

139E RONDE TafelBIJeenKOMST: TOEZICHT OP IT

# WERKEN AAN EEN BETERE WISSELWERKING

IT is in veel bedrijven de belangrijkste investeringspost geworden, met alle risico's, kosten en opbrengsten die daarbij horen. Daarmee trekt IT steeds meer de aandacht van de toezichhouders op het bedrijf: de raad van commissarissen. Hoe ga je als CIO om met die RvC? Daarover zou het gaan in deze rondetafelbijeenkomst, die op initiatief van ervaringsdeskundigen Arnoud Klerkx en Ries Bode werd gehouden. De discussie levert bovendien handvatten voor de commissaris zelf op. KPMG ondersteunde de sessie als kennispartner.

Afgaande op de opkomst in De Villa te Vught, is de RvC-dynamiek een onderwerp dat leeft. Deelnemers hebben allereerst vragen over hun eigen houding en competenties als IT-verantwoordelijken binnen de wisselwerking, maar zijn ook nieuwsgierig naar het profiel van het ideale RvC-lid. 'Hoe innovatief moet je zijn?' of 'wat moet ik als CIO doen om een goede commissaris te worden?' Diverse discussiepunten blijken overigens al een rol als toezichthouder te bekleden. Arnoud Klerkx, CTO van Sanoma Learning en CIO of the Year 2015, en Ries

Bode, directeur van Management in Motion, zijn zelf commissaris bij meerdere organisaties. Hierdoor kunnen ze op meerdere manieren een inkijkje geven in de dynamiek van de RvC, en daarbij ook enkele zwakke plekken blootleggen. Plus de beperkingen schetsen waar je als toezichthouder nu eenmaal tegenaan loopt. "Als commissaris kun je weliswaar veel dingen zien, je kunt door je rol niet heel veel dingen dóen." De invloed beperkt zich volgens Bode tot de driehoek 'conformereren aan de richtlijnen en de wet- en regelgeving', 'goed werkgeverschap' en ten slotte 'advisering'. "Commissarissen die zich richten op het laatste zullen de ontwikkelingen goed moeten bijhouden. Daar ligt volgens mij de kern: het gebruik van kennis en ervaring van toezichthouders, op basis waarvan ze kunnen inschatten waar de business en de markt heen bewegen."

## Competenties

Het competentievraagstuk zou tijdens de gehele discussie meerdere malen aan de orde komen. Het onderwerp heeft tevens de focus van Rob Fijneman, lid van de RvB van KPMG en hoogleraar IT-auditing van de Universiteit van Tilburg/TIAS. Volgens hem is vooralsnog sprake van drie werelden: de RvB, de RvC en de CIO. Hoewel er stappen in de juiste richting worden gemaakt, is van een echte gemeenschap-

pelijke taal en agenda nog niet echt sprake. Hij refereerde aan het in 2015 gepubliceerde onderzoek *Toezicht op IT* onder de top 50-bedrijven in de financiële sector, en een gezamenlijke studie van 'Tilburg' en de Universiteit van Antwerpen.

Uit het eerstgenoemde onderzoek blijkt dat volgens maar liefst 92 procent van de geïnterviewde commissarissen de kennis en ervaring van de gemiddelde commissaris binnen de financiële dienstverlening onvoldoende zijn. Dit zou komen door een gebrek aan affiniteit, snelle veranderingen op IT-gebied, een te hoge gemiddelde leeftijd en een combinatie van deze factoren. Uit de studie bleek bovendien dat zowel de rapportage over IT-kosten, IT-projecten en relevante IT-parameters te wensen overlaat. Maar liefst 21 procent van de rapportages is kwalitatief onvoldoende.

Aanbevelingen zijn volgens de KPMG-man te zorgen voor een goede basiskennis op het gebied van IT binnen de RvC, bijvoorbeeld door minstens één lid met diepgaande IT-ervaring te benoemen. Op basis van deze kennis en ervaring kan meer aandacht geschonken worden aan de mogelijkheden van IT bij de strategieontwikkeling. Verder achtte hij het noodzakelijk dat de basiskennis van de totale populatie toezichthouders verhoogd wordt. "Er moet op RvC-niveau niet alleen gesproken worden over risk & compliance, maar ook over de strategische mogelijkheden ▶

en keuzes rond IT. Mensen moeten daarvoor getraind worden in het stellen van de juiste vragen. En vervolgens de antwoorden kunnen valideren.”

### Onwetendheid

Maar liefst zes van de deelnemers vervullen reeds een rol als commissaris. De discussië beweegt daardoor heen en weer tussen ‘hoe ga je als CIO om met je RvC’ en ‘het op een hoger plan te brengen van diezelfde RvC’. Het ene perspectief blijkt het andere overigens niet te hinderen. Feit is dat traditionele CIO's hun boards meer dan eens aan het handje moeten nemen, omdat ten aanzien van technologie de onwetendheid en de onzekerheid overheersen. Of zoals een discussiedeelner het typeert: “Ze hebben er vaak de ballen verstand van.”

Bode en Klerkx hebben in hun duopresentatie een paar prikkelende slides opgenomen. Bijvoorbeeld vragen ter overdenking in de sfeer van ‘welk bedrijf hoort niet in dit rijtje thuis?’ Hint: Er is er maar één niet failliet gegaan vanwege gefaalde IT-investeringen. Of: ‘wat zou je als digicommissaris van dit bedrijf doen?’ Om vervolgens een rijtje logo's te tonen van organisaties die recent gehackt zijn. “Het punt is dat bedrijven een aantal zaken gewoonweg op orde moeten hebben.” Denk aan de operationele IT, inclusief continuïteit en beveiliging. Bovendien moet er – Rob Fijneman zei het al eerder – een visie zijn op businesstransformatie en nieuwe verdienmodellen.

Het voorgaande zal aan de CIO veelal niet liggen. Hij of zij heeft vaak een goed gevoel voor de urgentie van zaken. Toch heeft men niet altijd een pasklaar antwoord op lastige vragen vanuit de RvC. Denk aan: ‘Wat is de bijdrage van IT aan de business?’, ‘wat is er nodig om de verwachtingen van onze klanten te overtreffen?’, ‘voelen we ons comfortabel bij de IT-risico's?’ en: ‘wat is de killer-app voor onze industrie?’ Wanneer je als CIO een weldoordacht antwoord hebt op dergelijke vragen, of wanneer je de vraag vóór bent, dan zal de wisselwerking met de RvC daar wel bij varen, zo is het idee. “De diepgang van de gesprekken neemt dan toe”, aldus Bode. Een tendens die hij sowieso waarneemt.



### Dashboard

Een van de deelnemers stelt dat het ook weer niet zo hoeft te zijn dat iedereen overal verstand van moet hebben. “Ieder RvC-lid heeft vaak zijn of haar eigen specifieke kennis en ervaring, het is dus onzin om te verwachten dat iedereen diepgaand verstand van IT heeft.” Klerkx gaat er voor een deel in mee, maar werpt tegen dat IT tegenwoordig een dermate grote portefeuille is dat iedereen er eigenlijk wel iets vanaf zou moeten weten. Bode: “Je moet mensen de juiste handvatten geven.” Fijneman: “Zie het qua competenties als gedeeltelijk overlappende cirkels,





## “ALS COMMISSARIS KUN JE WELISWAAR VEEL DINGEN ZIEN, JE KUNT NIET HEËL VEEL DINGEN DOEN”

dat zal je als RvC moeten organiseren.”  
Conclusie: toezicht op IT is te veelomvattend om vanuit de losse pols te doen. Bode en Klerkx ontwikkelden derhalve op basis van hun ervaringen als CIO en toezichthouder een modelmatige aanpak, mede op basis van bestaande frameworks als COSO en COBIT. Het gehele werkveld van de toezichthouder is hierin opgenomen, met inachtneming van zowel de lange als korte termijn, de ‘conformance’ en de ‘performance’, de interne en externe dynamiek. Alle relevante raamwerken en inzichten gecombineerd levert een zogeheten Digitalization Dashboard (kortweg Digi-dashboard) op voor digitalisering en IT met vier kwadranten. Van linksboven met de klok mee: het creëren van businesswaarde, verandermanagement, het draaien van de IT-operatie tot risicomanagement in de linker benedenhoek. Zo kan bijvoorbeeld de implementatie van een nieuwe businessdienst worden meegenomen in de programmabeheersing en governance. Op basis van kosten en KPI’s en met inachtneming van risicomanagement kan uiteindelijk businesswaarde worden gecreëerd. In control zijn op IT geeft ruimte voor innovatie en vernieuwing, inclusief de disruptie, die volgens de bedenker precies in het midden zit.

### Wisselwerking

Het Digi-dashboard helpt commissarissen niet alleen om op een andere manier naar IT te kijken, het kan ook de wisselwerking en communicatie tussen CIO, RvC en de andere bestuurders verbeteren. Een grotere mate van bewustzijn over en weer kan ertoe bijdragen dat er op een meer volwassen manier naar IT gekeken wordt, waarmee IT een integraal onderdeel van de brede discussie op bestuursniveau wordt.

