceorganisatie.

Richtlijn 3402 is nu alweer zo'n acht jaar in gebruik en in de praktijk zien we in de dienstverleningsketen steeds vaker subserviceorganisaties opduiken. Maar het aantal rapporten dat zich ook tot deze subserviceorganisaties uitstrekt – de *inclusive*-rapporten – neemt nauwelijks toe. De ontvangers van assurancerapportages stellen dan ook steeds vaker vragen over subserviceorganisaties in de keten. Niet verwonderlijk, als de rapportage de subserviceorganisaties via de mededeling van de tekenende auditor expliciet uitsluit. Er zijn verschillende manieren om aan deze informatievraag tegemoet te komen. De belangrijkste zijn:

- 'leveranciersmanagement' als proces toevoegen;
- criteria op relevantie subserviceorganisaties toepassen (deze criteria komen verderop aan de orde);
- verwijzen naar een bestaand assurancerapport;
- een combinatie van een of meer van deze drie.

Hieronder worden bovenstaande elementen nader uitgewerkt.

## Leveranciersmanagement als proces toevoegen

Parallel aan de ontwikkeling van ISAE 3402 heeft ook de American Institute of Certified Public Accountants (AICPA) een nieuwe standaard ontwikkeld als opvolger voor de SAS70-standaard. De aankondiging daarvan vond plaats in de SSAE16 (SSAE: Statement on Standards for Attestation Engagements), en in april 2017 is in de SSAE18 de laatste wijziging aangekondigd van de Attestation Standards op dit gebied: AT-C

Section 100, *common concepts*, en AT-C Section 320, 'Reporting on an Examination of Controls at a Service Organization relevant to user entities' Internal Control over Financial Reporting'. Inhoudelijk is deze laatste standaard vrijwel gelijk aan de ISAE 3402. Wel zijn bij aankondiging in de SSAE18 enkele nieuwe elementen toegevoegd. Een daarvan is de verplichte toevoeging van het proces 'leveranciersmanagement' in het rapport, vanzelfsprekend alleen als er leveranciers zijn. Hiermee kan de serviceorganisatie laten zien hoe zij haar leveranciers 'beheerst'. Dit is een waardevolle toevoeging die de lezer relevante extra inzichten biedt, mits het rapport de juiste doelstellingen en maatregelen bevat, uiteraard. Een andere toevoeging is de eis dat het assurancerapport van de serviceorganisatie de aanvullende beheersingsmaatregelen bij die organisatie beschrijft.

In de Nederlandse praktijk zien we wel vaker het proces 'leveranciersmanagement' terug in het rapport, maar de aanvullende beheersingsmaatregelen zijn vaak nog niet beschreven. Voor alle duidelijkheid: dit laatste is onder de huidige Richtlijn 3402 niet verplicht, maar zou, in navolging van de aangepaste regelgeving AT-C Section 320, wel als sound practice omarmd moeten worden. Wel is in de definitie van het begrip 'uitsluitingsmethode' ('carve out') in de richtlijn opgenomen dat 'De beschrijving van de serviceorganisatie van haar systeem interne beheersingsmaatregelen van de serviceorganisatie [bevat] die de effectiviteit van de interne beheersingsmaatregelen van een subserviceorganisatie monitort, wat in kan houden dat de serviceorganisatie een assurancerapport betreffende de interne beheersingsmaatregelen van de subserviceorganisatie beoordeelt'. [NORE16a] Hiermee wordt al een indicatie gegeven dat ook de richtlijn al aandacht schenkt aan leveranciersmanagement.

## Criteria toepassen op relevantie subserviceorganisatie

De tweede mogelijkheid grijpt in feite terug op hoe de voorganger van ISAE 3402, de SAS70-standaard, de subserviceorganisaties behandelde. SAS70 bevatte criteria om te bepalen in welke mate de subserviceorganisatie relevant was voor het doel waarvoor het rapport werd gebruikt. Bij deze criteria werd gebruikgemaakt van de volgende elementen [AICP08]:

- Een risico-inschatting, waarbij specifiek wordt beoordeeld in welke mate de subserviceorganisatie 'significant' (van betekenis) is voor de diensten van de serviceorganisatie aan de gebruikersorganisatie.
- De term 'significant' slaat op functies die de subserviceorganisatie uitvoert die impact hebben op de informatiesystemen van de serviceorganisatie én op de assertions die gerelateerd zijn aan de externe verslaggeving van de gebruikersorganisatie.
- De impact van functies bij een subserviceorganisatie kan zijn: beperkt, gemiddeld en uitgebreid. Deze inschatting vereist professionele oordeelvorming. Aan de hand van de impact van de functies hebben we hieronder uitgewerkt wanneer sprake moet zijn van een 'inclusive' benadering van de subserviceorganisatie.

| Beoordeling impact functies subservice-organisatie | Effectiviteit van beheersingsmaatregelen bij de serviceorganisatie | | | |
|---|---|---|---|---|
| | Beheersings-maatregel dekt de relevante beheers-doelstelling af. | Een combinatie[2] van beheersings-maatregelen dekt de relevante beheers-doelstelling af. | Beheersingsmaat-regelen bij alleen de serviceorganisatie dekken de beheers-doelstelling **niet** af.[3] | Beheersingsmaat-regelen bij de serviceorganisatie dekken de beheersdoelstelling **niet** af. |
| **Beperkt** | Niet verplicht | Niet verplicht | Verplicht | Verplicht |
| **Gemiddeld** | Niet verplicht | Verplicht | Verplicht | Verplicht |
| **Uitgebreid** | Verplicht | Verplicht | Verplicht | Verplicht |

**Tabel 1:** Afweging wel of geen 'inclusive' benadering van de subserviceorganisatie

Door binnen de mogelijkheden van 3402 deze criteria toe te passen en dat in het rapport zichtbaar te maken, geven we de ontvangers van het assurancerapport duidelijkheid. De afwegingen worden dan in het rapport per subserviceorganisatie opgenomen, zodat voor de lezer duidelijk is welke inschatting de auditor heeft gedaan.

Deze criteria zijn nog geen oplossing wanneer de subserviceorganisatie zo relevant is dat deze zou moeten worden opgenomen in het assurancerapport, maar dit vanuit bepaalde overwegingen niet mogelijk is of niet is gebeurd. Daarvoor zouden we in Nederland de Richtlijn moeten aanpassen. Een mogelijke oplossing in de huidige situatie is dat de subserviceorganisatie haar eigen ISAE 3402 of SOC1-rapport opstelt en ter beschikking stelt aan de serviceorganisatie.

## Verwijzen naar een bestaand assurancerapport

In de praktijk wordt niet vaak verwezen naar een bestaand, relevant assurancerapport. De reden hiervoor is dat de tekenende auditor mogelijk ook verantwoordelijk wordt voor de inhoud van het rapport van, bijvoorbeeld, de subserviceorganisatie. Maar als we bedenken wat het doel van een 3402-rapport is, dan zou dat een aantrekkelijke mogelijkheid kunnen zijn. Dan wordt ondubbelzinnig duidelijk wie welke verantwoordelijkheid heeft. Wellicht zou NOREA de regelgeving in deze richting kunnen aanpassen. Daarbij zouden bijvoorbeeld de volgende beslissingscriteria kunnen horen die deels zijn ontleend aan ISA 402:

- Het assurancerapport is opgesteld volgens de Richtlijnen 3000 en/of 3402.
- Het assurancerapport heeft ten minste een reikwijdte die relevant is voor de dienstverlening van de serviceorganisatie.
- Het assurancerapport is een type II-rapport.
- De periode die is getoetst overlapt voor ten minste 75 procent de periode zoals die wordt getoetst bij de serviceorganisatie (voorstel van de auteur).
- Het assurancerapport is getekend door een RE of RA.
- Een getekende versie van het assurancerapport van de subserviceorganisatie is opgenomen in het dossier van de tekenende auditor van de serviceorganisatie.[34]
- Het assurancerapport van de serviceorganisatie beschrijft welke processen en doelstellingen zijn opgenomen in het assurancerapport van de subserviceorganisatie en maakt duidelijk of de auditor van de subserviceorganisatie uitzonderingen heeft vastgesteld.[45] Deze beschrijving moet onderdeel zijn van sectie II (de beheersorganisatie).

Hiermee zouden de gebruikers van het assurancerapport van de serviceorganisatie betere risico-inschattingen kunnen maken voor hun eigen werkzaamheden.[6]

### Een combinatie…

In de voorgaande paragrafen zijn 'oude' methodes besproken en nieuwe mogelijkheden waarin de regelgeving (nog) niet voorziet. Elk van de drie gepresenteerde 'oplossingen' heeft zijn eigen beperkingen, waardoor nog niet duidelijk is wat dé oplossing voor alle subserviceorganisaties zou zijn. Maar het voorafgaande kan wellicht wel helpen om tot een oplossing te komen voor dit *wicked* probleem[7], dat steeds dringender wordt.

## Impact van een afwijking

Elke audit levert afwijkingen op die een maatregel minder effectief maken. Een aantal van deze afwijkingen leiden tot een of meer opmerkingen in het rapport, en sommige afwijkingen leiden tot een beperking in de mededeling. Dit hangt af van de impact van de uitzondering op het mogelijk behalen van de doelstelling van de maatregel, maar uit de regelgeving blijkt niet altijd hoe je die impact bepaalt. Er zijn in principe twee mogelijkheden: de afwijkingen die betrekking op de effectiviteit van een maatregel vermindert, hebben geen of wél impact op het mogelijk behalen van de doelstelling.

Laten we beide mogelijkheden verder bespreken aan de hand van het proces dat de auditor moet doorlopen bij elke (potentiële) uitzondering:

1. De auditor vindt een afwijking ten opzichte van de verwachting. Vaak bestaat de afwijking eruit dat de auditor geen evidence heeft verkregen dat de maatregel is uitgevoerd.
2. Elke afwijking moet worden onderzocht om na te gaan of de gevonden afwijking representatief is voor de populatie, dan wel dat sprake is van een anomalie. Een anomalie is eenmalig en daarom niet representatief voor de populatie.

3. De auditor kan verschillende technieken inzetten om vast te stellen of de gevonden afwijking representatief is voor de populatie of niet. Bijvoorbeeld: de omvang van de deelwaarneming uitbreiden (zie paragraaf 'omvang deelwaarnemingen'), de achtergronden van de afwijking onderzoeken via gesprekken met hiervoor verantwoordelijke of anderszins relevante medewerkers, het management of de directie, of aanvullende documentatie opvragen en beoordelen. Aan de hand hiervan kan de auditor tot een conclusie komen over de effectiviteit van een maatregel.
4. Als een gevonden afwijking materieel is voor de effectiviteit van de maatregel, wordt dit opgenomen in sectie III, met vermelding hoeveel deelwaarnemingen (indien een deelwaarneming is genomen) de afwijking bevatten ten opzichte van het aantal uitgevoerde deelwaarnemingen (bijvoorbeeld: drie van de twintig).
5. Tot slot zal de auditor moeten beoordelen en documenteren of de gevonden materiële afwijking impact heeft op het behalen van de doelstelling. Als de impact zo groot is dat (een deel van) de doelstelling (mogelijk) niet wordt behaald, moet dit als een beperking in de mededeling worden opgenomen.

*Professional judgement* is vereist om te bepalen welke aanvullende werkzaamheden moeten worden verricht en voor het uiteindelijke oordeel of de afwijking wel of niet materieel is. Overleg met collega's hierover en bestudering van relevante documenten kan het professional judgement ondersteunen, maar uiteindelijk is het de IT-auditor zelf die een verantwoorde en onderbouwde beslissing moet nemen. Soms zullen anderen het niet eens zijn met een beslissing, en des te noodzakelijker is het daarom dat de auditor de beslissing goed kan onderbouwen.

Degenen die een assurancerapport gebruiken voor hun eigen assurancewerkzaamheden, bijvoorbeeld in het kader van de jaarrekeningcontrole, kunnen in de rapportage, met inbegrip van alle afwijkingen en hun onderbouwingen eventueel aanleiding vinden hun risico-inschatting en werkprogramma aan te passen.

**Beperking in mededeling? Of toch niet?**
Voorbeeld: een doelstelling bevat drie maatregelen. Bij elk van deze maatregelen is een afwijking aangetroffen. Vraag: wordt deze doelstelling nog wel behaald of mogelijk niet? Hoewel dit op het eerste gezicht een eenvoudig 'nee' oplevert, en dus een beperking in de mededeling, hoeft dat toch niet zo'n makkelijk antwoord, laat staan het juiste antwoord, te zijn. Aanvullende vragen die hierbij thuishoren zijn namelijk:

- Zijn de gevonden afwijkingen materieel?
- Wat heeft het aanvullende onderzoek opgeleverd?
- Kunnen de risico's die horen bij de doelstelling worden gemitigeerd door het aanvullende onderzoek? Kan bijvoorbeeld de gehele populatie worden onderzocht, zodat zekerheid bestaat of het risico zich heeft voorgedaan?
- Leiden de afwijkingen tot een beperking in de mededeling of niet, alle aanvullende informatie overziend?

# Omvang deelwaarnemingen

Een van de technieken om een (geautomatiseerde) beheersingsmaatregel te testen is een deelwaarneming op de populatie te gebruiken. Hoe groot de deelwaarneming moet zijn volgt echter niet uit de Richtlijnen, en daarom hebben de meeste auditkantoren hiervoor standaardtabellen ontwikkeld, waarvan de statistische onderbouwing niet altijd duidelijk is, of wellicht zelfs wankel. Deze tabellen verschillen per kantoor in geringe mate. Ook maakt een assurancerapport meestal niet duidelijk welke tabel is gebruikt, tenzij een afwijking is vastgesteld. Wanneer sprake is van een afwijking moet in elk geval de omvang van de deelwaarneming worden opgenomen. In het kader van transparantie zou altijd de gehanteerde tabel moeten worden opgenomen.8

Zodra je in trainingen IT-auditors en accountants vraagt waar de gehanteerde tabel op is gebaseerd en waarom de aantallen waarnemingen erin zijn zoals ze zijn, blijven de cursisten altijd erg stil. Vaak weten ze wel dat de aantallen deelwaarnemingen niet (altijd) statistisch zijn onderbouwd, maar niet hoe die aantallen zijn bepaald. Ook weten ze vaak niet dat beslissingen over het aantal deelwaarnemingen afhankelijk kunnen zijn van de risico-inschattingen bij de start van een assuranceopdracht en de vormgeving van de auditprogramma's. Tabel 2 geeft een overzicht van veel voorkomende 'standaard' deelwaarnemingen die auditorganisaties gebruiken:

| Frequentie van voorkomen | Aantallen deelwaarnemingen |
|---|---|
| **Jaarlijks** | 1 |
| **Kwartaal** | 1, 2 |
| **Maand** | 2, 3 |
| **Week** | 5, 7 |
| **Dagelijks** | 15, 25 |
| **Meermalen dagelijks** | 25, 30, 40 |
| **Geautomatiseerd** | 1 |

**Tabel 2:** Veel voorkomende 'standaard' deelwaarnemingen

Toch zijn deze aantallen wel te onderbouwen. Afhankelijk van de vereiste zekerheid bij een bepaald onderdeel is het aantal te trekken deelwaarnemingen te bepalen. Dit betekent echter wel dat per in te zetten techniek moet worden bepaald hoeveel zekerheid nodig is. Dit is beschreven in de 'Handleiding Nederlandse controlestandaarden bij de controles in het MKB deel 1 en deel 2' uit oktober 2012. [NBA12]

Een alternatief dat weinig wordt gebruikt, is een statistische steekproef. Hierbij moet ook specifiek worden bepaald met welke zekerheid moet worden gewerkt. Veel voorkomende maten van zekerheid zijn 90 procent of 95 procent. Aan de hand van de omvang van de populatie kan vervolgens eenvoudig worden berekend hoe groot de steekproef moet zijn. Een groot voordeel van deze techniek is dat bij afwijkingen duidelijk is hoe je die moet evalueren en inschatten. Er is immers een duidelijke norm met de daarbij horende maximale te accepteren afwijkingen.

# Tot slot

De besproken onderwerpen komen vaak aan de orde in trainingen en collegiale vaktechnische consultaties. Het lijkt erop dat de behoefte aan meer duidelijkheid groeit. Dit was dan ook de aanleiding om dit artikel te schrijven en daarmee aandacht te geven aan praktische oplossingen, soms zelfs verplichtingen. Op onderdelen lijkt het zelfs een wellicht wat onorthodoxe aanpak.
Dit artikel is niet bedoeld als stellig advies, maar als bijdrage aan vaktechnische discussies en om gezamenlijk te bezien of we met structurele oplossingen ons vakgebied verder kunnen brengen.

**Noten**

[1] Subserviceorganisatie: een serviceorganisatie die door een andere serviceorganisatie wordt gebruikt om sommige diensten uit te voeren die aan gebruikersorganisaties worden verleend, waarvan de diensten deel uitmaken van het voor de financiële verslaggeving relevante informatiesysteem van die gebruikersorganisaties.

[2] Dat wil zeggen een combinatie van maatregelen bij de serviceorganisatie en bij de subserviceorganisatie.

[3] Het verschil tussen de kolommen drie en vier betreft het volgende: in kolom drie wordt de doelstelling afgedekt door een combinatie van maatregelen bij de serviceorganisatie én de subserviceorganisatie. Als kolom vier van toepassing is, wordt de doelstelling alleen afgedekt door maatregelen bij de subserviceorganisatie.

[4] Daarmee geeft de auditor van de serviceorganisatie aan te hebben vastgesteld dat het rapport bestaat. Deze auditor is niet verantwoordelijk voor de inhoud van het rapport over de subserviceorganisatie.

[5] De verantwoordelijkheid van de serviceauditor is beperkt tot vaststellen dat de punten zijn opgenomen in het rapport en dat het rapport van de subserviceorganisatie is opgenomen in zijn dossier.

[6] De achtergrond van deze opmerking is dat het nog steeds geen standaardpraktijk van serviceorganisaties is om het gehele rapport ter beschikking stellen van de gebruikende entiteiten en externe auditors.

[7] Een wicked probleem is een probleem dat vaak diepgeworteld is en waarvoor niet een (eenvoudige) oplossing bestaat.

[8] Vanuit de theorie kan en mag de service auditor voor elke beheersingsmaatregel een andere deelwaarneming gebruiken: een die past bij de zekerheid die de auditor wil ontlenen aan de testwerkzaamheden. In de praktijk wordt echter een standaardtabel gebruikt.

**Literatuur**


[AAF0106] *Assurance reports on internal controls of service organisations made available to third parties.*

[EWAL10] Ewals, René, ISAE 3402, Een nieuw hoofdstuk voor de IT Auditor, de IT-Auditor, 2010, nr. 3. https://www.deitauditor.nl/wp-content/uploads/2014/09/isae-3402-….pdf, geraadpleegd op 27 november 2019.

[NBA12] NBA, *Handleiding Nederlandse controlestandaarden bij de controles in het MKB deel 1 en deel 2'*, oktober 2012.

[NORE16a] NOREA, *Richtlijn 3402*, 14 december2016. https://www.norea.nl/download/?id=474 (geraadpleegd op 27 november 2019).

[NORE16b] NOREA, *Richtlijn 3000A*, 14 december 2016. https://www.norea.nl/download/?id=5640, geraadpleegd op 27 november 2019.

[NORE16c] NOREA, *Richtlijn 3000D*, https://www.norea.nl/download/?id=5640, geraadpleegd op 27 november 2019, 14 december 2016.

[AICP08] AICPA, *Audit Guide, Service organizations: applying SAS No.70, as amended, with conforming changes as of March 1, 2008.*

## Drs. R.Ch.T. (René) Ewals RE | Managing Partner bij ACS

René is Managing Partner bij ACS te Doorn en heeft daarvoor twintig jaar bij de big four gewerkt als IT-auditor, waarbij hij in zijn laatste functie eindverantwoordelijk was voor de Europese praktijk op het gebied van assuranceonderzoeken (niet zijnde jaarrekeningcontroles) binnen de IT-auditorganisatie. Hij heeft een praktijk op het gebied van audit & assurance. Daarnaast is hij voorzitter van de Commissie Beroepsreglementering van NOREA en heeft hij actief meegewerkt aan de totstandkoming en invoering van de ISAE 3402-standaard.