**De raad van commissarissen en het toezicht op IT**
**Lineke Sneller, Ries Bode, Arnoud Klerkx**
**[Ter goedkeuring]**

## 1. Inleiding

Het belang van informatietechnologie, of kortweg IT, nam de afgelopen decennia snel toe. Zo zijn inmiddels vijf van de zes grootste Amerikaanse beursgenoteerde bedrijven, namelijk Google, Apple, Facebook, Microsoft en Amazon, uit de technologiesector afkomstig. De enige buitenstaander in de top zes is ExxonMobil[1].

Ook in Nederland zijn dagelijks organisaties in het nieuws vanwege IT. Een selectie uit het nieuws van de eerste week van augustus in 2016 levert het volgende op. Allereerst blijkt dat IT-projecten die niet volgens plan verlopen grote invloed kunnen hebben op de financiële positie van ondernemingen: het werd duidelijk dat ENO, de kleinste zorgverzekeraar van Nederland, als gevolg van een mislukt IT-project een schade heeft opgelopen van € 3,5 miljoen. In totaal leed het bedrijf over 2015 een verlies van € 5,9 miljoen, en zag het de solvabiliteit naar 115% dalen, onder de eigen doelstelling van 120%[2] [3]. Verder was ook de impact van de nieuwe privacywetgeving in het nieuws. Een leverancier van de gemeente Amsterdam verwerkte de gegevens van drieduizend uitkeringsgerechtigden verkeerd, waardoor in de specificatie van hun uitkering het burgerservicenummer en het rekeningnummer van andere Amsterdammers werden vermeld. In overeenstemming met de nieuwe wetgeving heeft de gemeente de betrokken burgers op de hoogte gebracht en hun gevraagd de verkeerde brief te vernietigen[4]. Tot slot was één van de markten in het nieuws die door IT volledig is getransformeerd, namelijk de markt van kranten en tijdschriften. De digitale kiosk Blendle kondigde aan de digitale verzamelsite Paper over te nemen van een uitgever van traditionele kranten, de Persgroep[5].

Niet alleen uit het nieuws blijkt het toenemend belang van IT. Ook wetenschappelijk onderzoek draagt steeds meer bij aan onze kennis over IT. Uit dit onderzoek blijkt onder meer dat IT risico's grote effecten kunnen hebben voor de financiële situatie van bedrijven. Zo concluderen onderzoekers op basis van ruim driehonderd beveiligingsincidenten dat na bekendmaking van een incident de beurskoers van het getroffen bedrijf met gemiddeld 2,1% daalt, terwijl de beurskoers van een groep van veertig bedrijven die diensten op het gebied van informatiebeveiliging aanbieden rondom hetzelfde incident juist met gemiddeld 1,4% stijgt[6]. Ander onderzoek laat zien dat wanneer bedrijven aankondigen dat zij incidenten

---

1 Broekhuizen, K. (2016). *Beurswaarde vijf toptechfondsen stijgt meer dan 100 mrd na kwartaalcijfers*. Retrieved 06/08/2016, from fd.nl/beurs/1162427

2 Aartsen, C. van. (2016). *Eno vertilt zich aan ict-project.* Retrieved 06/08/2016, from www.zorgvisie.nl/ICT/Nieuws/2016/7

3 Katen, M. ten (2016). *Kleinste zorgverzekeraar van Nederland Eno in de rode cijfers*. Het financieele dagblad, 2016 (25-7), 1.

4 Duin, R. (2016). *Gemeente blundert met gegevens 3000 uitkeringsgerechtigden.* Retrieved 06/08/2016, from www.parool.nl/amsterdam/

5 Het Financieele Dagblad. (2016). *Blendle neemt digitaal magazine Paper over.* Retrieved 06/08/2016, from fd.nl/ondernemen/1162505/

6 Cavusoglu, H., Mishra, B. & Raghunathan, S. (2004). *The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers.* International Journal of Electronic Commerce, 9 (1), 69-104.

proberen te voorkomen en investeren in informatiebeveiliging, hun beurskoers met gemiddeld 2,1%[7] stijgt.

IT leidt niet alleen tot risico's, maar biedt ook kansen. Het effect van het gebruik van IT op de financiële prestaties van ondernemingen is de afgelopen twintig jaar veelvuldig onderzocht. Zo zijn bijvoorbeeld veel bedrijven in deze periode enterprise resource planning (ERP) systemen gaan gebruiken. Deze complexe informatiesystemen maken het mogelijk gegevens slechts één keer in te voeren en vervolgens in de hele organisatie te gebruiken, en zij ondersteunen ook het gebruik van best practices voor bedrijfsprocessen. Uit onderzoek blijkt onder meer dat de inzet van ERP leidt tot verkorting van levertijden en hogere productiviteit[8], en dat de aankondiging van een ERP-implementatie een positief effect op de beurskoers heeft[9] [10]. De implementatie van ERP vraagt echter om de beheersing van vele factoren in de onderneming. Dit kan behoorlijk mislopen, met risico's voor het voortbestaan van de onderneming tot gevolg[11]. Naast ERP heeft ook e-commerce natuurlijk in de afgelopen jaren een enorme vlucht genomen, en aankondigingen van e-commerce initiatieven of lanceringen van websites leiden vaak tot positieve koerseffecten[12] [13]. Tot slot wordt er op dit moment veel onderzoek gedaan naar het effect van een sterke IT-functie op de bedrijfsprestaties, en hoewel dit onderzoek nog in de kinderschoenen staat is al wel aangetoond dat een sterke IT-functie het succes in geval van overnames vergroot[14].

Met het belang van IT neemt ook het belang van goede besturing van IT toe. In dit hoofdstuk gaan we in op dat aspect van de IT-besturing dat wordt uitgevoerd door het interne toezicht, dus door de RvC of een vergelijkbaar orgaan. We zijn daarbij vooral geïnteresseerd in de vraag hoe intern toezicht op IT georganiseerd zou kunnen worden. Allereerst besteden we aandacht aan een aantal veelgebruikte begrippen. Vervolgens bespreken we literatuur die over het onderwerp al is verschenen. Daarna doen we verslag van interviews, die we hebben gevoerd met een aantal mensen met ervaring met intern toezicht op IT, als toezichthouder, als bestuurder, of als IT-verantwoordelijke. We sluiten het hoofdstuk af met een aantal aanbevelingen.

## 2. Literatuuroverzicht

### *2.1 IT-governance*

---

7 Chai, S., Kim, M. & Rao, H. (2011). *Firms' information security investment decisions: Stock market evidence of investors' behavior.* Decision Support Systems, 50 (1), 651-661.

8 Cotteleer, M. & Bendoly, E. (2006). *Order Lead-Time Improvement Following Enterprise Information Technology Implementation: An Empirical Study.* MIS Quarterly, 30 (3), 643-660.

9 Poston, R. & Grabski, S. (2001). *Financial impacts of enterprise resource planning implementations.* International Journal of Accounting Information Systems, 2 (2), 271-294.

10 Ranganathan, C. & Brown, C. (2006). *ERP investments and the market value of firms: Toward an understanding of influential ERP project variables.* Information Systems Research, 17 (2), 145-161.

11 Sneller, L. & Bots, J. (2009). *De Hagemeyer case: De invloed van ERP op de waarde van de onderneming.* Maandblad voor Accountancy en Bedrijfseconomie, 83 (4), 126-135.

12 Dehning, B., Richardson, V., Urbaczewski, A. & Wells, J. (2004). *Reexamining the value relevance of e-commerce initiatives.* Journal of Management Information Systems, 21 (1), 55-82.

13 Benzion, U., Tavor, T. & Vagil, J. (2010). *Information technology and its impact on stock returns and trading value.* International Journal of Finance and Economics, 15 (1), 247-262.

14 Tanriverdi, H. & Uysal, V. (2011). Cross-Business Information Technology Integration and Acquirer Value Creation in Corporate Mergers and Acquisitions. Information Systems Research, 22 (4), 703-720.

IT-governance wordt veelal gedefinieerd als het geheel van drie aspecten, namelijk organisatiestructuren, processen en leiderschap, dat ervoor zorgt dat IT de strategie en doelstellingen van de onderneming zowel ondersteunt als verder brengt. IT-governance wordt hierbij gezien als de verantwoordelijkheid van bestuur en management[15]. IT-governance specificeert het raamwerk van beslissingsbevoegdheden en bijbehorende verantwoordingsplichten om wenselijk gedrag bij de toepassing van IT te stimuleren[16]. Hieronder zullen we per aspect van IT-governance een kort overzicht geven van de betreffende literatuur.

*2.1.1. Organisatiestructuren*

In de literatuur wordt in het kader van IT-governance vooral aandacht besteed aan de organisatiestructuur op het niveau van bestuur en het aan het bestuur rapporterende management. Er moeten beslissingen worden genomen over de rol van IT voor de onderneming in relatie tot de strategie, over de techniek, over de toepassing van systemen en over de benodigde investeringen. Er worden diverse modellen onderscheiden voor de verdeling van het recht om deze beslissingen te nemen. Er kunnen drie modellen van uitersten worden onderscheiden. In het eerste model, de IT-alleenheerschappij, liggen alle beslissingsrechten bij de leiding van IT. In het tweede model, de business-alleenheerschappij, liggen deze volledig bij de leiding van omzet-verantwoordelijke divisies. In het derde model, de anarchie, liggen de beslissingsrechten bij de individuele gebruikers. In de praktijk komen vooral mengvormen voor. Hoewel algemene richtlijnen moeilijk te geven zijn, lijken bedrijven die het meest winstgevend zijn beslissingen centraal te nemen, en bedrijven die het snelst groeien beslissingen decentraal te nemen[17].

In de definitie van IT-governance is zeker plaats voor intern toezicht zoals een RvC dat op andere gebieden uitoefent. Echter, in de afgelopen jaren is de organisatie van beslissingsrechten zowel in literatuur als praktijk vooral uitgewerkt voor het uitvoerend niveau van organisaties, en is de rol van de RvC onderbelicht gebleven.

*2.1.2 Processen*

Voor de besturing van processen wordt in IT net als in andere vakgebieden veel gebruik gemaakt van raamwerken. Het bekendste raamwerk zijn de Control Objectives for IT, ofwel CobiT. De eerste versie van CobiT werd in 1996 uitgebracht. Het raamwerk wordt onderhouden door de internationale organisatie van IT auditors. In het raamwerk worden de 37 belangrijkste IT-processen in een organisatie in een vijftal domeinen opgedeeld. De eerste drie domeinen omvatten de strategische, tactische en operationele processen in IT. Een voorbeeld van een strategisch proces is *Manage portfolio*, waarin wordt bepaald op welke gebieden IT voor de organisatie wordt ingezet. Een voorbeeld van een tactisch proces is *Manage projects and programmes*, waarin wordt bepaald hoe projecten worden uitgevoerd. Een voorbeeld van een operationeel proces is *Manage service requests and incidents*, waarin de werking van de IT helpdesk bij vragen of verstoringen wordt ingevuld. Naast deze drie domeinen die vooral de uitvoering van IT betreffen, zijn er twee toezichtsdomeinen. Allereerst is er het domein van audit, met bijvoorbeeld het proces *Monitor, Evaluate and Assess the System of Internal Control*. Tot slot is er het domein van intern toezicht, waarbij

---

[15] IT Governance Institute. (2005). *Cobit 4.0; Control objectives, Management guidelines, Maturity models.* Rolling Meadows IL: IT Governance Institute.

[16] Weill, P. (2004). *Don't just lead, govern: how top-performing firms govern IT.* MIS Quarterly Executive, 3 (1), 1-17.

[17] Weill, P. & Ross, J. (2005). *A Matrixed Approach to Designing IT Governance.* MITSloan Management Review, 2005 (Winter), 25-34.

bijvoorbeeld het proces *Ensure Stakeholder Transparency* is toegevoegd. Dit laatste domein is overigens pas in de vijfde en meest recente versie van CobiT toegevoegd. Deze versie geeft aan dat er een groeiend besef in IT-governance is van het belang van intern toezicht op IT[18]. CobiT is veruit het meest gebruikte raamwerk voor IT processen. Toezichthouders als De Nederlandse Bank maken bij hun toezicht gebruik van CobiT. Dit wil niet zeggen dat er geen andere raamwerken bestaan, maar deze dekken vaak niet alle vijf door CobiT onderscheiden domeinen af. Bekende alternatieven voor CobiT zijn het ITIL service management raamwerk, dat vooral voor de IT-processen in de tactische en operationele domeinen van CobiT geschikt is, en de ISO27000 normen voor informatiebeveiliging in de strategische en operationele domeinen van CobiT. Door het vaststellen van het volwassenheidsniveau waarop deze raamwerken zijn geïmplementeerd, kan een organisatie een indruk krijgen van de mate van de beheersing en de proceskwaliteit.

CobiT vindt zijn oorsprong in de IT audit. In de nieuwste versie van het raamwerk is naast aandacht voor risico's verbonden met IT ook plek voor de kansen geboden door IT. Een illustratie hiervan is de toevoeging van een proces *Ensure Benefits Realisation* in het toezicht-domein van CobiT. Het raamwerk is echter nog steeds beter toegesneden op de risico's dan op de kansen van IT.

### *2.1.3. Leiderschap*

Door het toenemend belang van IT neemt ook de invloed en verantwoordelijkheid toe van diegene die in organisaties verantwoordelijk is voor de goede werking van IT. De laatste jaren wordt deze verantwoordelijkheid steeds vaker toevertrouwd aan een zogenaamde chief information officer, ofwel CIO. Zo'n veertig jaar geleden werd de term CIO voor het eerst gebruikt in de Verenigde Staten en sindsdien heeft de CIO zich een plek verworven die past in het rijtje van chief executive officer (CEO) en chief financial officer (CFO). Niet alleen in de VS, ook in Nederland zijn inmiddels vele CIO's werkzaam. Hoewel aan het leiderschap van IT natuurlijk niet alleen invulling wordt gegeven door de CIO, willen we ons hier wel beperken tot het beschrijven van deze rol.

De CIO handelt op bestuursniveau en is verantwoordelijk voor het inrichten van een optimale informatievoorziening en toepassing van IT, zodat de strategische doelen van de organisatie kunnen worden gerealiseerd. Naarmate er meer overeenstemming is tussen de CIO en het bestuur over de de rol van IT in een organisatie wordt de bijdrage van IT aan de realisatie van strategische doelstellingen groter[19]. Bij de invulling van een CIO-rol speelt altijd de vraag of de CIO een algemeen manager kan zijn of dat IT-kennis en -ervaring noodzakelijk zijn. Uit onderzoek naar de CIO-positie blijkt in elk geval dat zij over het algemeen hoog opgeleid zijn en lange ervaring hebben in het IT-werkveld. Wanneer de rol met meer aandacht voor de techniek wordt ingevuld is er een positieve invloed op de financiële prestaties van de onderneming.[20]

Met het toenemende belang van IT voor de bedrijfsvoering is het belangrijk dat de CIO goed samenwerkt met anderen in de organisatie. Regelmatig wordt gesuggereerd dat het voor een goede invulling van de CIO-rol belangrijk is dat de CIO direct aan de CEO rapporteert en dat

---

[18] ISACA. (2012). *Cobit 5: A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows, IL: ISACA.

[19] Preston, D. & Karahanna, E. (2009). *Antecedents of IS Strategic Alignment: A Nomological Network.* Information Systems Research, 20 (2), 159-179.

[20] Sobol, M. & Klein, G. (2009). *Relation of CIO background, IT infrastructure, and economic performance.* Information & Management, 46 (1), 271-278.

de CIO deel uitmaakt van het hoogste managementteam van de organisatie. Hierover kan geen algemeen geldende uitspraak worden gedaan. Onderzoek dat het bekende model van Porter koppelt aan de rapportagelijn van de CIO geeft het volgende aan: de CIO van een bedrijf dat productdifferentiatie als strategie heeft kan het beste rechtstreeks aan de CEO kan rapporteren, terwijl dat voor de CIO van een organisatie die kostenleiderschap nastreeft niet nodig is. Bedrijven die de rapportagelijn van de CIO op deze manier laten aansluiten bij hun strategie, hebben significant hogere aandelenrendementen en realiseren significant hogere kasstromen uit hun operatie.[21]

In onderzoek naar de CIO-rol wordt vooral aandacht besteed aan de positionering in of ten opzichte van het bestuur. Over de relatie tussen de CIO en de RvC en de informatie-uitwisseling over de IT functie is nog weinig onderzocht.

*2.2 De raad van commissarissen en IT*

Hierboven concluderen we dat in de IT-governance literatuur weinig is geschreven over de rol van de raad van commissarissen. In deze paragraaf bespreken we de aandacht die in de corporate governance-literatuur aan IT wordt geschonken.

In de algemene corporate governance literatuur wordt relatief weinig aandacht besteed aan het toezicht op IT. Wel vraagt de Monitoringcommissie Corporate Governance Code in het concept van de herziening van de code expliciet aandacht voor IT en technologie: voorgesteld wordt om aan de code toe te voegen dat ten minste één lid van de RvC beschikt over de specifieke deskundigheid inzake bestaande en toekomstige technologische innovatie en business modellen. De best practice om binnen het kader van risicomanagement het toezicht op de toepassing van informatie- en communicatietechnologie van de vennootschap bij de audit-commissie te beleggen blijft in de conceptcode gehandhaafd.[22]

De conceptcode bespreekt verder niet hoe de RvC zich zou moeten organiseren om het belang van de vennootschap zo goed mogelijk te dienen bij het toezicht op IT. Wij zien hiervoor vijf mogelijke vormen. Allereerst is het mogelijk om de portefeuille IT niet specifiek toe te wijzen. Wij vinden met de monitoringcommissie dat gegeven het belang van IT in de huidige tijd, deze vorm eigenlijk geen goede oplossing meer is. Ten tweede kan IT belegd worden in de audit-commissie; dit heeft als nadeel dat de nadruk blijft liggen op de risico's van IT, en dat de kansen van IT wellicht onvoldoende aandacht van de RvC krijgen[23]. Ten derde is het mogelijk om een externe deskundige als adviseur van de RvC aan te wijzen, zoals dat nu ook wel gebeurt voor heel specialistische zaken op het gebied van belastingen, integriteit of internetcriminaliteit. Dit is een mogelijkheid, maar heeft als nadeel dat de RvC gaat bouwen op het oordeel van een externe adviseur, die andere bevoegdheden,

---

[21] Banker, R., Hu, N., Pavlou, P. & Luftman, J. (2011). *CIO Reporting Structure, Strategic Positioning and Firm Performance.* MIS Quarterly, 35 (2), 487-504.

[22] Monitoringcommissie Corporate Governance Code. (2016). *De Nederlandse Corporate Governance Code Voorstel voor herziening Een uitnodiging voor commentaar.* (11 februari 2016) Den Haag: Monitoringcommissie Corporate Governance Code.

[23] Hadden, L. & Hermanson, D. (2005). *Is Your Audit Committee Watching IT Risks?* The Journal of Corporate Accounting and Finance, 14 (5), 35-39.

aansprakelijkheden en informatierechten heeft dan de RvC zelf, en mede daardoor een eenzijdige blik zou kunnen hebben vanuit de IT-invalshoek[24]. Deze eerste drie opties hebben dan ook niet onze voorkeur.

De vierde mogelijke vorm voor de organisatie van het toezicht op IT door de RvC wordt in de conceptcode geopperd: een commissaris met specifieke deskundigheid kan de IT-portefeuille op zich nemen. Hiermee wordt de RvC in elk geval een betere gesprekspartner voor het bestuur, en wij zien dit dan ook zeker als een relevante optie. De vijfde mogelijkheid is het vormen van een speciale commissie, die wij verder zullen aanduiden als de IT-commissie. Zowel het expliciet toewijzen van de IT-portefeuille aan één commissaris, als het vormen van een IT-commissie zien wij als valide opties voor de inrichting van het toezicht op IT. Aandachtspunt bij alle opties is de informatie uitwisseling over IT binnen de raad, zodat recht gedaan wordt aan de collectieve verantwoordelijkheid en borging van de besluiten.

### *2.3 De IT-commissie als onderdeel van de raad van commissarissen*

In Nederland is een IT-commissie als onderdeel van de raad van commissarissen een ongebruikelijke vorm, maar in het buitenland komen IT-commissies wel voor. Van de bedrijven die in 2007 deel uitmaakten van de S&P 500 hadden er achtentwintig een dergelijke IT-commissie; deze bedrijven hadden een betere rendement op eigen vermogen en activa dan vergelijkbare bedrijven zonder IT-commissie [25] Van de driehonderd grootste beursgenoteerde bedrijven in Australië kenden er in 2010 acht een IT-commissie; deze bedrijven rapporteren beter over bedrijfsrisico's dan de bedrijven die niet een dergelijke commissie hebben.[26]

Richard Nolan, lid van de IT-commissies van de Amerikaanse bedrijven Fedex en Novell[27], ziet als belangrijkste rol van een dergelijke commissie het op gang houden van het voortdurende gesprek tussen top management en de IT-functie. Of een dergelijke commissie nodig is hangt af van de industrie waarin de onderneming werkzaam is. Onderwerpen van gesprek zouden moeten zijn: het beheren van de IT-activa, de strategie, kwaliteit van de dienstverlening, juridische aspecten en het voorkomen van onplezierige verassingen, en de werkwijze van commissie zou vergelijkbaar moeten zijn aan die van de audit-commissie. Als leden noemt Nolan in elk geval de CIO van het bedrijf, algemeen management- en IT consultants. Nolan ziet ook twee potentiële nadelen van een IT-commissie. Ten eerste kan de commissie gaan dienen als een excuus voor een gebrek aan inzicht in IT bij de hele RvC. Ten tweede kan de commissie zo dicht op de operatie gaan zitten dat zij de uitvoering gaat overnemen[28].

## 3. Uit de praktijk van het toezicht op IT

---

[24] Kantz, E. (2014). *Considerations in Drafting Board Advisor Arrangements.* Business Law today, 2014 (4), 1-4.

[25] Premuroso, R. & Bhattacharya, S. (2007). *Is There a Relationship between Firm Performance, Corporate Governance, and a Firm's Decision to Form a Technology Committee?* Corporate Governance: An International Review, 15 (6), 1260-1276.

[26] Buckby, S., Gallery, G. & Ma, J. (2015). *An analysis of risk management disclosures: Australian evidence.* Managerial Auditing journal, 30 (8/9), 812-869.

[27] Hoffman, T. (2004). *IT Oversight Gets Attention At Board Level.* Computerworld, 38 (20), 1-3.

[28] Nolan, R. (2004). *A committee of one's own.* CIO Insight, 2004 (2), 34-42.

Uit de inleiding blijkt een toenemend belang van de rol van de RvC bij het toezicht op IT. De literatuur geeft echter weinig aanknopingspunten voor de organisatie van dit toezicht. Om die reden hebben wij een aantal interviews gehouden met ervaringsdeskundigen. In deze paragraaf geven wij eerst een aantal kenmerken van de geïnterviewden, de rollen die zij in het toezicht op IT spelen of hebben gespeeld, en de organisaties waar zij hun ervaring hebben opgedaan. Daarna vatten wij aan de hand van een aantal thema's hun ervaringen samen.

### *3.1 De geïnterviewden*

In de maanden mei en juni 2016 hebben wij interviews uitgevoerd met een viertal mensen die betrokken zijn bij het toezicht op IT. In Tabel 1 staat aangegeven welke rollen de geïnterviewden spelen of hebben gespeeld in het toezicht, en in welke sectoren van de economie deze ervaring is opgedaan. De geïnterviewden zijn geselecteerd uit ons persoonlijke netwerk.

Tabel 1: Profiel van de geïnterviewden

| | Ervaring als: | | | Ervaring in: | | |
|---|---|---|---|---|---|---|
| | lid raad van commissarissen | lid raad van bestuur | chief information officer | publieke sector | semi-publieke sector | private sector |
| Geïnterviewde 1 | X | X | | | X | |
| Geïnterviewde 2 | X | | X | X | X | X |
| Geïnterviewde 3 | | | X | X | | X |
| Geïnterviewde 4 | X | | X | X | X | X |

De interviews zijn uitgevoerd door twee van de drie auteurs van dit hoofdstuk. Ieder interview duurde ongeveer een uur. De interviews waren semigestructureerd aan de hand van een vragenlijst. De interviews zijn opgenomen en woord voor woord uitgewerkt. Het transcript is op basis van thema's geclassificeerd. Per thema zijn citaten uit de interviews geselecteerd. De geselecteerde citaten zijn geanonimiseerd. Aan de geïnterviewden is toestemming gevraagd voor het publiceren van de geanonimiseerde citaten.

### *3.2 Het belang van IT voor de organisatie*

Wanneer we vragen naar het belang van IT voor de organisaties waar de geïnterviewden bij betrokken zijn dan neemt dat in de toekomst toe:

[G4] Ja, ik denk aan beide kanten, zowel overheid als bedrijfsleven, dat een sterk toenemende rol, je kunt bijna geen veranderingsinitiatief meer uitvoeren zonder dat IT daar een component of een zeer belangrijk deel van is. […] Of zelfs een randvoorwaardelijke component. En dat geldt zowel voor overheid als het bedrijfsleven.

[G1] En als we dat als [*organisatie*] niet op orde hebben, dan *doe* je straks geen logistiek meer. Zonder IT, was één van mijn slogans, geen logistiek. *Nu* snapt iedereen dat, maar toen we daar vier jaar geleden mee begonnen, was dat redelijk baanbrekend.

[G3] Mijn opdracht is om de IT op een hoger plan te brengen, dat het niet alleen facilitaire dienstverlening is, maar ook daadwerkelijk businessprocesverbetering….

Het belang van IT voor de organisatie zoals die er vandaag is verschilt. Sommige organisaties zien zichzelf al als een IT-bedrijf:

[G2] Nou ja, cruciaal, omdat we eigenlijk een dataprovider zijn, dus eigenlijk wat wij doen is data verzamelen. […] Dat is eigenlijk allemaal IT, dus wat moeten we als IT betekenen, uiteindelijk dat onze klant any information, any device, anywhere, any dimension kan krijgen, en daar heb je dus heel veel IT voor nodig,

Bij anderen is IT op dit moment nog geen primair proces:
[G3] We zitten nog erg in het facilitaire diensten denken, echter het toenemend belang van IT op de primaire processen wordt onderkend....

Hoe het belang dat de raden van commissarissen hechten aan IT zich verhoudt tot de agenda van de raad verschilt:
[G1] Dus die IT-component is zo van belang, daar moet je echt aandacht aan besteden want anders mis je straks ergens de boot. Dat bevestigt dus, dat IT ook gaat neerslaan in raden van commissarissen.
[G2] Dan is er heel lang over de finance, en terecht natuurlijk, gesproken, en dan mag je als CIO komen, maar ja, dat was gepland om elf uur, en om twee uur wordt je gebeld, en eigenlijk zo van met de mededeling: je hebt eigenlijk nog tien minuten, hahaha…

*3.3 Organisatie van het toezicht op IT*

In paragraaf 2.2 benoemen we op basis van de literatuur vijf mogelijke vormen voor de organisatie van het toezicht op IT. In de interviews komen we deze vormen stuk voor stuk tegen. In sommige organisaties is de portefeuille niet specifiek belegd:
[G3] De organisatie zit nog aan het begin van de IT-Governance leercurve… Dat betekent dat er nog niet specifiek een IT-portefeuille is toegekend, voor zover ik het kan overzien…

In andere organisaties wordt IT in de audit-commissie besproken:
[G4] Verwijzen naar de audit-commissie, en zeggen: ja, maar risicomanagement zit al in de audit-commissie, dan moet IT daar toch besproken worden, dus ik zie allerlei bewegingen… In de zin van men blijft daar liever wat van weg.

Ook is er wel sprake van portefeuillehouders:
[G2] Er is nu één lid van de RvC die heeft IT in de portefeuille…

Externe toegevoegde deskundigen worden op het gebied van IT ook wel ingezet:
[G4] Nou, dat, nee, dat heb ik niet als zodanig geformaliseerd gezien, er waren wel twee tot drie keer per jaar zelfs, gesprekken met de vertegenwoordigers vanuit RvC, RvB, CIO, en enkele […] toegevoegde deskundigen […] Waarbij ik in eerste instantie dacht als het een beetje ingewikkeld wordt dan gaat men naar de externe toegevoegde deskundigen kijken, in de trant van: “dat doen jullie wel”, maar die tijd is inmiddels wel voorbij.

Tot slot is bij één organisatie een IT-commissie opgericht:
[G1] En dat technical comité, dat geeft de hele vergadering wel rust, als je weet, want daar zitten we hier voor, met name op IT, dus zowel op de vernieuwing, de verandering, wat komt er op je af… […] Houd je je bedrijfsvoering goed, houd je je kosten op orde, heb je wel de juiste technische kennis voor dit soort technieken in huis, dat geeft een RvC-vergadering heel veel rust en ook verbetering. Verder blijkt dat de directie toch wel blij is, dat ze nu adviezen en raad en daad krijgen van iemand die er even

buiten staat, want ze zijn in hun eigen wereld toch heel erg bezig, met ik zou bijna zeggen, overleven.

Een mogelijk nadeel van een dergelijke commissie wordt ook onderkend:

[G1] De verleiding is groot, met name ook voor de twee commissarissen, om dan de diepte in te gaan, dat is natuurlijk toch nogal technisch gedreven, dus die denken wacht eens even, ben ik nu in m'n adviseursrol bezig, of in m'n toezichtrol. […] Maar eigenlijk, het is niet anders dan in je auditcommittee. Daar heb je precies hetzelfde, ga je op de stoel van de CFO zitten, of blijf je in je toezichtrol, ,het is niet wezenlijk anders, alleen omdat het techniek is, en we natuurlijk allemaal dat leuk vinden, ben je geneigd om daar wel eens wat te diep in te gaan. En soms moet dat ook.

Maar over het algemeen wordt de commissie in deze organisatie erg gewaardeerd:

[G1] Het geeft mij ontzettend veel rust dat ik nu weet, dat daar een IT-committee op zit en daar de directie frequenter op bevraagt.

Andere geïnterviewden spreekt het idee van een IT-commissie waarin ook innovatie wordt belegd erg aan:

[G2] Maar waar is de connectie met de supervisory board, die is er dus niet. Ik vind dat idee van een innovation comité eigenlijk ook wel heel erg goed.

*3.4 De informatie-uitwisseling*

De frequentie en de structuur van informatie-uitwisseling verschilt per organisatie, maar ook per onderdeel van de RvC:

[G2] De audit comité, is natuurlijk heel erg gestructureerd. […] Eerst rapporteert internal audit over de IT-bevindingen en ik rapporteer over de grote innovatieprojecten die er lopen. Nou, als je het binnen de RvC doet, dan is er gewoon belangstelling. […] Maar daar dus geen formele agenda, dat is meer vanuit mijzelf gedreven. De audit comité kent wel een veel vaster stramien.

[G3] We hebben een reporting schedule opgebouwd van CIO naar de CFO […] waar hij uit kan putten, in zijn rapportage aan de RvC.

In hun rol van toezichthouder noemen de geïnterviewden de behoefte aan informatie over de strategie en de lange termijn:

[G4] Daar wil ik het hebben over het meerjareninformatieplan, […] want dat is voor mij […] het handvat, de leidraad en de inhoud, om toch naar voren te kunnen kijken en daar de discussie over te voeren.

[G1] Zijn jullie wel alert genoeg op de nieuwe ontwikkelingen, ja daar zijn we mee bezig. OK, als commissarissen werden we geinformeerd in de volgende vergadering, en eigenlijk, als ik terugkijk, hebben we dat daar te weinig bovenop gezeten. […] Zowel als directie als als commissarissen. En daardoor hebben we gezegd: we moeten ons been weer bijtrekken op de techniek.

*3.5 De rol van de CIO*

De geïnterviewden die zelf CIO zijn geweest hebben een heldere mening over de relatie die de RvC zou moeten hebben met de CIO:

[G4] In het verlengde daarvan vind ik ook dat een toezichthoudend orgaan gewoon moet eisen dat ze tenminste één keer per jaar ook met de CIO aan tafel zitten. Uiteraard

prima wanneer de directie, of de raad van bestuur daar bij zit, maar een discussie met de CIO dient plaats te vinden met de voltallige RvC of RvT.

[G3] Dus dat was bijzonder prettig, wat je zag ontstaan is een setting, met de RvB en de RvC. […] Er ontstond een goede, inhoudelijke dialoog tussen de CIO en de RvC, waarbij de RvB aanvankelijk aandachtig luisteraar was, maar er geleidelijk een goede dialoog tussen CIO-RvB-RvC ontstond. Daarmee was het dus niet zo dat de raad van bestuur namens mij de discussie voerde.

[G2] Of ik meld mezelf weer aan, goh, ik ben een half jaar niet geweest, misschien is het goed dat ik weer wat vertel….

Ook contacten buiten de vergadering om worden aangeraden, mits een terugkoppeling aan bestuurders en commissarissen volgt:

[G4] En aan de hand daarvan kun je zeggen: we willen op een aantal onderwerpen nog een keer wat dieper ingaan met de CIO, en dat doen dan één of twee mensen uit de RvC , die daarover weer terugkoppelen aan de hele RvC.

[G3] Dus ik ga ervan uit dat een commissaris zijn eigen netwerk opbouwt binnen het bedrijf vanuit zijn eigen verantwoordelijkheid. […] En dan is het logisch, wanneer een commissaris mij vragen stelt, dat ik netjes antwoord geef, maar dat ik wel mijn portefeuillehouder op de hoogte stel van het hele verhaal…

## 4. Conclusie en aanbevelingen

Met het toenemende belang van IT voor alle aspecten van de bedrijfsvoering neemt ook het belang van het intern toezicht op IT toe. Dit betekent dat iedere RvC in de komende jaren het toezicht op IT zal moeten gaan inrichten of versterken. Het toezicht op de operationele risico's van IT moet worden uitgebreid met het toezicht op de strategische kansen van IT. Hierbij kunnen commissarissen zich in elk geval afvragen hoe zij dit toezicht kunnen organiseren, welke informatie-uitwisseling zij nodig hebben, en hoe zij contact onderhouden met de CIO.

Op basis van een klein onderzoek onder vier mensen die meerdere functies in het toezicht op IT vervullen of hebben vervuld, aangevuld met onze eigen inzichten en ervaringen, formuleren wij een aantal aanbevelingen. Het toezicht op IT kan door de RvC op een aantal manieren georganiseerd worden. Ons kleine praktijkonderzoek levert in elk geval de volgende aanbevelingen op:

- Benoem vooruitlopend op de best practice van de conceptcode Corporate Governance expliciet een portefeuillehouder IT
- Vul het toezicht op de risico's van IT aan met toezicht op de kansen van IT; beleg het toezicht op de kansen van IT niet als vanzelfsprekend in de audit-commissie
- Overweeg of de vorming van een IT-commissie passend is voor de organisatie

Verder verdient de informatievoorziening van de RvC en informatie-uitwisseling tussen de RvC en andere interne partijen aandacht. Uit ons praktijkonderzoek blijkt over het algemeen dat de informatie-uitwisseling zowel in frequentie als in inhoud weinig gestructureerd is. De vraag is of dit strookt met het toenemend belang van IT. Wij raden aan om in elk geval op gestructureerde wijze aandacht te schenken aan de strategische aspecten van IT.

Tot slot raden wij op basis van ons kleine praktijkonderzoek aan om de relatie tussen de RvC en de CIO te verstevigen. Uit academisch onderzoek blijkt dat naarmate er meer overeenstemming is tussen de CIO en het bestuur over de de rol van IT in een organisatie, de

bijdrage van IT aan de realisatie van strategische doelstellingen groter ook groter wordt. De CIO's in ons onderzoek zien ook voordelen in een betere relatie met de commissarissen. Wij verwachten dat het toezicht op IT aan effectiviteit wint, wanneer de relatie tussen de RvC en de CIO hechter wordt.

Toezicht op IT is een relatief nieuw werkveld. De effectiviteit van dit toezicht, en mate waarin deze beïnvloed wordt door de organisatievorm van dit toezicht en de informatie-uitwisseling is nog weinig onderzocht. Wij vinden dit interessante en belangrijke onderzoeksgebieden, en we willen daar in de komende jaren dan ook verder aan werken. Dit hoofdstuk is daarbij een eerste kleine stap.