Drs. Ferry Anwar RE RO
Drs. Björn Kempkes RE
Joop Winterink RA RE

IT-auditor: assurance provider en **bestuurlijke sparringpartner?**

De relevantie van IT Audit wordt evidenter, vooral omdat de diversiteit, omvang en complexiteit van IT én IT-gerelateerde risico's voortdurend toenemen. Dit brengt relevante en complexe beheersingsvraagstukken met zich mee voor directie, bestuurders, commissarissen en externe toezichthouders. Wat betekent dit voor de IT-auditor en de internal auditfunctie (IAF)?

IT-gerelateerde risico's staan de afgelopen jaren hoog op de risicoagenda's van bestuurders en het hoger management van grote organisaties. Het World Economic Forum onderkent in 2015 met 'data fraud or theft', 'cyber attacks' en 'critical information infrastructure breakdown' een drietal IT-gerelateerde risico's.
Dat IT-risico's voldoende onder de aandacht komen en blijven is een goede ontwikkeling. Ondertussen verandert de wereld van IT-mogelijkheden en de daaraan gerelateerde risico's in hoog tempo. In de praktijk stellen we vast dat deze risico's reëel zijn. Dit blijkt ook uit recente praktijkvoorbeelden waarbij de beschikbaarheid van infrastructuur en de bescherming van gegevens met regelmaat in het geding en in het nieuws komen. Denk hierbij aan de site van de Belastingdienst die moeilijk te bereiken was op de eerste dagen dat de ingevulde inkomstenbelasting beschikbaar was of aan het CBP (College Bescherming Persoonsgegevens) dat Google heeft gewaarschuwd de privacy van de Nederlandse gebruikers beter te waarborgen, omdat de aangepaste privacyvoorwaarden van Google in strijd zouden zijn met de Wet bescherming persoonsgegevens (Wbp).

Kritische risico's
Ook bij zorgverzekeraar Coöperatie VGZ (hierna: VGZ) zien we dat onze organisatie kritische risico's onderkent ten aanzien van effectiviteit van haar systemen. Het merendeel van de verzekerden dat van zorgverzekeraar wil wisselen, doet dit in de laatste week van december. Het niet beschikbaar zijn van de websites, achterliggende systemen en klantenservice kan in deze periode met recht een groot commercieel risico voor onze organisatie worden genoemd. Daarnaast speelt ook het beschermen van privacygevoelige gegevens een grote rol bij onze risicobeheersing, net als bij andere organisaties die grote hoeveelheden persoonsgegevens verwerken. Als privacygevoelige gegevens worden ontvreemd of op andere wijze onbedoeld buiten VGZ terechtkomen, dan heeft VGZ een groot probleem en veel uit te leggen aan belanghebbenden. Los van de financiële consequenties, heeft dit grote negatieve gevolgen voor het imago en de reputatie van VGZ, maar ook voor het imago van (zorg)verzekeraars in het algemeen.

Relevantie IT Audit
IT-risico's en de hieruit voortvloeiende beheersingsvraagstukken bepalen de relevantie van IT Audit. Hierin onderkennen wij twee rollen, de traditionele functie van IT Audit en IT Audit als bestuurlijke sparringpartner.

De traditionele functie van IT Audit: de professional audit opinion
De IT-auditor heeft in de traditionele rol als assurance provider een belangrijke functie bij het verstrekken van aanvullende zekerheid aan bestuurders, hoger management en toezichthouders over de beheersing van IT-gerelateerde risico's. Als normenkader hanteert IT Audit hiervoor gangbare modellen, best practices en volwassenheidsniveaus binnen deze modellen. Door hieraan te toetsen, stelt de IT-auditor vast dat beheersmaatregelen ten aanzien van IT-wijzigingen, autorisaties en continuïteit aantoonbaar hebben gewerkt voor de betreffende systemen en daaraan gerelateerde processen.
Niet alleen het IT-management is geholpen met de bevindingen, ook de externe accountant en de auditcommissie kijken vol verwachting uit naar de bevindingen en de conclusies. Im-

mers, aantoonbaar goed werkende IT-processen vormen een randvoorwaarde om op de gegevens uit IT-systemen te kunnen steunen en om op basis daarvan systeemgerichte controles uit te voeren. Het alternatief, het (laten) uitvoeren van gegevensgerichte controles, is tijdrovender en daardoor niet altijd gewenst. In de traditionele rol is de IT-auditor vooral van toegevoegde waarde met zijn 'professional audit opinion' door het geven van conclusies en aanvullende zekerheid.

IT Audit als bestuurlijke sparringpartner: een opinion of the audit professional

De complexiteit van IT staat niet alleen op de agenda van bestuurders, maar ook op die van auditcommissies én van toezichthouders zoals DNB. Dit blijkt uit het feit dat 'Complexe ICT' in 2015 een van de DNB-toezichtthema's is. DNB beschouwt complexe ICT als een belangrijke oorzaak van verstoringen in de dienstverlening van organisaties. Ook onze VGZ-voorbeelden ten aanzien van het niet-effectief zijn van systemen tijdens de piek van de zorgcampagne en privacyrisico's vallen hieronder.

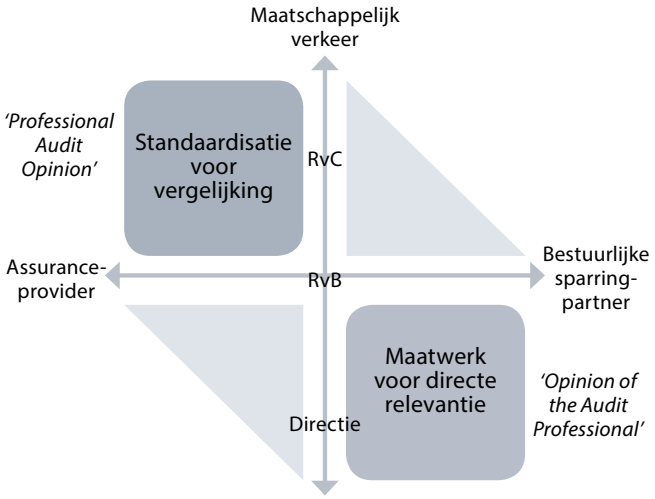
Naast het vervullen van haar traditionele rol, wordt IT Audit steeds meer gebruikt als bestuurlijke sparringpartner van organisaties, waarbij de nadruk minder ligt op het geven van assurance op basis van een onderzoek. Vanuit de traditionele functie heeft de IT-auditor specifieke en actuele kennis over (de beheersing van) IT-gerelateerde bedreigingen en risico's. Deze specifieke kennis is bij bestuurders vaak onvoldoende aanwezig, terwijl de behoefte aan deze kennis, en vooral een onafhankelijke mening, hierover er wel is. Het hoger management vraagt zich voortdurend af of de systemen met privacygevoelige gegevens wel veilig en voldoende beschermd zijn tegen uitval, cybercrime en andere ongewenste situaties. Ook wil het hoger management weten welke ontwikkelingen er in de markt zijn en of de IT-organisatie en -systemen voldoende robuust zijn om bedreigingen te weerstaan. De IT-auditor kan in deze situaties met zijn 'opinion of the audit professional' in toenemende mate van toegevoegde waarde zijn omdat de IT-auditor invulling kan geven aan een behoefte die leeft bij het bestuur en met hen kan sparren over bijvoorbeeld IT-bedreigingen.

IT Audit in beweging

De rol van IT Audit zit in een spagaat. *Figuur 1* geeft de rollen van de IT-auditor grafisch weer.[1] Op de verticale as zien we opdrachtgevers en gebruikers van IT Audit, terwijl op de horizontale as de rol van IT Audit is weergegeven. De traditionele IT Auditrol (professional audit opinion) staat linksboven; een standaard audit, bedoeld om assurance te verstrekken aan het maatschappelijk verkeer. In het kwadrant rechtsonder zien we de rol van bestuurlijke sparringpartner in de organisatie; de rol waarbij de opinion of the audit professional wordt gevraagd.

Stakeholders verwachten primair dat de IT-auditor op basis van kennis en expertise assurance kan geven met betrekking tot de effectieve beheersing van IT-gerelateerde risico's. De complexiteit en diversiteit van IT-risico's roept wel de vraag op of de IT-auditor voldoende geëquipeerd is om aan die verwachtingen te voldoen. Om de traditionele rol als assurance provider (het geven van de professional audit opinion) te kunnen vervullen, moet de IT-auditor vaak een 'IT-spaghetti' van de organisatie doorgronden en zal het slechts toetsen aan gangbare normenkaders niet volstaan. Daarbij is het legitiem de vraag te stellen of het inzichtelijk hebben van de IT-omgeving een verantwoordelijkheid is die vooral bij een IAF zou moeten liggen. Het verkrijgen van zekerheid bij de beheersing van bedrijfs- en IT-risico's is een gezamenlijke verantwoordelijkheid van alle lijnen uit het three-lines-of-defensemodel, waarin de eerste lijn verantwoordelijk is voor de aantoonbare beheersing, de tweede lijn ondersteunt en monitort en de derde lijn (vanuit de traditionele rol) aanvullende zekerheid (conclusies) geeft.

IT Audit zal in geval van complexe IT het inzicht en de durf moeten hebben om de gangbare modellen los te laten dan wel aan te vullen met overige inzichten. De IT-auditor moet de eerste en tweede lijn opzoeken en challengen op kritische IT-risico's en de beheersing ervan. De IT-auditor moet namelijk ook invulling kunnen geven aan zijn rol als bestuurlijke sparringpartner, wat betekent dat ook andere meer holistische benaderingen moeten worden gebruikt in het overleg met businesspartners. Het bestuur zal niet alleen willen weten dat de 'IT-spaghetti' goed beheerst wordt maar heeft wellicht voorkeur voor een 'overzichtelijk bord met asperges' (quote van Boonstra bij Philips).



Figuur 1. De rollen van de IT- auditor

Uitdaging voor IT Audit en de internal auditfunctie
Het IIA geeft in haar definitie aan dat de IAF een onafhankelijke, objectieve functie is die zekerheid verschaft en adviesopdrachten uitvoert om de organisatie te helpen haar doelstellingen te realiseren. Dit betekent dat zowel een professional audit opinion wordt gevraagd als een opinion of the audit professional. Vooral bij het vervullen van de laatstgenoemde rol moet IT Audit zich ervan bewust zijn dat traditionele modellen en normenkaders hun beperkingen kennen. Deze houden bijvoorbeeld geen rekening met menselijk gedrag, zoals weerstand tegen verandering of de neiging suboptimale oplossingen tegen beter weten in te accepteren. Daarnaast bestaat er niet zoiets als een objectieve waarheid, de wereld zit veel complexer in elkaar dan in modellen is te vatten.
Als traditionele normenkaders niet voldoende inzicht geven in de beheersing, wat moet de IT-auditor dan gebruiken en hoe onderscheidt hij zich in zijn werk ten opzichte van andere professionals? Ook door de beroepsorganisatie NOREA wordt erkend dat de Register IT-auditor (RE) in de adviesrol wordt ingehaald door de minder zwaar opgeleide en minder streng gereglementeerde professionals. Met andere woorden, om de toegevoegde waarde en betekenis van IT Audit te behouden is kennis van normenkaders niet meer voldoende. IT Audit als bestuurlijke sparringpartner moet ook inzicht hebben in de IT-complexiteit en de wijze waarop de risicobeheersing moet worden ingericht.

De historische kracht van IT Audit ligt op waarheidsvinding en deskundige onafhankelijke evaluaties rondom IT (de professional audit opinion). Om ook voldoende invulling te geven aan de rol van bestuurlijke sparringpartner (de opinion of a professional), zijn wij van mening dat de IT-auditor voor meer relevantie en effectiviteit kan zorgen door:
- zich meer te richten op de toekomst in plaats van op verantwoording over het verleden;
- zijn werkveld te verbreden, waarbij hij oog heeft voor going concern, verandertrajecten en strategische vraagstukken (advies) om het potentieel van IT uit te nutten;
- communicatieve en analytische vaardigheden te verbeteren.

Keuzen voor de internal auditfunctie en IT Audit
Het verstrekken van assurance is in onze ogen altijd de kurk waarop de IAF drijft. Daarbij verwachten de externe accountant, de raad van bestuur, de raad van commissarissen en de toezichthouders vooral de rol van assurance provider. Deze onafhankelijke professional audit opinion is en blijft de grondslag voor de IAF en IT Audit. Zonder een rol als assurance provider in de derde lijn ontbreekt de basis voor een andere rol voor het hoger management.
Ondertussen ontwikkelt IT Audit zich meer richting bestuurlijke sparringpartner. IT Audit wordt door het hoger management uitgedaagd om te zeggen wat hij ziet en te (laten) zien wat hij zegt. In deze rol is de toegevoegde waarde van IT Audit een opinion of the audit professional.
De centrale vraag die resteert is wat dit betekent voor de inrichting van de IAF. De professional audit opinion wordt van nature verwacht, maar de opinion of the audit professional moet je eerst verdienen! Voldoende draagvlak in de organisatie om deze rol te mogen vervullen is cruciaal. En hoe richt je de IAF zo in dat je beide rollen stimuleert? Vraagstukken die hierbij beantwoord moeten worden is hoe je het onderscheid tussen rollen en een verdeling tussen IT-auditors maakt. Een IT-auditor die beide rollen tegelijkertijd vervult, is dit vanuit de externe en interne assurancerichtlijnen wel toegestaan? Hoe ver moet deze scheiding gaan, welke afspraken maak je intern en met de klant en voor welke duur moet dit gelden? Allemaal vragen die je als IAF moet beantwoorden.
Dit betekent ook wat voor de IT-auditor zelf. Wil je enerzijds een traditionele rol als professional audit opinion blijven vervullen (die nog steeds nodig is) of wil je anderzijds met je opinion of the audit professional als bestuurlijke sparringpartner een bijdrage aan de organisatie leveren? De IT-auditor moet kiezen! <<

Noot
1. Figuur 1 is gebaseerd op Hartog, P.A. en R.W.A. De Korte, 'IT-Audit en Operational Audit: eenmanszaken of maten?', *EDP-Auditor*, 2-2005, pp. 20-27.

Ferry Anwar RE RO werkt sinds 2003 bij Coöperatie VGZ, waar hij als auditmanager vanuit Internal Audit de divisie Informatievoorziening als aandachtsgebied heeft. Daarvoor werkte hij bij Ernst & Young en FinAce.

Björn Kempkes RE werkt sinds 2007 bij Coöperatie VGZ, waar hij als auditmanager vanuit Internal Audit de stafafdelingen Financiën, Human Resources en Vermogensbeheer & Treasury als aandachtsgebieden heeft. Daarvoor werkte hij bij OHRA.

Joop Winterink RA RE is sinds 2007 directeur Internal Audit bij Coöperatie VGZ. Daarvoor werkte hij bij de interne accountantsdiensten van Philips, KPMG, Rabobank, De Nederlandsche Bank en PGGM. Ook is hij parttime docent IT-Auditing aan de TIAS Business School.