Voorwoord

Voor u ligt de tweede editie van het Handboek compliance in de zorg. De eerste druk heeft zijn waarde voor de praktijk ruimschoots bewezen, maar aangezien de zorgsector zeer dynamisch is, zeker ook qua regelgeving, werd het tijd voor een geheel herziene tweede editie. Zeker op het terrein van privacy (introductie van de GDPR) en governance (introductie van de nieuwe Code) was een update zeer gewenst.

Naast een breed scala aan onderwerpen die ook reeds in de eerste editie aan bod kwamen (van ethiek tot aan financiering en van mededinging in de zorg tot aan bezoldiging) is de tweede editie uitgebreid met hoofdstukken over eHealth, crisiscommunicatie en een praktisch hoofdstuk over de kwaliteit van zorg. Alle aspecten van compliance in de zorg zijn op een systematische wijze bijeengebracht, beschreven en praktisch toegankelijk gemaakt voor allen die werken in de zorgsector, ongeacht hun rol of functie.

Als voorzitter van het zorgteam van Loyens & Loeff zie ik dat de transitie naar marktwerking in de zorg ertoe heeft geleid dat onze betrokkenheid in de zorgsector de laatste jaren sterk is toegenomen. Nieuwe wet- en regelgeving leidt tot veel dynamiek en een keur aan vragen en zaken. Dit is voor ons reden geweest om een aantal jaar geleden alle kennis en expertise te bundelen in een geïntegreerd team van circa veertig advocaten, notarissen en fiscalisten dat '*dedicated*' werkt in de zorgsector.

Het handboek heeft zijn weg inmiddels gevonden in het onderwijs. Zo is het boek voorgeschreven bij de Grotius-specialisatieopleiding Gezondheidsrecht, waar auteurs prof. mr. dr. dr. Jaap Sijmons (Nysingh advocaten) en mr. dr. Marc Wiggers (Loyens & Loeff) tevens als hoofddocent aan verbonden zijn (samen met prof. mr. dr. Aart Hendriks, Universiteit Leiden). Daarnaast is het handboek voorgeschreven voor de Registeropleiding Compliance Officer in de Zorg. Deze opleiding wordt verzorgd door opleidingsinstituut Meer Kennis en Boerhaave Nascholing van het LUMC. Veel leden van ons Zorgteam zijn als docent betrokken bij deze opleiding.

Wij merken dat indien een organisatie 'compliant' wil zijn, er gewoon hard gewerkt moet worden. Door mensen die op alle niveaus in de zorg werkzaam zijn, van de zorgprofessional aan het bed tot de zorgbestuurder. Mensen die in hun werkzaamheden aanlopen tegen de noodzaak om diverse belangen en waarden tegen elkaar af te wegen en tegen regels die niet altijd even duidelijk zijn. Compliance is dan ook veel meer dan het mechanisch afvinken of aan de toepasselijke regels is voldaan. Juist omdat er sprake is van 'mensenwerk', is het goed om te kijken hoe anderen het doen. Het handboek speelt hierop in. Theorie wordt namelijk afgewisseld met praktische interviews met zorgprofessionals. Daarbij verstrekken de auteurs imple-

mentatietips (*do's and don'ts*) en concrete inspiratieparagrafen voor het opstellen van een complianceprogramma aan het einde van vrijwel ieder hoofdstuk, waardoor het handboek u direct toepasbare handvatten biedt om uw complianceprogramma op te stellen, te verbeteren of uit te breiden.

Het handboek is tegelijkertijd diepgaand. Mr. dr. Marc Wiggers en prof. mr. dr. Wilco Oostwouder hebben als redactie deskundigen bereid gevonden om bijdrages te leveren. Alle auteurs behoren stuk voor stuk tot de Nederlandse top en het is zeer bijzonder dat al hun expertise in een handboek is gebundeld.

Het is kortom (wederom) een prachtig, innovatief handboek geworden dat ik u van harte kan aanbevelen!

Mr. drs. T.R.M van Helmond, voorzitter Zorgteam Loyens & Loeff

Hoofdstuk 1

Inleiding Handboek compliance in de zorg

Prof. mr. dr. W.J. Oostwouder en mr. dr. M.Ph.M. Wiggers*

1.1 De aanleiding

Diverse zorginstellingen (inclusief ziekenhuizen) zijn negatief in het nieuws gekomen door deconfitures en schandalen die veroorzaakt zijn door een slechte governance en/of een slechte naleving van regelgeving. Het meest bekend zijn Meavita, Slotervaart, de IJsselmeerziekenhuizen en het Ruwaard van Putten Ziekenhuis. Deze gevallen vormen echter het topje van de ijsberg. Het belang van een goede controle op de naleving van normen en waarden bij zorginstellingen (*compliance*) is evident.
Binnen zorginstellingen is er een grote behoefte aan een naslagwerk dat voor en ook met input van sleutelfiguren uit verschillende geledingen van de zorgsector geschreven is.
De tweede druk van het handboek op dit gebied ligt nu voor u! Wij zijn alle auteurs bijzonder erkentelijk voor hun bijdragen en Uitgeverij Paris voor het stimuleren om tot een tweede druk te komen.

1.2 De wijze van totstandkoming van (de tweede druk van) dit handboek

Marc Wiggers, partner bij Loyens & Loeff en in 2013 gepromoveerd op het onderwerp 'De ACM en de *NZa* in de curatieve zorgsector', en Wilco Oostwouder, hoogleraar Bedrijfsfinancieel recht aan de Universiteit Utrecht en advocaat bij Loyens & Loeff, hebben in 2014 het initiatief genomen zo'n handboek te redigeren (en deels zelf te schrijven) dat de gehele zorg bestrijkt.
Op dit initiatief is enthousiast gereageerd door een keur aan experts op het gebied van regelgeving en compliance die de hoofdstukken (mede) voor hun rekening hebben genomen.
De eerste druk van dit handboek verscheen in 2016. Het handboek heeft inmiddels zijn weg in de praktijk gevonden en was voorgeschreven literatuur bij de Grotius-opleiding Gezondheidsrecht van de Radboud Universiteit Nijmegen edities 2016-2018 en de Registeropleiding Compliance Officer in de Zorg, die door Meer Kennis in samenwerking met Boerhaave Nascholing van het Leids Universitair Medisch Centrum (LUMC) en Loyens & Loeff in 2016 en 2018 is georganiseerd.
De ontwikkelingen binnen (de regelgeving die betrekking heeft op) de zorg gaan snel. Zo snel dat binnen drie jaar na het verschijnen van de eerste druk een tweede druk van dit boek door de redacteuren noodzakelijk werd geacht. Enkele opvallende nieuwe ontwikkelingen zijn: (1) de introductie van de Code Zorg 2017 (die de

* Wilco Oostwouder is hoogleraar Bedrijfsfinancieel recht aan de Universiteit Utrecht en advocaat bij Loyens & Loeff. Marc Wiggers is advocaat en partner bij Loyens & Loeff.

Zorgbrede Code uit 2010 heeft opgevolgd); (2) het op 25 mei 2018 van kracht worden van de Algemene Verordening Gegevensbescherming en (3) de snelle opkomst van eHealth. Deze ontwikkelingen zijn respectievelijk in de hoofdstukken 'Governance in de zorg' (hfdst. 3), 'Privacy' (hfdst. 8) en 'eHealth' (hfdst. 10) verwerkt.

1.3 De hoofdstukken

Ten opzichte van de vorige druk bevat de tweede editie drie hoofdstukken die geheel nieuw zijn ten opzichte van de vorige druk. Dit betreft de hoofdstukken 'Kwaliteit van zorg: meten en leren' (hfdst. 7), 'eHealth' (hfdst. 10) en 'Crisiscommunicatie' (hfdst. 11).
Bij het hoofdstuk 'Ethiek en een open compliancecultuur' (hfdst. 4) is alleen de titel gehandhaafd en het mooie interview met Marcel Canoy en Jonathan Soeharno vervangen door een systematisch geschreven tekst van de hand van Martine de Vries, hoogleraar Normatieve aspecten van geneeskunde bij het LUMC en Esther Oldekamp, docent onderzoeker Gezondheidsrecht bij het LUMC.
De inhoudelijke hoofdstukken van dit handboek zijn niet alleen theoretisch goed onderbouwd, maar ook praktisch ingestoken door daarin praktijkcases, inspiratieparagrafen en 'do's and don'ts' op te nemen. Het boek geeft daarmee uitdrukkelijk niet alleen handvatten voor kennisverdieping, maar ook voor de implementering van een (uitgebreider) complianceprogramma.
Het handboek bevat drie onderdelen waarin de diverse inhoudelijke hoofdstukken zijn ondergebracht.

Deel 1 *Compliance in de praktijk* bestaat, naast deze inleiding, uit *hoofdstuk 2* dat gaat over compliance in de praktijk.
In onderdeel 1 van hoofdstuk 2 gaat Ronald Notermans, partner bij NUX Compliance Consultancy, in op de 7 stappen die moeten leiden naar een effectief complianceprogramma. Hij schetst daarbij de verhouding tussen governance en risicomanagement en methoden om met risico's om te gaan. Vervolgens beantwoordt hij de vraag waar compliance in dit geheel past en geeft hij aan uit welke elementen een goed, effectief complianceprogramma bestaat. Daarna behandelt hij de wijze waarop de effectiviteit van zo een programma wordt geijkt. Ten slotte wordt in dit hoofdstuk het belang geschetst van een open meldcultuur en professionele onderzoeken alsmede aangegeven hoe een adequate organisatie de compliancefunctie actueel houdt. Dit is in de zorgsector lastig, omdat deze wordt geconfronteerd met voortdurend wijzigende regelgeving.
In onderdeel 2 van dit hoofdstuk behandelt Jan Cuppen, partner bij CILUX Compliance Consultancy, het onderwerp 'Compliance en integriteit in de energiesector'. Het energielandschap en de daarbij behorende regelgeving zijn het laatste decennium vanwege de liberalisering van de energiemarkt ingrijpend veranderd. In dit hoofdstuk worden ook voor de compliance in de zorg nuttige conclusies getrokken uit en tips gegeven op basis van tien jaar compliance en integriteit in de energiesector. Eén van de lessen is dat alles staat of valt bij een goede '*tone at the top*'. Er moet dus in de eerste plaats sprake zijn van een goed ondernemingsbestuur.
In onderdeel 3 van dit hoofdstuk geven Sarah Beeston en Nina Korstenbroek, advocaten bij Van Doorne, aan hoe compliance in de dagelijkse zorgpraktijk verankerd kan worden. Zij beschrijven de werking van een compliancecyclus die hiervoor

essentieel is. Zij merken op dat een voorwaarde voor de goede werking hiervan is dat bestuurders (samen met een complianceprofessional) de risico's in hun organisatie herkennen, benoemen en de juiste beheersingsmaatregelen nemen.

Deel 2 *Governance, ethiek en bezoldiging in de zorg* bestaat uit drie hoofdstukken: 'Governance in de zorg', 'Ethiek en een open compliancecultuur' en 'Bezoldiging, medezeggenschap en cliëntenraden in de zorg'.
In *hoofdstuk 3* gaan Frank Leijdesdorff, partner bij Loyens & Loeff, Lara Haanraadts, advocaat bij Loyens & Loeff en Wilco Oostwouder, allereerst in op het begrip 'governance' en schetsen de plaats daarvan in de voor de zorg geldende regelgeving. Aan de hand van praktijkvoorbeelden wordt aangegeven hoe de governance van een zorginstelling binnen de reguliere bedrijfsvoering, maar ook bij veranderingsprocessen zou moeten werken.
Hoofdstuk 4 is geschreven door Martine de Vries en Esther Oldekamp. Zij gaan daarbij in op de kern van de begrippen 'compliance' en 'ethiek', en bespreken zij hoe compliance zich tot de ethiek verhoudt. Voorts bespreken zij een aantal uitdagingen voor het complianceproces. Daarbij gaat het met name om uitdagingen op het gebied van het creëren van een veilige en open werkcultuur in een zorginstelling. In *hoofdstuk 5* schetsen Maureen te Poel, advocaat bij Loyens & Loeff, Arthur Hol, partner bij De Koning Vergouwen Advocaten en programmadirecteur bij de Governance University, en Wilco Oostwouder het regelgevend kader ten aanzien van de medezeggenschap van werknemers en cliënten alsmede ten aanzien van het issue 'bezoldiging van topfunctionarissen'. Aan de hand van voorbeelden worden vervolgens praktische tips gegeven om problemen op deze gebieden op te lossen.

Deel 3 *Zorgregulatoire compliance en extern toezicht* omvat zes hoofdstukken: 'Compliance en toezicht op kwaliteit en patiëntveiligheid in de zorg', 'Kwaliteit van zorg: meten en leren', 'Privacy', 'Mededinging in de zorg', 'eHealth' en 'Crisiscommunicatie'.
In *hoofdstuk 6* gaat Jaap Sijmons, hoogleraar Gezondheidsrecht aan de Universiteit Utrecht en partner bij Nysingh, in op de onderwerpen compliance en toezicht op kwaliteit en de patiëntveiligheid. Deze onderwerpen hebben betrekking op het hart van de zorgverlening. In dit hoofdstuk wordt een antwoord gegeven op de vraag welke normen, systemen en toezicht de kwaliteit en de veiligheid bewaken. Vervolgens wordt aangegeven op welke wijze de kwaliteit systematisch bewaakt kan worden.
Roos Mesman, zelfstandig organisatieadviseur en onderzoeker bij IQ healthcare, onderdeel van het Radboudumc, heeft *hoofdstuk 7*, 'Kwaliteit van zorg: meten en leren', geschreven. In dit hoofdstuk gaat zij dieper in op de wijze waarop zorgorganisaties kwaliteitsbewaking in de praktijk toepassen.

Een bijzonder actueel onderwerp — zowel in de zorg als daarbuiten — is privacy. Kim Lucassen, partner bij Loyens & Loeff, en Ellen Bosma en Jacobine van Beijeren, advocaten bij Loyens & Loeff, behandelen in *hoofdstuk 8* de kernbegrippen van het regelgevend kader van dit onderwerp: de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Vervolgens bespreken zij het belang van andere richtsnoeren en normen.

Ten slotte wordt in dit hoofdstuk ingegaan op privacy-issues in de praktijk (toegang tot patiëntendossiers, uitwisseling van patiëntgegevens en datalekken).
Zorginstellingen worden door de overheid en de zorgverzekeraars gestimuleerd om afspraken te maken over de spreiding en de specialisatie van de zorg. Voorts leidt de drang om efficiënter te werken ook tot een streven om fusies aan te gaan. Deze samenwerking en fusies kunnen de mededinging echter ook beperken. Tegen ongeoorloofde beperking van de mededinging kan door de externe toezichthouders ACM en NZa hard worden opgetreden. Compliance op dit gebied is derhalve van groot belang voor zorginstellingen. *Hoofdstuk 9* is geschreven door Marc Wiggers en Mark Brabers, advocaat bij Loyens & Loeff. Zij gaan in op een aantal mededingingsrechtelijke onderwerpen die voor de zorgsector relevant zijn. De bedoeling is dat daarmee de grootste risico's door de betrokken instellingen geïdentificeerd kunnen worden.
Wilco Oostwouder, Tamara Moll, consultant bij D&A Medical Group, en Mariska Kool, advocaat bij Loyens & Loeff, behandelen in *hoofdstuk 10* diverse aspecten van eHealth (o.a. het snel toenemende belang van eHealth voor de zorg, hoe zet je een eHealth-project op en waar moet je aan denken als je een ICT-contract met een leverancier sluit?).
Hoofdstuk 11 is geschreven door Marcel van de Berg, partner bij Rainmaker Communicatie. Deze ervaren consultant en expert in strategische communicatie belicht hierin hoe crisiscommunicatie in de praktijk in zijn werk moet gaan en welke valkuilen te allen tijde dienen te worden vermeden.

Deel 4 *Financiële compliance* omvat drie hoofdstukken: 'Compliance bij correct declareren in de praktijk', 'Financiering' en 'Fiscale compliance'.
Hoofdstuk 12 heeft betrekking op compliance bij correct declareren. Aris van Veldhuisen en Katy Hofstede, werkzaam bij Andersen Effers Felix (AEF), en Jasper Sluijs, universitair docent aan de Universiteit Utrecht, schetsen daarbij eerst het wettelijk kader: de Wet marktordening gezondheidszorg, de Wet langdurige zorg en de Zorgverzekeringswet. Een groot aantal compliancevraagstukken komt voort uit het gegeven dat de regels ten aanzien van het declareren de afgelopen jaren veelvuldig veranderd zijn. In dit hoofdstuk worden het toegenomen belang van betaalbaarheid van het zorgstelsel en het tegengaan van diverse vormen van onrechtmatigheid besproken. Maar ook wordt ingegaan op praktische problemen die voortvloeien uit wet- en regelgeving en toezicht daarop. Ten slotte wordt in dit hoofdstuk aangegeven hoe het beste gewaarborgd kan worden dat professionals in de zorg de ruimte vinden om kwalitatief hoogstaande zorg te bieden binnen het bestaande kader van wet- en regelgeving.
De '*cost gaat voor de baet uit*'. Dit geldt ook voor zorginstellingen. Daarom heeft vrijwel elke zorginstelling vroeg of laat externe financiering nodig. Hiervoor zijn zorginstellingen voornamelijk afhankelijk van banken (voor de financiering van werkkapitaal, vastgoed en andere investeringen) en zorgverzekeraars (bevoorschotting van onderhanden werk). Hoewel het wettelijk kader dat betrekking heeft op deze financiering beperkt en overzichtelijk is, speelt compliance op het gebied van financiering een belangrijke rol. Dit komt omdat banken en zorgverzekeraars zorginstellingen in respectievelijk de leningsovereenkomst en het contract met de zorgaanbieders regels opleggen waarvan niet-nakoming tot verstrekkende consequenties (o.a. opzegging krediet/contract, verhoogde rente dan wel boeterente) kan

leiden. Willem Jarigsma, partner bij Loyens & Loeff, en Bas Megens, Ehsan Shirzadi en Leon Engelen, advocaten bij Loyens & Loeff, pogen in *hoofdstuk 13* bewustheid te creëren bij zorgbestuurders en andere binnen een zorginstelling werkzame personen van de strekking van de financieringsvoorwaarden, het nut van het onderhandelen over deze voorwaarden en de risico's van niet-nakoming.
Patrick van Oppen, Ralph Ferouge, Bart Heijnen en Luca van Silfhout, belastingadviseurs bij Loyens & Loeff, behandelen in *hoofdstuk 14* de problematiek met de fiscale compliance bij zorginstellingen. Daarbij komen onderwerpen als de zorgvrijstelling voor de vennootschapsbelasting, de ANBI-regeling, winstuitkeringen in de zorg, loonheffingen, het werken met zzp'ers, inleners- en ketenaansprakelijkheid en verschuldigdheid van btw aan de orde. Ten slotte wordt aangegeven hoe fiscale compliance in de praktijk gewaarborgd kan worden.
Als bijlage bevat dit boek een aantal interviews uit 2015 met personen die werkzaam zijn (geweest) als bestuurder, wetenschapper, externe toezichthouder of beleidsmedewerker en uit dien hoofde kennis hebben van compliance in de zorg. Deze interviews maakten onderdeel uit van de eerste druk van het Handboek compliance in de zorg. Hoewel de standpunten een momentopname zijn en niet alle betrokkenen meer werkzaam zijn voor dezelfde organisatie als destijds, zijn de interviews toch integraal opgenomen. Deze interviews bevatten namelijk nog veel moois ten aanzien van compliance in praktijk. De lessen die daaruit kunnen worden getrokken, wil de redactie van dit handboek de lezers niet onthouden.

1.4 Het doel

Met dit boek wordt beoogd om bestuurders, commissarissen en compliance officers bij zorginstellingen op een toegankelijke en efficiënte wijze inzicht te verschaffen in de diverse issues die op het terrein van naleving van waarden en normen op het gebied van de zorg leven.
Voorts verschaft het een goede basis voor op maat gesneden complianceprogramma's voor zorginstellingen. Het bevat praktische tips ('do's and don'ts') en inspiratieparagrafen die gebruikt kunnen worden bij het opzetten van zo'n programma en de controle op de naleving daarvan. Dit boek is niet alleen nuttig voor compliance officers in de zorg, maar ook voor bestuurders van zorginstellingen, die immers eindverantwoordelijk zijn voor de naleving van wet- en regelgeving door de betrokken instelling, en commissarissen van zorginstellingen die toezicht houden op de voornoemde naleving. De leiding van de Grotius-opleiding Gezondheidsrecht en de leiding van de Registeropleiding Compliance Officer in de Zorg hebben besloten dat de tweede druk van dit handboek voorgeschreven wordt bij deze opleidingen.

1.5 Het (noodzakelijke) voorbehoud

Compliance is altijd afhankelijk van de concrete omstandigheden van het geval en zal derhalve voor iedere zorginstelling anders uitpakken. De diverse onderdelen van dit handboek zijn zorgvuldig opgesteld en geredigeerd. Echter voordat deze in een zorginstelling worden toegepast/geïmplementeerd, moet zorgvuldig worden nagegaan of deze volledig zijn, up-to-date zijn en voldoen aan de dan geldende wet- en regelgeving die op uw instelling van toepassing is. De redactie en de auteurs aanvaarden derhalve geen aansprakelijkheid voor het gebruik van de informatie

uit de diverse onderdelen van dit boek (waaronder begrepen de inspiratieparagrafen) en de eventuele implementatie ervan bij uw zorginstelling.

1.6 Afsluiting kopij

De definitieve versies van de meeste hoofdstukken van dit handboek zijn op of enige tijd na 1 december 2018 bij de redactie ingeleverd. Bij wijze van uitzondering zijn in bepaalde hoofdstukken enkele belangrijke ontwikkelingen van na 1 december 2018 meegenomen.
Maar met andere relevante ontwikkelingen na die datum is geen rekening gehouden.

1.7 Suggesties

De redactie houdt zich van harte aanbevolen voor suggesties die de bruikbaarheid van dit boek nog kunnen verbeteren. We danken allen die ons van suggesties hebben voorzien naar aanleiding van de eerste druk, in het bijzonder enkele deelnemers van de Registeropleiding voor Compliance Officer in de Zorg. Ook veel dank aan het Zorgteam van Loyens & Loeff en met name ten aanzien van de inspanningen op ondersteunend gebied.

Hoofdstuk 2-1

Compliance officers en experts aan het woord

Onderdeel 1 — De zeven elementen van een effectief complianceprogramma

Mr. R.M. Notermans*

2-1.1 Inleiding

Mijn bijdrage gaat over de zeven elementen die naar mijn mening in elk effectief corporate complianceprogramma moeten voorkomen. De lezer kan zelf parallellen trekken naar zijn/haar eigen werkomgeving en op die manier leren van good en best practices, valkuilen en tips uit de corporate wereld.

Dit deel van het boek beoogt in korte schetsen met eenvoudige, begrijpelijke voorbeelden aan te geven hoe compliance zich verhoudt tot governance en risicomanagement, alsmede wat die zeven elementen behelzen. Compliance is een van de vele maatregelen die een organisatie neemt om haar medewerkers de kernwaarden en visie op 'verantwoord handelen' bij te brengen, risico's beheersbaar te maken en haar reputatie te beschermen.

2-1.2 Beginnen bij het begin: governance

Organisaties ontstaan vanwege een visie, doel en/of ideaal. Een commerciële ondernemer begint met het zien van kansen. De mogelijkheid om geld te verdienen. Kansen omzetten in producten of diensten vergt vroeg of laat financiering, bijvoorbeeld om prototypen te (laten) ontwikkelen of nieuwe diensten te kunnen ontwikkelen (zoals in de zorg). Financiering kan plaatsvinden uit eigen vermogen (meestal ontoereikend) of vreemd vermogen: bankleningen en/of private geldschieters. Zodra een ondernemer met partners of vermogensverschaffers te maken krijgt, ontstaat de noodzaak om governance-afspraken te maken. Immers, men gaat met het geld van derden aan de slag en die derden willen dat met hun geld zorgvuldig, verantwoord wordt omgesprongen.

Het principe van verantwoord omgaan met het geld van anderen en dus verantwoordelijkheid nemen voor interne afspraken is in essentie ook van toepassing op een beursgenoteerde vennootschap, een familiebedrijf, een woningcorporatie en een zorginstelling. Ook daar wordt verwacht dat zorgvuldig wordt omgesprongen met geld. Ook daar moet het bestuur van de organisatie zich houden aan de opgelegde wettelijke en afgesproken contractuele beperkingen. Ook daar worden nadere governance-afspraken gemaakt. Compliance begint dus met goede governance.

---

* Roland Notermans is eigenaar van NUX Compliance Consultancy & DeComplianceAcademie.nl. Deze bijdrage is gebaseerd op jarenlange compliance-ervaring in corporate omgevingen waarmee compliance professionals in de zorg hun voordeel kunnen doen.

Mijn bijdrage gaat niet uitgebreid in op goed ondernemingsbestuur, over de relatie tussen aandeelhouders, raad van commissarissen (toezichthouders) en raad van bestuur (in de zorgsector ontbreekt zelfs vaak een aandeelhouder). Evenmin ga ik uitgebreid in op de Governancecode Zorg 2017; governance komt elders in dit boek uitgebreid aan de orde.
Het moge echter duidelijk zijn dat organisaties niet behoorlijk kunnen functioneren zonder heldere afspraken tussen toezichthouders en bestuurders (en in sommige gevallen de aandeelhouders). De basis daarvoor ligt bij het richtinggevend wettelijk kader en een actuele governancecode die steeds wordt verbeterd teneinde doelmatigheid en vertrouwen te bevorderen.[1]

Of we nu het voorbeeld van een ondernemer bespreken met zijn eerste externe geldschieter of de positie van een hedendaagse raad van bestuur in de zorgsector: governance-afspraken zijn het eerste voorbeeld van het beheersbaar maken van de risico's verbonden aan het bereiken van de organisatiedoelen. Risico's beheersen vergt echter méér, zoals we in de navolgende paragrafen zullen zien.

2-1.3 Risicomanagement

Risico's kunnen eigenlijk op vier manieren worden benaderd: door ze te elimineren, over te dragen, te verminderen of zelf te dragen. Laat ik heel kort over elk van deze manieren iets zeggen.

Elimineren
Elimineren is vaak de moeilijkste optie, omdat het doorgaans onevenredig veel tijd en geld kost om alle risico's geheel ongedaan te maken. In een latere paragraaf zien we dat organisaties veel bewuster dan in het verleden keuzes maken om bijvoorbeeld wel of niet in een land zaken te blijven doen, wel of niet bepaalde diensten aan te bieden, omdat de risico's (te) groot zijn geworden. Elimineren gaat over keuzes maken, waarbij de optimale balans tussen kosten en risico's steeds wordt meegewogen: gaan wij wel of niet een bepaalde deelmarkt betreden (diensten en/of productmarkten); gaan we wel of geen interne en externe maatregelen nemen om bepaalde risico's te elimineren. Dat blijkt soms noodzakelijk en kostbaar.[2]

Overdragen
Overdragen klinkt mooi in theorie, maar in de praktijk is dit geen goedkope optie. Verzekeringsmaatschappijen maken gezonde winsten, anders zouden ze niet meer bestaan. Om nu alle risico's te gaan verzekeren is een te dure optie, zeker in de ogen van de aandeelhouders. Het is ook onnodig. Alleen indien en voor zover de organisatie heel grote calamiteiten niet zelf kan opvangen, is een financiële buffer in de vorm van een verzekering waarschijnlijk nodig. Waarbij helder zal zijn dat

1. Zie bijvoorbeeld www.commissiecorporategovernance.nl. De huidige Corporate Governance Code legt veel meer nadruk op vooruitblikkende risicobeheersing, langetermijnwaardecreatie alsmede cultuur als drijvende krachten voor goed ondernemingsbestuur.
2. Compliancemaatregelen zijn soms kostbaar, non-compliance echter ook. Zie het zeer recente voorbeeld bij de ING Bank die jarenlang geld bespaarde op het controleren van mogelijk witwassen. De boete lijkt zesmaal hoger dan de winst die zou zijn gemaakt gedurende een vijftal jaren met die transacties.

een eenmalige uitkering door de verzekeraar uitgekeerd in de daaropvolgende jaren als een verhoogde premie zal terugkeren als een boemerang. Daarom gaan steeds meer organisaties ertoe over om zelf reserves aan te leggen en alleen boven een bepaald (hoog) drempelbedrag zich nog tegen zeer specifieke risico's te verzekeren.

Overdragen kan ook (gedeeltelijk) door in overeenkomsten de risico's anders te beleggen dan de wet dat normaliter zou doen. Hier ligt een belangrijke taak voor de juristen. Samen met management wordt op basis van de risk appetite[3] van de organisatie bepaald welke risico's tot op welk niveau uitonderhandeld moeten worden om tot acceptabel handelen te komen. In het nieuws zien we soms allerlei machtsvertoon waarbij inkopers eenzijdig afkondigen dat enige weken later de leveranciers nog maar 98 of 97% van de rekeningen betaald zullen krijgen, of dat de betalingen een maand langer op zich laten wachten. Overdragen en 'weg-onderhandelen' klinken dus aantrekkelijk in theorie, maar zullen in de praktijk alleen voor heel sterke marktpartijen zijn weggelegd.

Verminderen
Het COSO-model van risicobeheersing[4] is een gangbare methode om intern risico's inzichtelijk en beheersbaar te maken teneinde de vastgestelde doelstellingen te kunnen halen op strategisch, operationeel, financieel en compliancegebied. Dit zogenaamde Enterprise Risk Management Framework indiceert welke maatregelen ingevoerd zouden moeten worden om de risico's te managen (lees: verminderen/mitigeren) en de organisatiedoelstellingen te kunnen halen. Ook in de zorgsector geldt: 'De raad van bestuur bespreekt en verantwoordt regelmatig de risicoanalyses en de werking van de risicobeheersingssystemen met de raad van toezicht.'[5] Verminderen vergt veel tijd en inspanningen.

Accepteren
De term *(legal) risk management* wordt doorgaans gebruikt om de veelheid aan interne maatregelen aan te duiden om de (juridische) risico's verbonden aan de organisatie te beheersen. De vierde beheersingsmaatregel — accepteren — komt in ieder geval in het bedrijfsleven naar mijn mening vaak voor: het financieel zelf dragen van risico's. Op de langere termijn moet een organisatie haar risico's gestructureerd en continu inventariseren, inschatten, beheersen, accepteren en daarmee financieel grotendeels zelf dragen. Dat vereist heel veel aandacht voor kwaliteit in alle geledingen van de organisatie, in geoptimaliseerde processen en procedures.

Hieraan draagt positief bij dat het Hoofd Juridische Zaken ('HJZ'), Hoofd Compliance en de Chief Risk Officer de laatste jaren steeds meer een business partner zijn geworden. Zij zijn 'risicomanagers' geworden die proactief, continu, integraal toegevoegde waarde (moeten) leveren door de risico's te managen binnen de grenzen

3. Een mooi voorbeeld van een Nederlandse vennootschap die over haar risk appetite bericht, is: 'De bereidheid van Ballast Nedam om risico's te nemen beperkt zich tot verantwoorde ondernemingsrisico's: de waarschijnlijkheid van het optreden van risico's en de mogelijke gevolgen daarvan mogen de continuïteit van de onderneming niet in gevaar brengen.' In de praktijk blijkt dit een forse uitdaging.
4. Committee of sponsoring organizations of the Treadway commission, www.coso.org.
5. Governancecode Zorg 2017, art. 5.4.2.

gesteld qua budgetten en risicoprofiel (risk appetite). Hun werkgever is steeds vaker op zoek naar het spreekwoordelijke 'gat in de muur' in plaats van een boor: de oplossing staat voorop.

2-1.4 Managen betekent keuzes maken

De organisatie zal — met inachtneming van missie en visie — voortdurend keuzes moeten maken bij het analyseren en optimaal inrichten van het risicomanagement. Waar verdient deze organisatie het meeste geld? Waar wordt het meeste geld verloren? Waar zouden beperkte middelen optimaal ingezet kunnen worden om de organisatiedoelstellingen het beste te ondersteunen?
Een ontwikkelings- en/of productieonderneming als Canon of Panasonic heeft heel andere risicobeheersingsmaatregelen nodig dan een dienstverlener als PwC of Randstad. Een lokaal opererende zorgverlener heeft weer andere nodig dan een landelijk opererende privékliniek of zorgverzekeraar. Ook de marktpositie is van belang: een dominante partij die de algemene voorwaarden kan doordrukken in de meeste onderhandelingen heeft de ruimte om andere keuzes te maken dan kleine partijen.

Verder is relevant de keuze tussen wat (juridisch) noodzakelijk is en wat verstandig zou zijn indien meer middelen ter beschikking zouden staan. Datgene wat juridisch noodzakelijk is, moet worden gecommuniceerd in de gehele organisatie teneinde de organisatie zich aan de wet te laten houden: zie daar, regulatory compliance is geboren!

2-1.5 Waar past compliance in dit geheel?

Compliance heeft een lange ontwikkeling doorgemaakt van oorspronkelijk regulatory compliance (je houden aan wet- en regelgeving met veel regels en hard controls) naar ethical, behavioural of corporate compliance (met veel meer aandacht voor cultuur, gedrag, principes en soft controls). Een ontwikkeling van controlerende naar 'stimulerende' compliance.

Regulatory compliance was oorspronkelijk een uitvloeisel van legal risk management, beperkt tot enkele juridische gebieden teneinde de medewerkers erop te wijzen dat men zich aan specifieke wetten diende te houden. Vaak werd het HJZ geconfronteerd met de opdracht om compliance in bredere zin wereldwijd te gaan organiseren want '(…) de juridische functie gaf toch al voorlichting over een aantal wetten?' In de praktijk bleek dat de nadruk op regulatory compliance alléén echter tekortschoot: de gemiddelde medewerker moest méér bewustzijn worden bijgebracht dan wetgeving met behulp van regeltjes en afvinklijstjes.

Langzamerhand beginnen organisaties ervan doordrongen te raken dat lang niet alles dat wettelijk is toegestaan (bijvoorbeeld kinderarbeid in bepaalde landen) ook legitiem is in de ogen van de gemiddelde belanghebbende. Je houden aan wetten is niet langer voldoende. Goede reputaties worden in jaren opgebouwd en die wil de organisatie niet in korte tijd verliezen door het gedrag van een paar 'rotte appels'.

In de praktijk staat reputatiemanagement steeds vaker expliciet centraal in corporate complianceprogramma's.

2-1.6 Regulatory, stimulerend, corporate compliance?

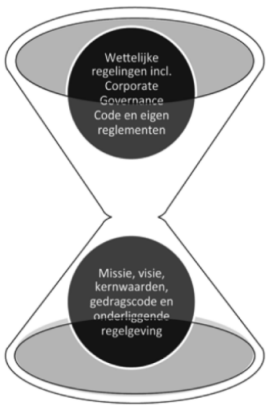
Corporate compliance zou ik willen omschrijven als het gehele programma dat een onderneming doorvoert om alle medewerkers en andere belanghebbenden uit te leggen wat deze onderneming verstaat onder verantwoord zakendoen. Vertaald naar de zorgsector: wat verstaat deze organisatie onder 'verantwoord handelen'? Hoe willen wij onze doelen bereiken? Verantwoord handelen omvat zowel controlerende (regulatory) als stimulerende (ethische) aspecten. Kort samengevat:

- Waar staat deze organisatie voor (missie, visie, kernwaarden, beloften aan de buitenwereld)?
- Hoe trekt die haar grenzen (zoeken we randen op van de wet of blijven wij daar ruimschoots binnen)?
- Welke principes (liefst beschreven in een gedragscode) moet de gemiddelde medewerker tot uitgangspunt nemen bij moeilijke beslissingen?
- Wat verwachten wij van iedere medewerker (bijvoorbeeld dat zij op gepaste wijze van zich laten horen indien zij een vermoeden hebben van een overtreding van de gedragscode)?

2-1.7 Governance en compliance

De relatie tussen governance en compliance zou ik als volgt willen visualiseren:

governance < - > compliance



Governance[6] duidt in het algemeen op de regels en afspraken tussen toezichthouders en bestuur van de vennootschap (soms ook aandeelhouders, waar van toepassing), terwijl corporate compliance wordt gebruikt om aan te geven hoe 'verantwoord handelen' intern is geregeld. Voor de relatie tussen governance en compliance gebruik ik het beeld van een dubbele trechter omdat beide normenkaders elkaar

6. Zie hoofdstuk 3 over governance in dit boek.

voortdurend beïnvloeden en in open verbinding staan met elkaar: de normen uit de ene trechter zijn van invloed op de principes en uitgangspunten in de andere trechter. Het eerste gedeelte ziet op de bovenste lagen van de organisatie. Het tweede raakt bestuur, medewerkers en derden zoals leveranciers en klanten.

First things first
Als organisatie kom je pas toe aan een gedegen (stimulerend) corporate compliance-programma als je je governance — waaronder de interne governance (tot in de kleinste haarvaten van de organisatie) — en (controlerende) regulatory compliance op orde hebt. Wat bedoel ik daarmee?

Je begint, zoals in de inleidende paragrafen geschetst, eerst met alle noodzakelijke interne regelingen om te kunnen functioneren en blijven voortbestaan. De nadruk ligt daarbij op de governance van de organisatie (wie mag wat) en de noodzakelijke prioriteiten voortvloeiend uit de analyse van doelen en risicomanagement. Zoals governance tussen raad van toezicht en raad van bestuur is geregeld en binnen de raad van bestuur, zo moet de organisatie verder in alle haarvaten helder regelen wie welke (contractuele) afspraken mag maken. Wanneer moet een medewerker goedkeuring van hogerhand vragen? Dan gaat het niet alleen om financiële limieten aan de volmachten van verkoop- of inkoopmedewerkers en andere functionarissen, maar ook om de afspraken omtrent risicoverdeling. Een voorbeeld: als organisatie wil je niet geconfronteerd worden met een situatie waarin de verkoopmedewerker — door het ondertekenen van een standaard inkoopcontract van een klant — in ruil voor een geringe omzet onbeperkte aansprakelijkheden (gevolgschaden) en vrijwaringen heeft geaccepteerd.

2-1.8 Corporate compliance: good practices

De zeven elementen van een goed, effectief corporate complianceprogramma (regelstellend én stimulerend) zijn volgens mij:
1. de toon aan de top (én eigenlijk bij alle leidinggevenden);
2. een risicoanalyse met navenante beheersing waaronder hard en soft controls;
3. een heldere gedragscode;
4. een gedegen communicatie- en trainingsprogramma;
5. een adequate organisatie van de compliancefunctie;
6. een open meldcultuur; en
7. het voortdurend monitoren, controleren en opvolgen.

Deze zeven elementen komen niet zomaar uit de lucht vallen, maar zijn her en der terug te vinden in publicaties van tal van toezichthouders alsmede recentelijker in schikkingsovereenkomsten met toezichthouders (bijvoorbeeld deferred prosecution agreements). Denk aan de toelichting, de Federal Sentencing Guidelines,[7] op de Amerikaanse Foreign Corrupt Practices Act. Denk aan de toelichting op de UK

7. www.ussc.gov/guidelines-manual/guidelines-manual; alsmede het in 2017 door het Amerikaanse Ministerie van Justitie gepubliceerde 'Evaluation of Corporate Compliance Programs': https://www.justice.gov/criminal-fraud/page/file/937501/download.

Bribery Act[8] en diverse publicaties van het Office of Fair Trading,[9] de OECD-aanbevelingen op het gebied van interne controlemaatregelen, ethiek en compliance (m.n. gericht op corruptiebestrijding),[10] de ICC[11] en de Franse Autorité de la concurrence (met name hun framework-document over het optimaal inrichten van mededingingsprogramma's).[12] Waardevol is ook de richtlijn (geen standaard of norm, hoewel de naam anders doet vermoeden) ISO 19600[13] (mede gebaseerd op de al langer bestaande Australische AS 3808-2006-norm) en in Nederland de wel certificeerbare norm van de Stichting Stimuleringskader Integere Organisatie.[14]

Deze zeven elementen zal ik achtereenvolgens bespreken en er enige persoonlijke opmerkingen bij plaatsen.

#1 De toon aan de top (én op alle managementlagen)

Alle managementlagen zullen het goede voorbeeld moeten geven door iedere dag weer de kernwaarden van hun organisatie als leidraad te kiezen in hun beslissingen. Zij moeten als het ware de kernwaarden en uitgangspunten zoals beschreven in de gedragscode in hun DNA hebben en dagelijks ademen, het levende voorbeeld zijn, niet alleen in woord maar vooral in daad.

De toon aan de top is een noodzakelijke maar niet voldoende voorwaarde voor verantwoord handelen. Indien een lid van de raad van bestuur een scheve schaats rijdt (bijvoorbeeld een familielid inhuurt voor diensten of zich ruimhartig op een sportevenement laat fêteren), dan weten waarschijnlijk veel medewerkers in zijn naaste omgeving dat binnen korte tijd. Slecht voorbeeld doet vervolgens velen volgen: medewerkers besteden onder kantooruren daarna meer tijd aan privézaken, dienen privébonnetjes voor taxi's in als zakelijke kosten et cetera. Als de baas het mag dan… Laat het dus duidelijk zijn dat op alle niveaus het voorbeeldgedrag van de leidinggevenden vele malen belangrijker is dan hun woorden.

De toon die wordt gezet door het middenkader en iedere 'lagere' leidinggevende is net zozeer van belang voor een integere werkhouding. Te vaak worden de lagere managementlagen vergeten. Ga ervan uit dat zij onder zeer hoge druk staan om financiële doelen te halen, te veel e-mails per dag krijgen, te veel open issues moeten oplossen. Moeten ze daarnaast ook nog tijd besteden aan het onderwerp 'compliance'? Maak het hen dus heel gemakkelijk. Verplaats je in hun positie en zorg dat ze wél aandacht geven aan het onderwerp, wél het goede voorbeeld geven en wél de juiste verhalen (kunnen) vertellen. Doe dat door hun dagelijkse werk te verlichten, bijvoorbeeld met hulpmiddelen, voorbeeldteksten, dilemma's, toolboxen et cetera. De meeste medewerkers kijken vooral naar hun direct leidinggevende. Daar ligt dus een eerste sleutel tot succes.

8. https://www.gov.uk/government/publications/bribery-act-2010-guidance.
9. https://www.gov.uk/government/organisations/office-of-fair-trading.
10. www.oecd.org/investment/anti-bribery/anti-briberyconvention/44884389.pdf.
11. https://iccwbo.org/publication/icc-rules-on-combating-corruption/.
12. www.autoritedelaconcurrence.fr/doc/framework_document_compliance_10february2012.pdf.
13. www.nen.nl/NEN-Shop/Compliancemanagement-1.htm.
14. www.stichtingsio.nl.

#2 Risicoanalyse en beheersing

Zoals eerder besproken zal een organisatie keuzes moeten maken aan de hand van regelmatig terugkerende risicoanalyses.[15] Sommige risico's kunnen het beste met hard controls worden beperkt, andere met soft controls (daarover meer in de subparagraaf hierna). Geen organisatie zal alle risico's uitputtend kunnen aanpakken. Dat doe je als privépersoon ook niet (hoeveel mensen kopen een zogenaamde 'slecht weer'-verzekering indien ze een vakantie boeken?).

Organisaties beschikken over beperkte middelen die ze optimaal willen inzetten. Aan de hand van de risicoanalyses en reeds genomen beheersingsmaatregelen zal ieder jaar een plan van aanpak moeten worden opgesteld om te beslissen welke risico's wel, geen of minder aandacht gaan krijgen. De raad van bestuur zal, tegenwoordig vaak in samenspraak met de leden van een Governance, Risk & Compliance Commissie, helder moeten maken wat de ambities, risk appetite en doelen zijn op het gebied van organisatierisico's.

Een risicoaanpak kijkt niet alleen naar de kans, maar ook naar de termijn waarop zich dat risico waarschijnlijk zal verwezenlijken. Verstandig is het om ook te kijken naar de omvang van de financiële en reputatieschade die kunnen optreden. Zoals we eerder bespraken, is reputatiemanagement een van de motivaties om een effectief corporate complianceprogramma in te richten.

Hard en soft controls
Effectieve risicobeheersingsmaatregelen bestaan meestal uit een combinatie van hard en soft controls.
Hard controls zijn controlemaatregelen die zodanig in processen en procedures zijn vastgelegd dat ze niet of heel moeilijk te omzeilen zijn. Ze zijn concreet en vaak tastbaar, zoals fysieke beveiligingsmaatregelen of toezicht. Denk hierbij ook bijvoorbeeld aan de eis van twee handtekeningen, in ICT-ingebedde goedkeuringsprocedures voor investeringen, voor (contractuele) goedkeuringen of het openen van bankrekeningen.

De onderwerpen die vaak in gedragscodes terugkomen, zijn zelden met hard controls alleen te beheersen. Soft controls zijn weliswaar niet tastbaar maar wel waarneembaar en zelfs meetbaar: '*(s)oft controls zijn sturings- en beheersingsmaatregelen die erop gericht zijn om gewenst, integer, gedrag bij medewerkers en management te bevorderen.*'[16] Denk aan normen en kernwaarden van de organisatie, de bedrijfscultuur, de codes en impliciete regels. Verder kan ook worden gedacht aan de helderheid van de interne regels, de uitvoerbaarheid (krijgt de medewerker tegenstrijdige doelen mee?), transparantie in de organisatie, zichtbaarheid van gedrag en correcties daarop alsmede de bereidheid van de organisatie om sancties op te leggen bij overtredingen.

15. In de zorgsector bespreekt de raad van bestuur die regelmatig met de raad van toezicht; zie art. 5.4.2 Governancecode Zorg 2017.
16. M. Lückerath-Rovers in: *Jaarboek Compliance 2011*, Capelle aan den IJssel: Nederlands Compliance Instituut 2011, p. 77.

Een van de belangrijkste soft controls ná voorbeeldgedrag vind ik zelf 'bespreekbaarheid'. Medewerkers durven in de praktijk een ander zelden aan te spreken op ongepast gedrag,[17] met name indien die ander een leidinggevende betreft. Dilemma's in de eigen afdeling bespreekbaar maken waarbij het individuele integriteitskompas wordt geijkt op dat van de organisatie is echter essentieel om compliance effectief te maken. Daarover schreef ik eerder elders uitgebreid.[18]

Zakenpartners
De risicoanalyse zal de organisatie waarschijnlijk tot de conclusie brengen dat zij ook haar zakenpartners moet meenemen op het pad richting verantwoord handelen. Een eerste stap kan zijn het screenen van belangrijke derden met wie eventueel zaken zal worden gedaan. Een goed voorbeeld is ook het invoeren van een gedragscode voor leveranciers.[19]

#3 Een heldere gedragscode

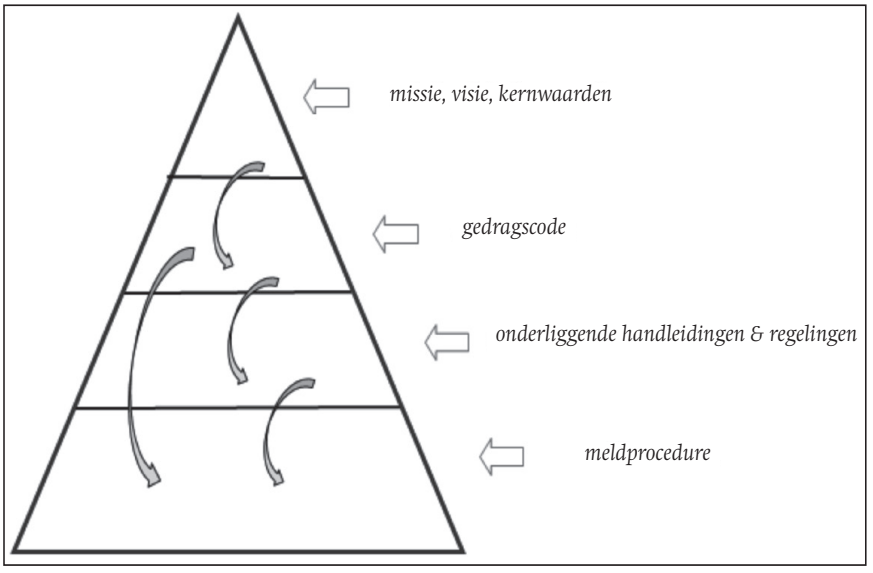
Essentieel voor het slagen van een effectief corporate complianceprogramma is dat *alle* medewerkers een duidelijk beeld hebben van wat van hen in welke situatie wordt verwacht; dat ze begrijpen — zodra ze bij de organisatie komen werken — wat 'verantwoord handelen' betekent in deze organisatie en hóé de doelen moeten worden bereikt. Waar de organisatie haar grenzen trekt. Vroeger zongen we het liedje '*zo zijn onze manieren…*'. Die manieren moeten helder en duidelijk zijn, op alle niveaus in de organisatie, en bij twijfel zullen simpelweg vragen moeten worden gesteld alvorens te handelen.

Een gedragscode is een heel geschikt instrument daartoe. Het document verwoordt vaak niet alleen wat de buitenwereld en de medewerkers van deze organisatie mogen verwachten, maar ook hetgeen van iedere medewerker wordt verwacht. Ingewikkeld, juridisch taalgebruik of de neiging om werkelijk alles tot in detail in een gedragscode te regelen leidt ertoe dat weinig medewerkers enthousiast worden om te lezen en gaan begrijpen hoe zij zich aan 'die regeltjes' moeten gaan houden. Met name in Amerikaanse organisaties heerst nog wel eens de gedachte dat alles op papier moet staan en weinig aan de vaagheid van principes mag worden overgelaten. Codes van 50 tot 80 pagina's worden zelden geheel gelezen en leiden dan te vaak tot een 'afvink'-mentaliteit. Een dergelijke vorm van controlerende compliance is weinig effectief gebleken en kan goede bedoelingen zelfs ondergraven.[20]

17. Zie bijvoorbeeld het grote aantal anonieme meldingen (ruim 60%): https://www.navexglobal.com/en-us/resources/benchmarking-reports/2018-hotline-incident-management-benchmark-report?RCAssetNumber=3309.
18. Roland Notermans, 'Compliance cultuur vergt georganiseerd weerwoord', in: P. Dinjens (red.), *Goede raad voor commissarissen: 21 inzichten voor toezichthouders en bestuurders*, Amsterdam: Mediawerf 2018, p. 105 e.v.
19. Een mooi initiatief om leveranciers de onderhandelingen over botsende gedragscodes te besparen, maar wel zorg te dragen dat zij op hun beurt ook weer hun eigen leveranciers verplichten tot verantwoord zakendoen, is te vinden bij de Responsible Business Alliance: http://www.responsiblebusiness.org/.
20. Ik ben een fel tegenstander van de Amerikaanse neiging om medewerkers in de gedragscode te verplichten om elk vermoeden van welke overtreding van welk onderdeel in de code ook te moeten melden. Dat doet geen enkele medewerker. Een dergelijke verplichting ondergraaft de geloofwaardigheid van het programma. Liever die verplichting beperken tot zware misstanden waarvoor mensen gevangenisstraf kunnen krijgen of de organisatie zware boetes. Zie verder mijn website.

Een gedragscode gebaseerd op inspirerende compliance geeft de basis voor verantwoord handelen; die code gaat over goede business-principes en 'onze' manier van werken. Die benoemt en verduidelijkt de kernwaarden van de organisatie[21] en de wijze waarop zij haar uitstekende reputatie verder wenst uit te bouwen en beschermen. Specifieke regels, procedures en hulpmiddelen worden uitgewerkt in bijlagen, praktische handleidingen en dergelijke waardoor de gedragscode zelf helder, kort en behapbaar voor de gemiddelde medewerker kan blijven.

Het is verstandig om de gedragscode kort te houden maar elk onderwerp uit de code wel te vergezellen van een alinea met de strekking: 'Wat betekent dit voor jou?' Juist het concreet maken slaat een brug naar het individu en zijn eigen verantwoordelijkheid. Nadere uitleg, regelingen, voorbeelden, vragen en antwoorden zou ik liever plaatsen in onderliggende beleidsdocumenten om ervoor te zorgen dat de medewerkers snel en gemakkelijk uitsluitend die informatie kunnen vinden en lezen die zij op dat bewuste moment daadwerkelijk nodig hebben.
Zo'n ideale structuur zou er dan als volgt uit kunnen zien:



Wat regel je dan in zo'n gedragscode?
De onderwerpen die in een gedragscode bij grote organisaties het vaakst voorkomen (naast de specifieke missie, visie en kernwaarden) zijn de navolgende:
- respect voor elkaar (antidiscriminatie) en respect (soms: 'steun') voor internationaal erkende mensenrechten;
- veiligheid voor mens en milieu;

21. De meest voorkomende kernwaarden zijn: integriteit, respect, eerlijkheid, verantwoordelijkheid en vertrouwen.

- zorgvuldig gebruik en behoud van bedrijfsmiddelen, bedrijfsgevoelige informatie, persoonsgegevens (privacy), social media-uitingen, knowhow en intellectuele eigendom;
- het vermijden van belangenconflicten;
- gepaste geschenken en vermaak;
- verbod op corruptie en regels om corruptie te voorkomen;
- mededingingsrecht en het verbod om deze regelgeving te overtreden;
- juistheid van financiële en niet-financiële documentatie en communicaties;
- verbod op frauduleuze handelingen.[22]

Bovengenoemde onderwerpen worden normaal gesproken aangevuld met branchespecifieke onderwerpen als misbruik van voorwetenschap, exportcontrole en sanctieregels, marketing en promotionele communicatie et cetera.

Managers hebben additionele verantwoordelijkheden
Tenslotte pleit ik er altijd voor om in de gedragscode zelf enige alinea's te wijden aan de extra verantwoordelijkheden die leidinggevenden hebben. Van hen mag worden verwacht dat zij de code implementeren, uitleggen, het goede voorbeeld geven, dilemma's bespreekbaar maken en een open cultuur creëren waarin elke medewerker zich veilig voelt om gevoelige zaken bespreekbaar te maken.

#4 Een adequaat communicatie- en trainingsprogramma

Een gedragscode werkt naar mijn mening alleen goed indien de gedragscode kort, helder en begrijpelijk is verwoord. Een moeilijk en vaag woord als 'compliance' zegt de gemiddelde werknemer erg weinig en zou zo veel mogelijk vermeden moeten worden in de communicatie naar medewerkers. Compliance kan anders te snel geïnterpreteerd worden als een taak van (alleen) de compliance officer (nog een woord om te vermijden). Zie daar de reden dat ik in interne communicaties het woord compliance steevast vermijd en liever spreek van 'verantwoord handelen'. Dat is een verantwoordelijkheid van élke medewerker, niet slechts de compliance officer.
De individuele medewerker moet daadwerkelijk begrijpen wat de veelheid aan externe en interne regels nu eigenlijk betekent voor zijn of haar dagelijkse werk. Dit is wellicht het belangrijkste element van een effectief corporate complianceprogramma: de heldere vertaalslag naar het individu. Het benodigde begrip bijbrengen blijkt een enorme klus waarvoor (forse) investeringen in tijd en geld nodig zijn.

Deze middelen worden niet altijd vrijgemaakt. Te vaak wordt de gedragscode slechts per post meegestuurd met het salarisstrookje of per e-mail naar alle medewerkers tegelijk. In een iets betere situatie wordt de medewerker toegesproken door de eigen leidinggevende, die het belang van verantwoord handelen nogmaals uitlegt. Gevolgd door een zeer algemene cursus op het intranet. Dat creëert het risico dat de medewerker het gevoel krijgt dat de cursus wel heel algemeen en breed is opge-

22. Als 'catch all' wordt veelal een statement toegevoegd waarin de organisatie aangeeft dat zij van haar werknemers verwacht dat zij zich niet alleen aan de letter, maar ook aan de geest van toepasselijke wet- en regelgeving zullen houden.

zet, maar weinig relevant is voor zijn of haar dagelijkse werk. Of erger nog, het geeft de medewerker de indruk dat de organisatie een standaard cursus heeft ingekocht die voortdurend spreekt over '*our company and our values*' zonder die daadwerkelijk te benoemen.

Een adequaat trainingsprogramma zou idealiter moeten worden ingebed in bestaande HR-processen en procedures. Elke nieuwe medewerker krijgt in de eerste maand een introductie over kernwaarden, gedragscode en 'onze manier van werken'.
Bij de jaarlijkse beoordelingen kunnen het gevolgd hebben van verplichte trainingen en het voorbeeldgedrag zelf niet ontbreken, want anders wordt het complianceprogramma door weinigen meer serieus genomen (zie mijn latere paragraaf over congruentie).

Leren en willen leren
Leren begint met willen leren door betrokken, actief, geïnspireerd en aandachtig luisteren. Dat bereik je door de medewerkers in het begin uit te leggen *waarom* de te volgen onlinecursus of persoonlijke training voor hun eigen dagelijkse werkzaamheden belangrijk is. Wellicht omdat zij bij een integere organisatie willen werken en een eigen steentje willen bijdragen. Wellicht omdat zij ook in de toekomst een baan bij deze organisatie willen behouden en naleving van de gedragscode een noodzakelijke maar niet afdoende voorwaarde daarvoor is.
Pas nadat de medewerkers actief, bereid en betrokken de training ingaan, kan het leren beginnen. Over de kernwaarden, de basisprincipes, het belang van overleggen met elkaar en met de leidinggevende bij twijfels en het melden van vermoedens van overtredingen van de code.

Eerst online?
Online leren heeft wel degelijk een positieve plek in een effectief complianceprogramma, maar een onlinecursus alleen blijkt in de praktijk onvoldoende.[23] Verstandig is om een dergelijke cursus door de leidinggevende zelf te laten aankondigen, het belang ervan voor de dagelijkse praktijk uit te leggen en te onderstrepen en aan te kondigen dat lokaal follow-up plaats zal vinden.

Vervolgens?
Zelfs indien veel waardevols via een online training wordt overgebracht, blijft de noodzaak bestaan om vervolgens in kleinere groepen binnen de eigen afdeling *dilemma's* te bespreken: uitdagende situaties waar deze groep medewerkers daadwerkelijk tegenaan loopt, waarvoor geen duidelijk antwoord bestaat omdat gekozen moet worden tussen botsende waarden. Een onlinecursus kan nooit alle nuances en moeilijke praktijkvoorbeelden volledig nabootsen. Leidinggevenden moeten dat met hun eigen groep vervolgens oppakken en daarbij aangeven hoe te handelen in dergelijke situaties. Medewerkers hebben namelijk behoefte aan duidelijkheid. Waar trekt deze organisatie haar grenzen en waarom, want de praktijk blijkt veel

23. Zie voor een overzicht van de vele valkuilen en good practices bij e-learning het artikel van Michael van Woerden en mijzelf in het *Tijdschrift voor Compliance* 2014, afl. 2, getiteld 'Over e-learning gesproken'.

genuanceerder dan de e-learning doet vermoeden: er bestaan wel meer dan honderd tinten grijs.

Follow-up

Het kan niet blijven bij een onlinecursus en een eenmalige dilemmaworkshop want een eenmalige communicatie die de maanden daarna geen follow-up krijgt, is als een auto die zonder benzine komt te staan. De boodschap uit je gedragscode wil je levend houden. Medewerkers kunnen anders gaan denken dat het gebrek aan aandacht voor dit onderwerp betekent dat zij het ook niet serieus hoeven te nemen. Bovendien blijkt uit veel sociaalpsychologische experimenten[24] dat medewerkers veel afspraken vergeten en het vaak van de omstandigheden laten afhangen of ze wel of niet de 'integere' keuze maken. Nobelprijswinnaar en gedragseconoom Richard Thaler[25] pleit terecht voor het introduceren van 'nudges': kleine duwtjes in de goede richting.

Dit levend houden van het belang en de noodzaak kan op verschillende manieren. Essentieel is dat de manier van communiceren past bij de betreffende organisatie, bij de specifieke fase waarin het programma zich inmiddels bevindt, en consistent wordt overgebracht zodat het in het DNA van de organisatie en iedere medewerker kan komen. Zodanig dat men het zó vanzelfsprekend vindt wat wordt gecommuniceerd dat het een gewoon onderdeel van normale interne processen en procedures wordt, geen extra aandacht behoeft en is verworden tot onze manier van 'verantwoord handelen'.

#5 Adequate organisatie

Een dergelijk ingrijpend en omvangrijk complianceprogramma kan niet door één persoon vanuit een klein kantoortje[26] worden verwezenlijkt. Integendeel, de boodschap zou juist vooral moeten doorklinken dat verantwoord handelen een verantwoordelijkheid is van iedere medewerker.
Een centrale '*business conduct office*' kan de ontwerper, coördinator en manager zijn van het gehele programma. Zo hoeft het wiel slechts eenmaal uitgevonden te worden, kan kostenefficiënt worden gewerkt (denk aan het inkopen van expertise, trainingen etc.) en ontstaat een expertisecentrum/vraagbaak in plaats van een aparte afdeling die er '*verantwoordelijk voor is dat elke medewerker zich aan de regels houdt*'.[27]

---

24. Zie bijvoorbeeld Dan Ariely, *Heerlijk oneerlijk*, Amsterdam: Maven Publishing 2012, p. 51, en Muel Kaptein, *Waarom goede mensen soms de verkeerde dingen doen*, Amsterdam: Business Contact 2011.
25. Richard Thaler & Cass Sunstein, *Nudge*, Amsterdam: Business Contact 2008.
26. Jaap van Maanen, van 2013-2018 voorzitter Monitoring Commissie Corporate Governance Code, verwoordde het als volgt: 'Het gaat dan om een duurzame manier van winst maken en het creëren van meerwaarde voor de onderneming. Daarbij speelt compliance een essentiële rol. Nog te vaak wordt compliance geïsoleerd benaderd en wordt volstaan met het benoemen van een persoon in een functie. De schandalen van de afgelopen jaren hebben aangetoond dat deze functie heel serieus moet worden genomen en de hele organisatie doordrongen moet zijn van het belang van compliance.', www.overondernemen.com/hr/bestuur/corporate-governance-verdient-de-volle-aandacht.
27. Die neiging bestaat althans in de bankensector waar de zwarte piet van overtredingen in de eerste lijn vaak bij het falen van de compliancefunctie (tweedelijns) lijkt te worden gelegd. Een dergelijke aanpak moeten we in de niet-financiële wereld pogen te vermijden.