Column

Assuranceontwikkelingen: een visie

16 juni 2020

Jaap van Beek en Herman van Gils

In dit artikel geven wij onze visie over de huidige, en vooral ook de toekomstige assurancedienstverlening. IT-auditors bieden tegenwoordig niet alleen ondersteuning bij de jaarrekeningcontrole, maar geven veel meer zelfstandig oordelen over uiteenlopende onderwerpen dan in het verleden. Toch is het gros hiervan nog jaarrekening-gerelateerd, via de bekende assurancerapporten gebaseerd op ISAE 3402. Maar zoals we in dit artikel aangeven, is er steeds meer behoefte aan een veel breder scala aan onderwerpen waarover assurance bestaat.

IT-auditors zijn bij uitstek de professionals om assurance te verlenen over vraagstukken waarbij ICT een belangrijke rol speelt, bijvoorbeeld bij uitbesteding van processen, bij informatieverwerking in een keten of bij het beoordelen van software en data. Dit artikel gaat in op een aantal ontwikkelingen op het gebied van risico's en de behoefte aan assurance die kansen betekenen voor de IT-auditor. Tegelijk wordt ook een aantal uitdagingen uit de praktijk benoemd die voor het benutten van deze kansen relevant zijn. De vraag is of de IT-auditor van nu daar klaar voor is.

Welke ontwikkelingen zien we?

De trend om meer zaken uit te besteden vanuit de eigen organisatie aan gespecialiseerde serviceorganisatie neemt alleen nog maar toe in de komende jaren. Combineer dit met de maatschappelijke roep om meer transparantie in de keten en de continue ontwikkeling van technologie waardoor iedereen en alles tegenwoordig verbonden is. Deze combinatie geeft een voortdurende impuls aan de vraag naar meer zekerheid van ketenpartijen in de vorm van assurance door onafhankelijke IT-auditors. De vraag is dan vervolgens of de huidige standaarden nog wel geschikt zijn om aan die nieuwe assurancebehoeften te voldoen.

Nieuwe assurancebehoeften

Het management van een organisatie is verantwoordelijk voor het gevoerde beleid. Vroeger was dat misschien nog eenvoudig te doen, toen de organisatieleiding het hele bedrijf overzag. Nu vrijwel iedere organisatie in een keten werkt, is dat gevoerde beleid veel minder makkelijk inzichtelijk geworden. En dat juist in een tijd dat organisaties transparanter moeten zijn en zich veel meer en op allerlei gebieden moeten verantwoorden.

Bijvoorbeeld niet alleen meer details in het financiële jaarverslag, maar ook over de CO2-uitstoot in het milieuverslag of de wijze waarop aan de privacyverordening is voldaan. En dat ook nog in een tijd dat de maatschappij kritischer wordt en bestuurders veel harder worden afgerekend op eventuele tekortkomingen. In de krant en sociale media staan bijna dagelijks wel berichten over aftredende bestuurders in verband met malversaties ergens in de organisatie.

Uitbesteding aan gespecialiseerde organisaties is een van de oorzaken dat het overzicht over de bedrijfsvoering minder makkelijk is te verkrijgen. En deze trend zal nog zeker in de toekomst doorzetten. [VERH18] De afhankelijkheid van de eigen bedrijfsvoering wordt daarmee van de eigen organisatie verlegd naar de outsourcing partner. En daarmee is de klassieke motivatie voor assurance over de serviceprovider nog springlevend. Waar voorheen de boost van assuranceopdrachten vooral vanuit de financiële hoek kwam (met name introductie van SOX), lijkt de behoefte van het management nu ook veel meer de operationele processen te raken. [ALST17]

Naast deze klassieke bron voor assurance, uitbesteding, zien we tegenwoordig een nieuwe bron in de exponentiële groei van technologie die iedereen en alles tegenwoordig met elkaar verbindt. Deze ontwikkeling heeft ertoe geleid dat een nieuw type organisatie is ontstaan: digitale platformorganisaties zoals Amazon, Uber, Facebook en Google. De platformsamenleving die hierdoor ontstaat, heeft vaak een disruptieve impact op de bestaande businessmodellen. [FIJN18] Ook de opkomst van *artificial intelligence* maakt ons steeds afhankelijker van de kwaliteit van de software en de data die bij de gegevensverwerking wordt gebruikt.

Als gevolg van alle ontwikkelingen zien we behoefte ontstaan aan meer zekerheid over de afspraken in het (uitbestedings)contract, kwaliteit van software en data, maatschappelijke relevante onderwerpen en voorschriften vanuit wet- en regelgeving of ketens van dienstverlening of informatieverstrekking. Er is een groeiende behoefte aan een assurancerapport dat inzicht en zekerheid verschaft over operationele en financiële processen, softwareproducten (bijvoorbeeld calculaties daarin) en onderwerpen die al dan niet tijdelijk in verhoogde aandacht staan, zoals privacywetgeving, PSD2, processen ter voorkoming van witwaspraktijken en allerlei milieurapportages. Hiervoor zijn verschillende standaarden beschikbaar.

Daarbij tekent zich de trend af dat organisaties niet alleen assurancerapporten afgeven omdat ze daar contractueel toe verplicht zijn door partners in een keten of uitbestedingsrelaties, maar ook uit eigener beweging aan een breder maatschappelijk verkeer. Zie als voorbeeld het kader.

Voorbeeld
Een grote organisatie ziet de beschikbaarheid van het webportaal (en de daarin opgenomen diensten) als een key factor voor het succes van de organisatie. Daarom rapporteert zij frequent over de (hoge) performance van het webportaal. Aangezien de organisatie internationaal opereert, veelal via lokale systemen, kan de performance per land verschillen. Door enkele incidenten in bepaalde landen krijgt de performance van de totale organisatie negatieve aandacht in de sociale media, terwijl de performancecijfers in de meeste landen toch goed blijven. Het management wil geen discussie en wil dat externe IT-auditors voortaan een assurancemededeling afgeven bij de performancecijfers ten behoeve van het brede publiek.

Wij verwachten ontwikkelingen – die overigens deels al zijn ingezet –die weer een specifieke behoefte aan assurance zullen oproepen. Enkele voorbeelden:

- **Algorithm assurance of, breder, artificial intelligence assurance.** Steeds vaker wordt de vraag gesteld in hoeverre we eigenlijk op de uitkomsten van deze data-analyses kunnen vertrouwen. Is er sprake van *trusted analytics*? Zijn de juiste beheersingsmaatregelen bij het ontwerp, de implementatie en de uitvoering getroffen? In recent onderzoek worden vier key-elementen onderkend: kwaliteit, effectiviteit, resilience en integriteit. [ERWI18] Er is een groeiende behoefte aan assurance over de data in de vorm van een audit dan wel digital assurance, oftewel het gebruikmaken van data mining en/of proces mining gedurende het onderzoek om zekerheid te verkrijgen.
- **Cyber assurance (zekerheid over de informatiebeveiliging).** In de VS kan *cyber* assurance onder de SOC-standaard worden uitgevoerd. Inmiddels bestaat de standaard twee jaar, maar er zijn voor zover wij weten nog geen assuranceverklaringen afgegeven. Voorlopig is het gebleven bij het uitvoeren van gap-analyses. Vanwege de complexiteit, het volume en de dynamische aard van hun informatiesystemen zijn nog niet veel organisaties bereid om een onderzoek op entiteitsniveau te ondergaan. Sommige experts vragen zich ook af of het echt mogelijk is assurance te verlenen. Toch wel bijzonder voor een onderwerp dat zo in het centrum ligt – of dient te liggen – van de IT-auditor.
- **Blockchain of *digital ledger technology* assurance.** Deze ontwikkeling wordt gezien als een nieuwe technologie waarmee potentieel enorme voordelen zijn te behalen, zoals efficiency, transparantie, controleerbaarheid en onweerlegbaarheid. In Malta heeft de overheid (Malta Digital Innovation Authority) een control framework opgesteld voor deze technologie. Het bevat vele elementen van SOC2, maar de IT-auditor wordt ook gevraagd zelf de kwaliteit van de software te testen – wat in de meeste gevallen een nieuwe stap zal zijn voor IT-auditors. Binnen NOREA is op dit gebied de kennisgroep Keteninformatiemanagement en Control actief om hier ook over na te denken. Op 6 juni 2019 presenteerden zij hun visie tijdens het seminar Digital Ledger Technologie en Assurance.
- ***Process controlling***. Deze essentiële bedrijfsfunctie voor de beheersing van industriële processen behoorde tot voor kort hoofdzakelijk tot het domein van technical engineers. De laatste jaren zien we een integratie van technische processen en administratieve processen (inclusief robotisering) , een trend die zeker de komende jaren zal doorzetten. Door die integratie zal er meer druk komen te staan op de expliciete beheersing van de technische processen en als een logisch vervolg daarop in de verantwoording daarover. Zoals hiervoor al is aangegeven zal dat kunnen leiden tot meer behoefte aan assuranceonderzoeken.

Onder invloed van deze ontwikkelingen zien we steeds meer stakeholders die behoefte hebben aan assurance op een steeds breder vlak. Tabel 1 bevat een niet-uitputtend overzicht van de assurancebehoefte van verschillende stakeholders.

	STAKEHOLDERs				
	Management	**Accountant**	**(potentiële) gebruiker**	**Wetgever**	**Maatschappelijk verkeer**
ASSURANCE-VOORBEELDEN	Operationele processen (zoals blockchain, kerngetallen, cybersecurity)	Financiële processen	Calculaties in software en systemen (algorithm assurance)	Privacywetgeving	CO2-uitstoot, security in web portal of Facebook etc., kerngetallen

Tabel 1: Stakeholders en hun behoeften aan assuranceproducten

Voor een aantal van genoemde assuranceproducten zijn verschillende standaarden beschikbaar.

Standaarden en commerciële vertaling lopen achter en zijn verwarrend

Met al deze nieuwe assurancebehoeften mag verwacht worden dat de standaarden zich ook ontwikkelen en verder gaan dan het domein van de jaarrekeningcontrole. De bekendste assurancestandaard is Richtlijn 3402 (ISAE 3402/SSAE 18/SOC1), specifiek gericht op uitbesteding van processen en beheersmaatregelen die relevant zijn voor financiële verslaggeving. Maar een Richtlijn 3402-rapport heeft ook zijn beperkingen. Dit komt voort uit de oorspronkelijke doelstelling van de richtlijn, namelijk het informeren van de accountant van de partij die uitbesteedt (de gebruikersorganisatie). Deze afgrenzing richt zich niet alleen op de scope, maar ook op de kwaliteitsaspecten die het 3402-rapport afdekt. Dit zijn de aspecten juistheid, volledigheid en tijdigheid, de aspecten die van belang zijn voor een betrouwbare financiële verantwoording. Vertrouwelijkheid en Continuïteit worden vaak niet volledig door het rapport afgedekt omdat ze niet of beperkt van belang zijn voor de financiële verslaggeving. De verwachting is dat de Richtlijn 3402 nog jaren 'mee kan' voor het beoogde doel. Hooguit is periodieke aanpassing aan nieuwe auditinzichten nodig, zoals in de Amerikaanse standaard enkele jaren geleden is gedaan. [GILS17]

De vraag is of de groeiende assurancebehoeften van andere stakeholders dan accountants dan maar simpelweg kan worden afgedaan met 'de moeder der assurancestandaarden', de Richtlijn 3000 (ISAE 3000). De afgelopen jaren zijn risico's in de operationele beheersing actueel geworden. Voorbeelden zijn security, cyberincidenten, privacy, performance, maar denk bijvoorbeeld ook aan gebieden als organisatiecultuur, *soft controls* en datakwaliteit. Heel bijzonder dat assuranceopdrachten voor dit soort risico's allemaal wordt uitgevoerd volgens de ISAE 3000. Menig IT-auditor heeft aan potentiële opdrachtgevers met moeite kunnen uitleggen wat zo'n richtlijn dan eigenlijk doet en waarom de Richtlijn 3000 een *fit for all* is. Men kan zich afvragen of de Amerikaanse poging om 'commerciële' namen

aan assuranceproducten te koppelen heel succesvol is. De SOC1 is wel duidelijk maar de SOC2, is wel een ISAE 3000, maar toch weer heel anders. En dan is er nog een SOC voor cyber security, die weer een andere ISAE 3000 implementatie is, net zoals overigens de SOC3. En ten slotte verandert ieder jaar de implementatie van die specifieke SOC-standaarden (SOC2-2017 of SOC2-2018). Bijzonder is ook dat de afkorting 'SOC' sinds de invoering van de SOC voor cyber zonder veel ruchtbaarheid is aangepast.

Het voordeel van SOC2 is dat hierin expliciet controledoelstellingen en een set van minimale normen (*focus point*s in de nieuwste versie) zijn benoemd, zodat een marktstandaard is gezet. De uitgever van een SOC2-rapport en de ontvanger van zo'n rapport weten hierdoor enigszins waar ze aan toe zijn.

De 3000-richtlijn bepaalt wat ten minste in een assurancerapport moet zijn opgenomen, maar laat de vorm vrij. In de praktijk zien wij dan ook veel verschijningsvormen van deze assurancerapporten. De lezer van het rapport moet door eigen beoordeling van het rapport vaststellen of dit aansluit op de eisen waarvoor het gebruikt gaat worden. Belangrijke aandachtspunten zijn daarbij de timing van het rapport en de periode waarover het is afgegeven, de scope (alle relevante objecten meegenomen?), de criteria die zijn gehanteerd bij de toetsing (bekende standaarden, voldoende diepgang?), de eventuele beperkingen (bijvoorbeeld indicatie dat gebruiker aanvullende maatregelen moet uitvoeren) en de verklaring van de auditor (was het een betrouwbare partij en wat waren bevindingen?). Kortom, de lezer dient (bijna) een RE te zijn om het rapport echt te kunnen doorgronden en wijzelf hebben al menigmaal bij de bespreking van een concept-rapport van een bestuurder de vraag gekregen: 'waar nu staat dat het goed is?'.

Natuurlijk kan van de 'kale' 3000-standaard gebruik worden gemaakt, waarbij vervolgens een normenstelsel wordt ingevoegd dat of gebaseerd is op een normenstelsel dat al door de dienstverlener is opgesteld of bij voorbeeld is afgeleid uit één van kenmerkende normenstelsels uit de markt. Denk hierbij aan Cloud Security Alliance, NIST, COBIT-normenkader DNB, normenkaders van NOREA et cetera. Ook in de nieuwste versie van SOC2 wordt ruimte gemaakt om dit soort normenkaders in te voegen en ook om eventueel in de toekomst over te gaan tot *cyber assurance* op basis van het organisatiebrede cybersecurity-riskmanagementstelsel. De AICPA beschikt al over een SOC Cybersecurity-raamwerk dat kan worden ingezet.

Voor iemand die dertig jaar actief geweest is in het IT-auditvak is het opvallend hoeveel specifieke controleraamwerken er inmiddels zijn, waarvan er ook veel op de NOREA-site te vinden zijn. De controleraamwerken zijn zowel specifiek voor producten of processen als voor bepaalde branches en overheden. Maar ook meer in de diepte op het gebied van bijvoorbeeld cybersecurity. Wij noemen hier nog DigiD (Digitale Identiteit), ENSIA (Eenduidige Normatiek Single Information Audit) voor gemeenten en VIPP

(Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional) en natuurlijk Privacyproof.

Ook bijvoorbeeld de Duitse collega's hebben afzonderlijke standaarden voor specifieke assuranceproducten. Wellicht het meest bekend is de IDW PS880 (weer een invulling van de ISAE 3000!) voor de beoordeling van financiële aspecten en controls in financiële pakketten die nog niet zijn geïmplementeerd. Als het financiële pakket dan vervolgens is geïmplementeerd kan assurance worden gegeven over de implementatie via de IDW PS 850. Hoewel dit meer 'accountancymededelingen' zijn, blijkt ook in de Duitse praktijk dat vooral IT-auditors deze onderzoeken doen.

Dichter bij huis is ook een goed voorbeeld voor handen. De NBA heeft de assurancestandaard 3810N uitgegeven, gericht op maatschappelijke verslagen ('het sustainability verslag') De (deskundige) markt herkent dit nummer van de assurancestandaarden en weet wat de assurancerapporten behelzen. En ook hier blijkt in de praktijk dat IT-auditors regelmatig worden ingezet omdat ook hier de meet- en rapportageprocessen veelal sterk IT-ondersteund zijn.

Conclusie is dat er diverse standaarden zijn, maar dat buiten enkele heel gerichte standaarden veel assurancewerk terugvalt op de Richtlijn 3000, die daardoor weinig generiek is en voor de ontvanger altijd maar afwachten is wat het gebruikte normenkader is geweest. Het wordt volgens ons tijd om de standaarden verder te ontwikkelen vanuit het IT-auditvakgebied.

Gewenste ontwikkelingsrichting van het beroep

De IT-auditor is inmiddels een algemeen aanvaarde deskundige met betrekking tot het beoordelen van diverse IT-vraagstukken. Daarom is het belangrijk dat dit wordt ondersteund door een stevige beroepsgroep die de verantwoordelijkheid voor assuranceoordelen kan dragen en derhalve gezien wordt als een vertrouwenspersoon in het maatschappelijk verkeer.

IT-auditing als zelfstandig volwassen (assurance)beroep

We hebben hiervoor toegelicht dat de vraag naar assurancediensten zich zowel verbreedt als verdiept. Verbreding zit hem in het scala van onderwerpen waarop assurance wordt gevraagd, verdieping komt door specifieke controle-frameworks vanuit verschillende branches en door de voortdurende technologische verdieping. Aangezien de objecten van onderzoek van diverse assuranceopdrachten enorm kunnen verschillen, is het voor de verantwoordelijke IT-auditor van belang om na te gaan of de noodzakelijke gespecialiseerde vaardigheden en kennis in het team zijn opgenomen. Zo mag worden

verwacht dat in geval van cyberassurance of privacyassurance de auditor ervoor zorgt dat specialisten worden ingezet, en dat geldt nog sterker voor bijvoorbeeld assurance rond artificial intelligence en distributed ledger technology. Data scientists en softwarespecialisten komen er dan bij en misschien ook nog specialisten in soft-controls en ethiek. Meer dan dertig jaar geleden ontstond de IT auditor als specialist vanuit de jaarrekeningcontrole. Nu zien we dat als de IT auditor zich niet verder bijschoolt, hij meer generalist gaat worden. In die rol moet hij het team kunnen blijven aanvoeren en naast kennis van de assurancestandaarden ook in staat moet zijn de werkzaamheden van de specialisten te beoordelen. Kenmerkend is in dit kader een recente rapportage ('Verkenning') van de NBA over de rol van de auditor bij het beoordelen en afgeven van assurance bij algoritmes. [NBA20] Opvallend daarbij is dat consequent bewust wordt gesproken van 'auditor' en niet van 'accountant'. Maar het feit dat het NBA deze verkenning uitgeeft, roept de vraag op of de accountant zich hier in de leidende rol ziet en IT-auditors beschouwt als de specialisten die ingehuurd kunnen worden. Is dit misschien het moment voor de IT-auditor om uit de schaduw te stappen en meer de leiding te nemen en te krijgen bij dit soort ontwikkelingen?

Naar onze mening ligt bij de IT-auditorsopleiding nog te veel het accent op de ondersteuning van de jaarrekeningcontrole. Ook het onderwijs kan zijn steentje bijdragen aan de noodzakelijke voorbereiding van RE's op nieuwe auditvragen. De opleidingen zouden ondersteuning van de jaarrekeningcontrole niet meer als de belangrijkste dienst moeten behandelen maar als één van de vele specifieke diensten.

IT-auditors als vertrouwensman maatschappelijk verkeer

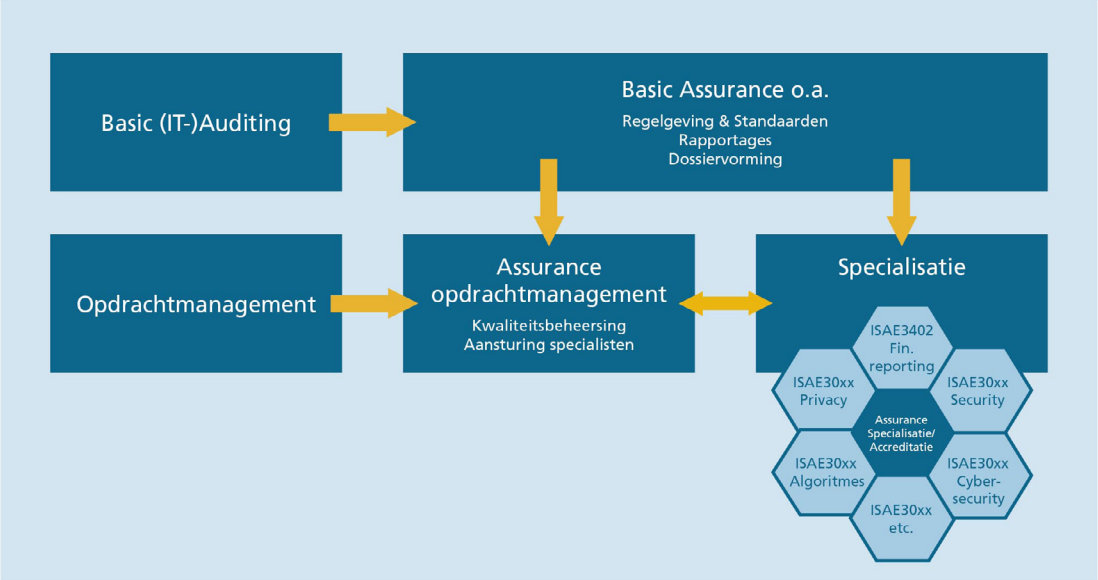
De IT-auditor als specialist is voortgekomen uit het accountantsberoep. De auteurs zijn van mening dat de IT-auditorsberoepsgroep meer dan nu het geval is, naar voren moet treden als beoefenaars van een eigen volwassen (assurance)beroep. Daar hoort bij dat ze ook producten opleveren die ver weg van de accountants kunnen staan. De slogan 'vertrouwensman van het maatschappelijk verkeer', al jaren niet weg te denken bij het accountantsberoep, geldt bij deze ontwikkelingen misschien nog sterker voor de IT-auditors, het liefst in een toekomstvaste, genderneutrale variant.

Hoe de IT-auditor zich moet ontwikkelen

De IT-auditor zal zich in twee richtingen moeten ontwikkelen: enerzijds als de teamcaptain die de aansturing van opdrachten doet, anderzijds als de specialist die op (deel)gebieden echte experts zijn.
Daarnaast zien wij dat meer gebruikgemaakt dient te worden van de technische middelen die beschikbaar zijn, zoals digital assurance, maar ook dat juist het menselijk aspect kritisch is om daadwerkelijk kwaliteit te borgen (soft controls).

Ontwikkelen in twee richtingen

Om succesvol te blijven, is het wel zaak om antwoord te vinden op de uitdagingen die voor ons liggen. De IT-auditor moet zich zowel ontwikkelen als een teamcaptain die een team van verschillende specialisten kan aansturen, maar ook als specialist op deelgebieden waarover assurance moet worden afgegeven (zie figuur 1). Door de verbreding en verdieping van de onderwerpen lijkt het niet meer mogelijk tot verantwoorde assurancemededelingen te komen met uitsluitend generalistische IT-auditors. Voor bredere assuranceopdrachten zal met name een teamcaptain essentieel zijn om vast te stellen of met de kwaliteit van de verschillende ingezette specialisten voldoende grondslag is voor het afgeven van de assurancemededeling.



Figuur 1: Assurance als specialisatie binnen het IT-auditdomein

Over het accountantsberoep is momenteel veel discussie, IT-auditors zijn tot nu toe redelijk buiten schot gebleven. Het zou wel goed zijn lering te trekken uit de maatschappelijke discussie die rond accountants gevoerd wordt. Als je vertrouwensman wilt zijn van het maatschappelijk verkeer moet je ook gereed zijn om extern getoetst te worden op de kwaliteit van de verrichte werkzaamheden. Op dit moment vindt de toetsing nog door NOREA zelf plaats, net als in het verleden de accountants door hun eigen beroepsorganisatie werden getoetst. Als de IT-auditor meer uit de schaduw wil treden en zelfstandig de rol van vertrouwensman van het maatschappelijk verkeer gaat oppakken, verdient dit absoluut aandacht. De meetlat gaat ongetwijfeld verder omhoog. Dit zal dan ook zeker impact op kwaliteitssystemen en (brede en gespecialiseerde) opleidingen moeten krijgen.

De 'team-captain IT-auditor' is verantwoordelijk om te bepalen of een specialist betrokken moet worden bij de assuranceopdracht en om overeen te komen en vast te leggen wat de werkzaamheden van de ingeschakelde specialist zullen zijn. Overwegingen hierbij zijn de professionele vaardigheden, het doel en de scope van de door de specialist uit te voeren

werkzaamheden en de mate waarop bij het vormen van assuranceoordeel wordt gesteund op de werkzaamheden van de specialist. Gegeven de kwaliteitseisen (zoals onder meer onafhankelijkheid, dossiervorming et cetera) die aan die specialisten worden gesteld, zal steeds meer behoefte ontstaan aan IT-auditors in de specialistenrol.

Vooral richten op digital assurance, continuous assurance en soft controls

Hoewel het de verwachting is dat het IT-auditvak zich zal ontwikkelen tot een digital assuranceberoep, werken we momenteel in de uitvoering van assuranceopdrachten nog steeds met *walkthroughs* aan de hand van interviews en documenten, en doen vervolgens deelwaarnemingen om een oordeel met een redelijke mate van zekerheid te kunnen geven. Technieken als data- en proces-mining staan nog in de kinderschoenen. Controls zijn nog vaak afgetekende papieren documenten. Hier ligt nog een flinke uitdaging om het assuranceproces te digitaliseren en veel meer gebruik te maken van data-analyses om volledige populaties te kunnen onderzoeken. Als we cyberassurance willen geven, moeten detectie en response veel meer aandacht krijgen en feitelijke technische (real time) gegevens onderdeel worden van het rapport. Daarnaast moet worden nagedacht of in de toekomst assurance niet langer gebaseerd moet worden op controls opgenomen in de processen (die kunnen falen) maar veel meer rechtstreeks aan de hand van de data zelf. Als de opdrachtgever proces-mining toepast, zal dit gemakkelijker worden.

Continuous assurance

Als leveranciers in de cloud een continu dashboard kunnen leveren met hun belangrijkste KPI's daarin opgenomen, dan mag verwacht worden dat er ook behoefte ontstaat aan assurance daarover. [BEEK13] Maar veel assurancerapporten zijn nog steeds maar een keer per jaar beschikbaar. De assurancestandaarden schrijven overigens niet voor hoe vaak een assurancerapport beschikbaar moet zijn. Vanuit de jaarrekeningcontrole is de gedachte van jaarlijks in onze beeldvorming terecht gekomen, maar als de trend in de maatschappij gaat naar het continu beschikbaar stellen van informatie, het continue controleren daarvan door de organisatie (continuous monitoring) dan moet het mogelijk zijn om continuous assurance te verlenen. In toenemende mate wordt gewerkt aan het operationaliseren van deze belofte en hiervan zijn reeds concrete voorbeelden gerealiseerd. Wij verwijzen hier naar [BAUT18]. In dat artikel wordt beschreven hoe ondanks investeringen in GRC-tools de uitvoering van die processen nog steeds handmatig, in silo's en gefragmenteerd wordt uitgevoerd. Door de lessen toe te passen vanuit digitale businesstransformatie zijn aanzienlijke verbeteringen mogelijk en ook al gerealiseerd. Op basis daarvan wordt een *digital risk platform* beschreven dat het mogelijk moet maken om *integrated and continuous assurance* te gaan verlenen. Gegeven de behoefte van veel stakeholders om assuranceinformatie frequenter en tijdiger te ontvangen, zou het wenselijk zijn dat de

IT-auditor zich hierop meer zou profileren, waarvoor het waarschijnlijk nodig is eerst het management te motiveren continuous monitoring in de organisatie (beter) toe te passen.

Hard- en soft controls onderdeel van assurance

Onze praktijkervaring leert dat het management een toenemende behoefte heeft aan betrouwbare en relevante informatie over gedrag. Tot voor kort werd in het kader van interne beheersing vooral gekeken naar beheersingsmaatregelen als functiescheiding, procedures en autorisaties, de zogenaamde hard controls maar in toenemend mate wordt ook het belang onderkend van *soft controls*, Dit zijn gedragsbeïnvloedende factoren als cultuur en voorbeeldgedrag. Ook als onderdeel van de jaarrekeningcontrole wordt hier meer en meer aandacht aan besteed. Binnen het auditberoep is daarbij wel veel discussie of soft controls onderdeel zijn van de controleomgeving dan wel van control activities. Hoe kan de werking van soft controls aantoonbaar worden gemaakt op het niveau van de control activities? Volgens de theorie zou het mogelijk moeten zijn een assuranceopdracht volgens het stramien uit te voeren over de werking van de soft controls. Inmiddels is sprake van een eerste assurancerapport over soft controls en dat is inderdaad ook onder de Richtlijn 3000 (type I) uitgebracht. [TAGA18] Duidelijk is dat dit onderwerp momenteel nog in de kinderschoenen staat maar dat dit voor de nabije toekomst waarschijnlijk sterk gaat ontwikkelen.

Conclusie

Maatschappelijke ontwikkelingen zoals transparantie en ketenorganisaties, en nieuwe technologieën zoals digitale platformorganisaties, artificial intelligence, cyber en digital ledger technology leiden tot nieuwe behoeften rond assurance, waarvan mag worden aangenomen dat deze behoefte ook in de toekomst nog lang zal bestaan.

Tegelijkertijd worden de onderzoeken complexer door geschetste ontwikkelingen, waardoor enerzijds behoefte bestaat aan de meer generieke IT-auditor, die het gehele onderzoek overziet en aanstuurt, als aan gespecialiseerde IT-auditors die op de complexe deelgebieden de audits met goede deskundigheid kunnen uitvoeren. Op dit moment lijken de beroepsorganisatie en de opleidingen vooral aandacht te geven aan de generieke IT-auditor. Gespecialiseerde (IT-audit)opleidingsmogelijkheden en beroepskwalificaties voor specialisten op deelgebieden zijn niet voorhanden. De behoefte daaraan lijkt groter te worden naarmate de assurancewerkzaamheden toenemen met de daarbij gepaard gaande verbreding en verdieping. Dat zal dan ook gevolgen hebben voor de kwaliteitsbeheersing van assuranceopdrachten en aandacht van de toezichthouders.

Literatuur

[ALST17] Alst, R. van; Stoof,S. *De pensioenwereld in 2017: Pas op voor schijnzekerheid bij assurance over uitbesteding*. KPMG, 2017.

[ALST19] Alst, R. van; Bruin, A. de; Langen, R. van; Suntjens A., met medewerking van Beek, J.J. *van Praktijkgids Assurance-rapport 3000*, KPMG, 2019/4.

[BAUT18] Bautista, M.C. Krutzen, B. Digitization of risk management. *Compact* 2018/2.

[BEEK13] Beek, J.J. van, Gils, H. van. Assurance in the cloud. *Compact* 2013/2.

[GILS17] Gils, H. van, Beek J.J. van. The new US assurance standard SSAE18. *Compact* 2017/4.

[ERWI18] Erwin, T., Klous, S. e.a. *Guardians of trust: Who is responsible for trusted analytics in the digital age*? KPMG International, 2018.

[FIJN18] Fijneman, R. e.a. *Unlocking the value of the platform economy: Mastering the good, the bad and the ugly*. KPMG, 2018/11.

[NBA20] *WhatIf Wat als auditors een rol gaan spelen bij het temmen van algoritmes?*. NBA Verkenning, 2020/2.

[TAGA18] M.Tagage, Tiggelen, E. van, Eerste assurancerapport bij gedrag en cultuur. *Accountant* 2018/3.

[VERH18] Verhaart, J., Ibrahim, A. Editorial: Outsourcing resolutions- be agile, automate, multisource. *Compact* 2018/1.

Drs. J.J. (Jaap) van Beek RE | zelfstandig professional

Jaap van Beek RE is zelfstandig professional. Hij heeft meer dan 30 jaar ervaring met alle aspecten van het IT-auditvakgebied. Van 2000 tot 2019 was hij werkzaam als partner bij KPMG waar hij een focus had op het beoordelen en adviseren over de kwaliteit van de geautomatiseerde informatievoorziening bij financiële instellingen, mede in het kader van de jaarrekeningcontrole. Hij was trekker binnen Europa van de global IT assurance-dienstverlening van KPMG.

Drs. H.G.Th. (Herman) van Gils RE RA

Herman van Gils is, na 40 jaar KPMG werkzaam bij KPMG, nu met (pre)pensioen. Hij heeft jaren training gegeven aan de UvA en de VU, met name ook op het gebied van assurance in het IT-domein. Binnen KPMG was hij vertegenwoordiger voor Nederland voor het domein IT in de jaarrekeningcontrole alsmede voor IT assurancedienstverlening.