Inhoudsopgave

Inleiding

In het verleden stond het onderwerp informatietechnologie, of kortweg IT, niet helemaal bovenaan de agenda van de raad van commissarissen in ondernemingen. IT is nu echter direct van invloed op de relatie tussen de onderneming enerzijds en stakeholders als klanten, leveranciers, medewerkers, banken, de belastingdienst, externe toezichthouders en het algemeen publiek anderzijds. Ook kan een goede inzet van IT het verschil maken op de markt en kan een storing in IT van directe invloed zijn op de continuïteit van de onderneming. Verder ontstaat er rondom IT een steeds strakker wettelijk kader, waardoor compliance een steeds groter punt van aandacht wordt. Het is dan ook onontkoombaar dat IT een prominente plaats krijgt in het werk van de commissaris[1].

Voor veel commissarissen is het toezicht op IT een nieuw terrein. Goed toezicht begint veelal met het formuleren van goede vragen. De vraag is immers het belangrijkste middel van de commissaris in de dialoog met het bestuur van de onderneming. Daarom staat de vraag centraal in dit boek.
Allereerst wordt aandacht besteed aan het formuleren van vragen. In het eerste hoofdstuk van het boek worden voor dit doel de belangrijkste algemene en IT specifieke raamwerken voor risicomanagement en interne beheersing gepresenteerd. Deze raamwerken delen het brede IT werkgebied op in deelgebieden die gerichte vragen mogelijk maken.
Op basis van deze raamwerken zijn zeven vragen geformuleerd die aansluiten bij de rol van de commissaris in het toezicht op IT. Ieder van de zeven vragen wordt vervolgens in een apart hoofdstuk behandeld. In elk hoofdstuk wordt aangegeven

[1] In het boek worden de termen *commissaris* en *onderneming* gebruikt waar respectievelijk eigenlijk *commissaris, lid raad van toezicht, lid raad van advies of andere interne toezichthouder* en *onderneming of andersoortige organisatie* zou moeten staan. Dit is alleen om de tekst beknopt en leesbaar te houden. Toezicht op IT is zeker ook van groeiend belang voor toezichthouders in andersoortige organisaties. Zowel in de private als in de publieke sector wordt IT een steeds belangrijker en omvangrijker onderdeel van het toezicht.

waarom de vraag van belang is voor het toezicht. Daarna wordt een voorbeeld gegeven van een onderneming waarbij de vraag aan de orde is geweest. Tot slot wordt een aantal mogelijke vervolgvragen besproken. Omdat de vragen gebaseerd zijn op algemeen bekende raamwerken sluit het boek op deze manier aan bij de praktijk zonder de theorie uit het oog te verliezen.

Zoals gezegd staan in dit boek zeven vragen centraal. Wie in dit boek het enige juiste antwoord op de zeven vragen denkt te vinden komt helaas bedrogen uit. Bij de voorbeelden worden wel oplossingsrichtingen gegeven, maar die zijn afhankelijk van de geschetste situaties en zeker niet algemeen toepasbaar. Voor het IT werkgebied geldt hetzelfde als voor de rest van het werk van de commissaris: als eenvoudige en eenduidige antwoorden voorhanden zouden zijn zou aandacht van de commissaris niet nodig zijn.
Ook de lezer die verwacht dat met zeven vragen het IT werkgebied in de onderneming volledig is afgedekt zal waarschijnlijk worden teleurgesteld. De vragen zijn weliswaar zo gekozen dat ze voor de meeste ondernemingen relevant zullen zijn, maar omdat iedere onderneming uniek is, zal de commissaris ook eigen vragen willen formuleren. De gepresenteerde raamwerken bieden aanknopingspunten voor het formuleren van een scala aan ondernemingsspecifieke vragen.
De vraag staat centraal in dit boek, maar dit boek is nadrukkelijk niet bedoeld als de weg naar het enige juiste antwoord. De vraag wordt in dit boek gezien als een startpunt voor dialoog, verdieping en verbetering.

Dit boek is geschreven om commissarissen voor wie IT een relatief onbekend terrein is in staat te stellen een goed eerste inzicht te ontwikkelen in de IT van de onderneming. Ook kan het boek worden gebruikt door commissarissen die zich bij aanvaarding van een nieuw commissariaat een beeld willen vormen over de stand van zaken rondom IT bij de onderneming.

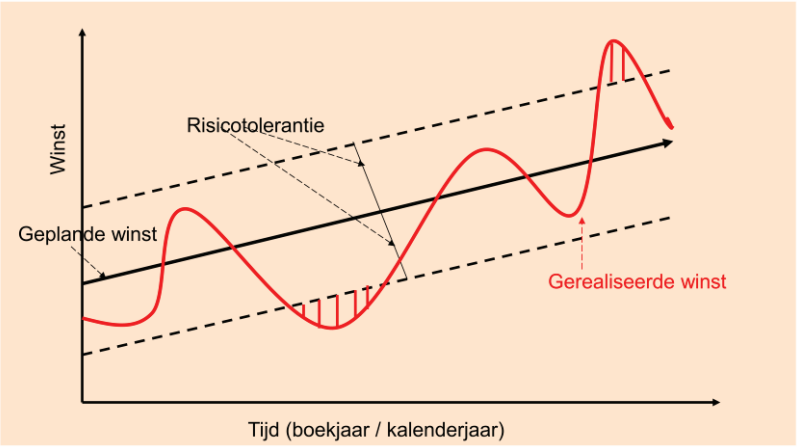
Ik heb met veel plezier aan dit boek gewerkt. IT is fascinerend, zowel in de theorie als in de praktijk, en IT biedt kansen in alle facetten van ons dagelijks leven. Inspiratie voor het schrijven dit boek heb ik van veel kanten gekregen, maar misschien wel het meest van de deelnemers van de diverse groepen van de Nyenrode Commissarissencyclus, waar de zeven vragen diverse malen aan de orde zijn gekomen. Daarnaast ben ik dank verschuldigd aan ing. Ries Bode, drs. ir. Michiel van de Duin en prof. dr. Fieke van der Lecq voor hun waardevolle commentaar op de conceptversie van dit boek.

Ik hoop dat de lezer ook plezier beleeft aan het lezen van dit boek en dat het een nuttige bijdrage levert aan het verder professionaliseren van het toezicht op IT in ondernemingen. Natuurlijk ben ik bereid om over de inhoud van dit boek van gedachten te wisselen.

Lineke Sneller
l.sneller@nyenrode.nl
april 2016

INLEIDING

Commissarissen en andere toezichthouders moeten beoordelen of de onderneming waarop zij toezicht houden *in control* is. Wat dit betekent, wordt geïllustreerd aan de hand van een voorbeeld in Figuur 1. In de figuur worden de geplande en gerealiseerde prestaties van een onderneming in beeld gebracht. Bij wijze van voorbeeld wordt in de figuur de winstontwikkeling gehanteerd, maar een soortgelijke figuur zou getekend kunnen worden voor andere operationele of financiële doelstellingen van de onderneming.



Figuur 1: Risicotolerantie en in control zijn. *Bron:* Paape [2008]

De geplande winstontwikkeling wordt in de figuur weergegeven door de zwarte pijl. Veelal zal het bestuur van de onderneming deze geplande winstontwikkeling jaarlijks voorafgaand aan een nieuw boekjaar of kalenderjaar voorleggen aan de raad van commissarissen.

Gedurende het jaar wordt er winst gerealiseerd. Omdat de werkelijkheid zich nooit helemaal volgens plan ontwikkelt, zal de winstrealisatie afwijken van het budget. In de figuur wordt de gerealiseerde winst weergegeven door de rode lijn. Om te kunnen