Controleur, ontwaakt als I-Auditor!

JURGEN VAN DER VLUGT

Onlangs verscheen in De EDP-Auditor een opiniebijdrage van collega Kersten waarin hij aangaf het nut en de gevolgen in twijfel te trekken van het IFAC-lidmaatschap en de daaruit dwingend volgende overname van regelgeving.

Voor de goede orde; de NOREA is net als de ISACA *affiliate member* van de IFAC, waardoor overname van de IFAC-regelgeving wordt aanbevolen maar niet verplicht is. Zo wordt het door de NOREA ook opgepakt, veel regelgeving is immers niet relevant voor IT-auditors.

Herziening van de regelgeving was al in gang gezet vanwege maatschappelijke druk, onder andere door het Reglement Gedragscode en het Raamwerk en de Richtlijn voor Assurance-opdrachten naar IFAC-model te herzien. Dit was in de visie van het bestuur ook noodzakelijk omdat de rol en positie van RE's bij assurance opdrachten werd betwist op grond van 'nadere voorschriften' die door het NIVRA werden uitgevaardigd. Hierdoor zouden uitsluitend accountants verantwoordelijkheid kunnen dragen voor assurance-opdrachten, terwijl RE's juist op het terrein van IT-assurance over de vereiste expertise hiervoor beschikken.
Het was dus met name voor de RE's, die niet tevens RA zijn, van belang om in dit verband een zelfstandige positie veilig te stellen. Op grond van onze statuten worden RE's geacht op te treden als IT-auditor wanneer zij een oordeel of advies geven. De belangen in samenhang met beide taken horen door de beroepsorganisatie te worden behartigd. Hierdoor was ook de structuur voor de andere reglementen aan herziening toe, en is een nieuwe structuur neergezet. Voor zover daarin relevante IFAC-reglementen passen, worden die ingepast met behoud van (oftewel aanpassing naar) onze eigen smaak en insteek. En dus gaan we niet de kant van de financial auditor op, haast integendeel.

Niet te veel regels

Kersten noemt onder andere een dreiging van een 'te-veelheid' aan regels, hetgeen volgens mij zowel gevolg als medeoorzaak is van een mentaliteit gericht op rule-based auditing. Maar wat blijkt bij goede lezing van de 'IFAC-aligned' nieuwe regelgeving? Die is net zo principle-based als onze oude GBRE en nieuwe regels.
Hoewel er misschien wel zó veel toelichting en nuancering bijstaat, dat een te snelle lezing het beeld verduistert. Door de nieuwe regels te volgen, zal het dus niet een kwestie zijn van rule-based de plank precies misslaan, maar juist de spijker op de kop. 'Voldoen aan de normen' is sommigen wellicht duidelijker dan 'effectief zijn', maar het is het laatste wat de klant[1] wil weten.
Wat de klant wél wil, daar heeft de auditor maar naar te luisteren (sic), anders maakt hij/zij zichzelf onmogelijk of ten minste nutteloos. Het is immers de assurance zoals de klant die vraagt die leidend zou moeten zijn. En rule-based vinkwerk of alleen maar voldoen aan willekeurige (!) normen, is *niet* waar de klant om vraagt. Dat het mocht hebben geleken of de klant alleen om compliance-vinkwerk vroeg, was vooral in het wereldbeeld van rule-based denkende auditors die wellicht dachten hun dromen van eeuwige checklists eindelijk verwezenlijkt te zien.
Gelukkig dus; stel je voor dat we niet verder komen dan aangeven of een organisatie 'voldoet aan de normen' of dat het normenstelsel 'effectief' is. Dan hebben we het nog steeds alleen over machinale beheersing, gedachteloos de procedures volgend. Deels nodig, maar niet voldoende. En blokkerend voor de gezondheid van de organisatie als we zouden streven naar perfecte beheersing in plaats van naar optimale beheersing. Want bij optimale beheersing hoort (situationeel bepaalde) inschatting van materialiteit van gebrek of verbetermogelijkheid en doelbewust afwijken als daar door de auditee naar zijn kennis, inzicht en ervaring voldoende reden toe is. Als de auditor het er dan niet mee eens is, moet de auditor eerst maar nagaan of hij wel deskundiger is dan de auditee en of hij wel het 'recht' heeft de auditee weg te lokken of te dwingen van de, in de ogen van de auditee en *waarschijnlijk* van diens chef, ad hoc te bepalen beste handelwijze.

Immaterieel

En wat *materieel* is of niet, daar kan in tegenstelling tot wat Kersten zou willen, ten principale geen 'guidance' of handreiking voor worden opgesteld. Materialiteit is een van die zaken die bij uitstek situatiegebonden is, en kan alleen door het professional judgement van de auditor op basis van het gewicht van de getroffen informatie in de specifieke situatie worden ingeschat. Lukt dat de auditor niet, dan moet hij/zij constateren niet de juiste ervaring te bezitten en dus niet voldoende gekwalificeerd te zijn. Als materialiteit zou verworden tot een meetlat, waarom dan nog auditors ingezet? Een expert system of gewoon rekenprogramma is dan veel sterker en zuiniger.
Terzijde – de term 'evidence' is niet ontleend aan het Stramien van de accountants. Typisch een geval van *cum hoc ergo propter hoc*: correlatie betekent geen oorzaak-gevolg. Dat de NIVRA ook IFAC-teksten als bron neemt, betekent niet dat wij de NIVRA volgen maar dat we gelijkop gaan.

En zelfs al wordt een insteek vanuit risico-analyse gekozen om materialiteit in te kaderen, dan nog weet de auditor zelden meer op te merken dan dát de risico-analyse is uitgevoerd, of eventueel dat die naar behoren is uitgevoerd hetgeen alleen wil zeggen dat de procedures zijn gevolgd. Over de inhoud en uitkomsten van de risico-analyse durft een auditor vaak niks te zeggen – wellicht terecht als degenen aan de leiding daar zitten omdat ze de risico's beter kennen dan de auditor.
Dat de collega's van ISACA pogen allerlei nadere aanwijzingen te geven, geeft geen blijk van loskomen van de beperkingen van rule-based denken. Overigens niets ten nadele van de Nederlandse ISACA-collega's met wie de NOREA steeds inniger samenwerkt.

Van IT-audit naar I-audit

Waarmee we komen op het werkelijke punt waarop we ons zouden moeten ontwikkelen: Van IT-auditor naar I-auditor. Niet langer gericht op de (micro-, meso- en/of macro-)syntax maar op de semantiek van informatie. Gelijkop met de ontwikkelingen in de IT-wereld naar 'commoditisation' van IT, 'IT uit de kraan' en dergelijke op standaardisering van IT-diensten duidende termen, zien we immers een steeds grotere vraag van onze klanten naar zekerheid over *bruikbaarheid* en *betekenis* van gegevens[2]. Informatie over informatie dus.
Hieruit volgt wel dat we ons zullen moeten herbezinnen op onze methoden en technieken van audit. We zullen kennis en inzicht moeten hebben in wat informatietheorie ons brengt, we zullen moeten gaan leren begrijpen wat ons I-auditwerk bijdraagt in raamwerken van managementbesluitvorming (op welk niveau dan ook). Nee, dat begrijpen we nog nauwelijks, anders zouden we vanzelf al niet langer spreken over 'voldoen aan normen' waar de klant zo weinig aan heeft. We zullen los moeten gaan komen van de Starreveld'se en Looyen'se gedachten van administratiefabrieken waarin het bedrijfsgebeuren wordt afgebeeld, met een goedkeuring van de fabriek niet van de waarde van de erin en erdoor vervaardigde producten. Oftewel loskomen van de jaarrekening en andere vergelijkbare te-late stempeltjes op informatie en veeleer à tempo assurance voor web-published externe en interne informatiesnippers geven. Uitkomstgericht, niet gericht op de totstandkoming!
De I-auditor zal zich dus niet langer kunnen verschuilen achter een vaag soort afstandelijkheid van 'Ik heb vastgesteld dat aan allerlei pietluttige regeltjes, proceduretjes en vormvereisten is voldaan, maar of je iets met de informatie uit de systemen kunt, daar kan ik niks mee', of in analogie voor de jaarrekening 'Het recordverlies zoals dat door de directie wordt gepresenteerd, klopt nauwkeurig, binnen ruime [!] marges'. Dat vult op zich leuk de losse uurtjes(-factuurtjes) maar qua zekerheid voegt het zo weinig toe.
We zullen, gebaseerd op *onder andere* toetsing aan normen en effectiviteit van normenstelsels voor beheersing, toe moeten naar assurance in de vorm van 'Ik heb vastgesteld dat de totstandkoming niet je van het is, maar op deze informatie kan vertrouwen' of in analogie voor de jaarrekening 'De directie heeft geen ideeën om de ingelegde gelden rendabel te maken'. Evenzo zullen aanbevelingen niet gericht moeten zijn op symptoombestrijding maar op wezenlijke en haalbare verbeteringen. Dit geldt voor interne en voor externe auditors... (Ga maar na.)
Ja, ook de accountant zal inderdaad de kant van de I-auditor op moeten schuiven of overbodig worden. Maar gaan wij terug naar een ondergeschikte rule-based rol of gaan we, komende uit een ander specialisme, werkelijk nuttig worden op een principle-based leest ..?
We hebben daarvoor wel een uitbreiding nodig van onze onderzoeksmethodes en waarschijnlijk ook van onze kennis en kunde. Dat we het nog niet kunnen, wil niet zeggen dat we het niet zouden moeten gaan kunnen.

Eigen koers

Wat betekent dat we niet alleen los van financial audit-angehauchtheid maar ook los van de formaliteiten van zusterverenigingen een eigen koers kiezen. Het door Kersten gewenste wakker worden is dus al bezig. Voor de rule-based'en betekent dit een uit een diepe slaap (of autisme) komen, voor de overigen slechts een ontwaken uit een sluimer, om verfrist weer een bijdrage te kunnen leveren.
Een gewone update-actie op de regelgeving, halverwege de voor de hand liggende teksten van de IFAC invoegend waar die van pas komen, is dan ook niet een ontwikkelrichting maar een parallel lopende huishoudelijke taak. De Commissie Herziening Beroepsregels (CHBr) poogt dan ook niet 'alle' mogelijke regels over te nemen maar streeft juist naar zo min mogelijk regels – maar dan wel de goede, met guidance waar nodig en waar ten principale mogelijk.
En de CHBr werkt aan de vernieuwing, onder andere door de initiatieven om 'advies' maar ook 'beoordeling/quick-scan/doorlichting/review' als werksoorten en inhoud eens tegen het licht te houden, *voordat* wordt besloten óf en hoe reglementering nodig zou kunnen zijn. Tot slot zullen we met ons allen het terra incognita van de nieuwe 'assurance' moeten gaan verkennen.
Voorwaar is het dus een goede oproep om wakker te worden, maar laten we dan met twee goede benen uit bed stappen om de toekomst in te wandelen in plaats van weg te lopen van de werkelijke problemen. ■

Noten

[1] **Waarmee wordt gedoeld op alle mogelijke belanghebbenden die, op welke afstand dan ook, opdracht geven.**

[2] **Assurance over de standaard-IT blijft natuurlijk wel, maar als bijzaak; routinematig uitgevoerd.**

Ir.drs. J. (Jurgen) van der Vlugt RE CISA is senior manager voor advies- en auditdiensten op gebied van IT-governance en risicobeheer bij Noordbeek B.V. Hiervoor was hij onder andere IT Audit Manager bij KPMG, en IT Audit Manager en Group Security Information Manager bij ABN AMRO Bank. Tevens is hij lid van de Commissie Herziening Beroepsregels en de Vaktechnische Commissie, voorheen voorzitter van de Commissie Educatie, secretaris van ISSA NL, en regelmatig publicist en spreker op conferenties. Dit artikel is geschreven op persoonlijke titel.