

Integriteit in control: een praktische handleiding

Ed Creusen/Natascha Westen¹

Samenvatting

In de context van een integere bedrijfsvoering is het nodig het begrip integriteit als het ware te operationaliseren. Als aan een medewerker wordt gevraagd of hij/zij rechtschapen, onomkoopbaar en betrouwbaar is, zal het antwoord vrijwel altijd positief luiden. Deze abstracte noties helpen dus niet als we willen beoordelen of een organisatie en haar medewerkers integer zijn. In het voorgaande is aangegeven op welke manier integriteit in een organisatie toetsbaar kan worden gemaakt. Belangrijk onderdeel daarvan is een zekere mate van objectivering van het begrip. Een tekort aan integriteit (dat door de gemiddelde medewerker zo wordt ervaren) kan ook aanwezig zijn zonder dat de betrokkene zich daarvan bewust is. Maak integriteit bespreekbaar en geef het “handjes en voetjes”.

Integriteit kan een volwaardig en toetsbaar onderdeel worden van het compliance framework en de daarbij behorende periodieke rapportage.

Welke specifieke problemen op het gebied van integriteit kunnen zich voordoen bij het besturen van een pensioenfonds door met name *part-time* bestuurders? Er worden enkele praktische handvatten gegeven hoe part-time bestuurders zouden kunnen acteren om op een integere wijze tot oordeelsvorming te komen.

Inleiding

Maatschappelijke context

In de afgelopen decennia hebben boekhoud- en corruptieschandalen bij de overheid en in de marktsector veel aandacht getrokken. Ondanks veelal goedkeurende accountantsverklaringen en andere verklaringen/statements ging het fout. Belangrijkste oorzaken: een (te) weinig systematische naleving van (wettelijke) regels, alsmede een tekort aan integriteit.

Compliance is reeds lang een veel breder begrip dan alleen maar het voldoen aan wet- en regelgeving. Van organisaties wordt verwacht dat zij bij hun handelen rekening houden met de belangen van alle stakeholders zoals klanten, medewerkers, aandeelhouders, en ook maatschappelijke organisaties, bijvoorbeeld op het gebied van milieu. Daarom zijn compliance en vooral ook integriteit hoog op de politieke en toezichthouderagenda geplaatst, zowel nationaal als internationaal.

¹ Ed Creusen en Natascha Westen zijn Partner bij Compliance-i-Consultancy

Compliance en integriteit moeten veel steviger verankerd moeten worden binnen organisaties. Was voorheen de focus met name gericht op financiële instellingen, tegenwoordig wordt ook de aandacht steeds meer gericht op andere organisaties.

Organisaties –zowel in een overheidsomgeving als in de marktsector- zijn zich in toenemende mate bewust van het grote bedrijfsmatige belang van het beheersbaar houden dan wel meer beheersbaar maken van de compliance en integriteitrisico's. Door niet-integer gedrag van werknemers (op alle niveau's) en/of derden kunnen organisaties immers ernstig worden benadeeld, zowel in financieel als in reputatie opzicht. Daarnaast draagt een goede integratie van compliance en integriteit in de organisatie en haar processen bij aan de kwaliteit van de dienstverlening.

Bij dit alles moet wel de kanttekening worden geplaatst dat compliance en integriteit niet altijd 'kenbaar' zijn; er doen zich situaties voor waarin medewerkers weliswaar te goeder trouw zijn (ze zijn oprecht van oordeel dat ze alles correct doen), terwijl er toch sprake is van non-compliant of niet-integer gedrag.

Bij compliance vraagstukken speelt immers niet alleen het juridische perspectief een rol, maar zeker ook ethiek en risicobenadering. Met name deze laatste twee aspecten kunnen leiden tot zogenaamd 'onbewust onbekwaam' gedrag.

Hard en soft controls

In de praktijk wordt onderscheid gemaakt tussen de 'harde' en de 'zachte' kant van compliance. Met de harde kant wordt dan meestal bedoeld op de correcte naleving van wet- en regelgeving, alsmede de prudentiële kant van het toezicht, de financiële toestand van de organisatie. De zachte kant heeft het oog op gedragsaspecten, op integriteit. Risico's aan de harde kant worden beheerst door de zogenaamde 'hard controls', risico's aan de zachte kant door 'soft controls'. In de praktijk gaat het voornamelijk om het vinden van de juiste balans tussen hard en soft controls, want beide kunnen niet los gezien worden van elkaar. Soft controls ondersteunen de werking van hard controls, maar kunnen ook aanwezig zijn als er geen hard controls zijn. Anders dan de naamgeving doet vermoeden kunnen niet goed werkende soft controls onder omstandigheden ernstiger gevolgen hebben voor een organisatie dan niet goed werkende hard controls. Problemen met de integriteit in een organisatie kunnen de reputatie aantasten met alle mogelijke economische en financiële gevolgen van dien.

Wat is integriteit en hoe identificeer je de risico's?

Van Dale ² omschrijft integriteit als rechtschapenheid, onomkoopbaarheid. Dit omvat begrippen als eerlijkheid, oprechtheid en betrouwbaarheid. Dit zijn stuk voor stuk abstracte begrippen, die geoperationaliseerd moeten worden om ze in een organisatie te kunnen toepassen.

Overigens is deze notie van het begrip integriteit te beperkt, in elk geval in de context van het inrichten van een integere bedrijfsvoering. Zoals in de Inleiding aangegeven is het ook mogelijk dat een medewerker *onbewust* niet-integer gedrag vertoont. Er zijn voorbeelden van topmanagers die zich volstrekt te goeder trouw schuldig maakten aan belangenvermenging. Anders gesteld: het begrip integriteit kan (in zekere mate) worden geobjectiveerd. Een doorsnee persoon kan een bepaalde handelwijze niet-integer vinden ('men' vindt dit, dus een zekere mate van objectiviteit), terwijl een individu daar te goeder trouw anders over kan denken (subjectieve opvatting).

Operationalisering middels getrapte model

Operationalisering vindt plaats met behulp van een getrapte benaderingswijze.

Vanuit de hierboven genoemde abstracte notie worden voor een organisatie *risicocategorieën* op het gebied van integriteit gedefinieerd. Hierbij kan worden gedacht aan categorieën als belangenverstremgeling, handelen in effecten met voorwetenschap, fraude, benadeling van derden, onoorbaar handelen, een niet-integer behandeling van klanten, een verkeerde uitbesteding van werkzaamheden (aan een onvoldoende integere partij). Hierbij passen twee kanttekeningen.

In de eerste plaats is het moeilijk om scherp afgebakende categorieën te definiëren. Zo lopen bijvoorbeeld fraude, benadeling van derden en onoorbaar handelen in elkaar over. Niettemin is het nuttig ze afzonderlijk te benoemen.

In de tweede plaats kunnen de categorieën per branche verschillen vertonen. Integriteitrisico's zijn immers afhankelijk van de betreffende organisatie, bedrijfscultuur en de mate waarin de medewerkers zich bewust zijn van integriteit en integriteitrisico's. Zo zullen bijvoorbeeld in de branche pensioenen en verzekeringen deels andere risicocategorieën dominant zijn dan in de bouwwereld. Naarmate evenwel de categorieën meer een 'containerbegrip' zijn, zoals de hierboven genoemde, zullen de afwijkingen per branche minder groot zijn.

Nadat de integriteitrisico categorieën zijn gedefinieerd begint het 'echte' werk.

² Groot woordenboek van de Nederlandse taal

De toch nog tamelijk abstract geformuleerde risicocategorieën moeten vertaald worden naar *concrete integriteitrisico's*; deze kunnen per afdeling van een organisatie verschillen. Zo zal handelen in effecten met voorwetenschap met name spelen bij een afdeling vermogensbeheer, en belangenverstremgeling eerder bij een afdeling inkoop (vermenging van zakelijk en privé belang); fraude en onoorbaar handelen zullen zich bij meer afdelingen kunnen voordoen.

De vertaalslag naar concrete integriteitrisico's vergt een analyse van de bedrijfsprocessen per afdeling, waarbij wordt gezocht naar de processtappen die een integriteitrisico binnen een van de van toepassing zijnde risicocategorieën met zich meebrengen.

Een voorbeeld: hoe kan zich belangenverstremgeling bij een inkoopafdeling manifesteren? Door als medewerker privé 'mee te liften' met een inkooporder van de organisatie. Waar het nu om gaat is om in het inkoopproces te identificeren op welk moment (bij welke processtap) een medewerker de fout in kan gaan.

Het 'compliance proces' moet er derhalve in voorzien dat bij elke afdeling van een organisatie door de compliance functie alle bedrijfsprocessen worden geanalyseerd op processtappen die een integriteitrisico in zich hebben (binnen een van de integriteitrisico categorieën).

Deze procesanalyse vraagt veel van de creativiteit en het 'out-of-the-box' denken van de medewerkers die deze analyse moeten uitvoeren. *Creatief* out-of-the-box denken vergroot de praktische toepasbaarheid van het model. Het idee dat er integriteitrisico's worden gelopen kan gemakkelijk weerstanden oproepen. Het heeft een negatieve, misschien zelfs criminele, klank. Het is daarom belangrijk dat integriteittekorten niet vanzelfsprekend worden geassocieerd met handelen te kwader trouw, maar worden benaderd met een analytische, 'waardevrije' blik. Zoals in de Inleiding reeds is aangegeven kan 'onbewuste onbekwaamheid' ook leiden tot integriteittekorten, terwijl er geen sprake is van kwade trouw.

Nadat via bovenbeschreven methodiek de concrete integriteitrisico's voor de hele organisatie in kaart zijn gebracht, moet worden vastgesteld hoe deze risico's het beste kunnen worden beheerst; welke moeten bij voorkeur worden geëlimineerd, en welke worden aanvaardbaar geacht. Anders gesteld: op basis van de 'risk appetite' moet het beheersingsbeleid worden bepaald. Met andere woorden het geven van een oordeel over het intern beheersings- en controle instrumentarium.

De beheersing van de integriteitrisico's

Nadat de integriteitrisico's in een organisatie in beeld zijn gebracht is –zoals gesteld- het vraagstuk van de beheersing aan de orde.

Bij alle geïdentificeerde risico's zullen de risico beheersingstechnieken moeten worden geïnventariseerd en zal op basis van die inventarisatie een selectie moeten worden gemaakt van de toe te passen techniek(en).

Risk appetite

In de algemene leer inzake risicomanagement speelt de risicohouding ('risk appetite') een belangrijke rol bij de beantwoording van de vraag welke risico's wel en welke niet moeten worden beheerst. Beheersing kost immers geld. Een organisatie kan besluiten om bepaalde risico's te aanvaarden, zeker als de kosten ter beheersing onevenredig hoog zijn. Aanvaarding zal met name aan de orde zijn indien de kans dat een bepaald risico zich voordoet en de impact op de organisatie als het risico zich toch manifesteert, gering worden geacht. De bedrijfseconomische afweging geeft in dat geval de doorslag. In de literatuur wordt wel gesproken over een risiconeutrale instelling, een risiconemende instelling en een risico-averse instelling. De suggestie wordt dan gewekt dat een organisatie een van de drie houdingen kan aannemen. Het is evenwel heel goed mogelijk om per type risico een verschillende 'appetite' te hebben. Daarbij kunnen ook andere dan bedrijfseconomische motieven een rol spelen. Met name met betrekking tot integriteit is de vraag of een soepeler houding dan 'risico-avers' moreel-ethisch verantwoord is. Met andere woorden: dienen misschien andere overwegingen (dan bijvoorbeeld bedrijfseconomische) hier dominant te zijn om het risicobeheersingkader te bepalen. Dit kan er dan bijvoorbeeld toe leiden dat met betrekking tot het aanvaarden van integriteitrisico's een (bijna) zero tolerance geldt.

In dat geval moet de kans dat een integriteitrisico zich manifesteert derhalve nagenoeg geheel worden geëlimineerd.

Optimale beheersing/eliminatie van integriteitrisico's

Uitgaande van de wens om de in een organisatie geïdentificeerde integriteitrisico's zoveel mogelijk te elimineren is de vraag aan de orde welke *beheersingsmaatregelen* 'zwaar genoeg' zijn om dit doel te bereiken, dan wel zo veel mogelijk te benaderen. Vervolgens moet over de werking van die maatregelen *verantwoording* worden afgelegd.

Beheersingsmaatregelen

Ten minste twee instrumenten moeten worden ingezet om de beheersing zo goed mogelijk te laten verlopen.

1. Nadat de integriteitsrisico's per organisatieonderdeel zijn geïdentificeerd en vastgelegd, moet het (decentrale) lijnmanagement zich –in samenspraak met de compliance- en riskfunctie- beraden op maatregelen om de risico's zo veel mogelijk te elimineren (aanpakken bij de bron). Per geïdentificeerd risico dienen zoveel als mogelijk een of meer adequate beheersingsmaatregelen te worden ontworpen. Tevens moet worden vastgelegd hoe de implementatie van deze maatregelen in de bedrijfsprocessen wordt verankerd. De maatregelen moeten immers geen dode letter worden, de werking ervan moet periodiek worden getoetst, teneinde de mate van in control zijn te kunnen vaststellen.
2. Naast de onder het vorige punt beschreven 'hard controls' is het noodzakelijk om als een soort flankerende maatregel periodiek trainingen voor het management te organiseren. Deze dienen twee doelen. In de eerste plaats kunnen ze worden beschouwd als een beheersingsmaatregel waar 'harde' maatregelen niet voorhanden zijn. In de tweede plaats is het in elke organisatie nodig om voortdurend awareness te behouden voor de juiste *mindset* waar het integriteitvraagstukken betreft.
Deze trainingen, die onder het hoofdstuk 'soft controls' kunnen worden gerangschikt, moeten periodiek worden gevolgd door alle managementlagen: van Raad van Commissarissen, Raad van Bestuur tot aan het laagste operationele management. De 'tone at the top' is hier essentieel. Zodra de organisatie het gevoel krijgt dat integriteit alleen een feestje voor de werkvloer is, kunnen alle inspanningen verder worden gestaakt.

De inhoud van de "standaard" training is tweeledig.

Het eerste onderdeel bestaat uit het toelichten van de gedragscode van de organisatie. In de praktijk is gebleken dat dit nogal eens een 'eye-opener' is, die – met name bij het topmanagement- kan leiden tot schrikreacties ('dit heb ik dus altijd verkeerd gedaan').

Het tweede onderdeel is een dilemmaspel. Casusposities op het gebied van integriteit worden voorzien van een aantal mogelijke gedragingen/reacties op de geschetste casus. Plenair of in kleine groepjes wordt de casus bediscussieerd. Daarbij gaat het niet perse om goed of fout, maar vooral om redeneringen, waarom in een situatie een bepaalde gedragslijn wordt gevolgd. Het is zinvol om twee soorten casusposities te bespreken. Zowel situaties met een algemeen karakter, dat wil zeggen toepasbaar op iedereen, als situaties die zijn

toegesneden op de business van het bedrijfsonderdeel waar de training wordt gegeven.

De trainingen worden over het algemeen als zeer zinvol ervaren en leiden veelal tot een vergroot inzicht in het fenomeen integriteit, en hoe hiermee omgegaan kan worden.

Daarnaast kan ook een E-learning worden ingezet om met een bepaalde frequentie een aantal aspecten van de gegeven training te herhalen (vooral geschikt voor grotere organisaties); hierbij gaat het vooral om kenniselementen, zoals de inhoud van de gedragscode.

Naast de hiervoor beschreven standaard training levert Compliance-i-Consultancy maatwerk dat in overleg met de opdrachtgever tot stand komt.

Verantwoording

Na implementatie van de maatregelen zal de werking daarvan moeten worden aangetoond. De resultaten van de toetsing van de werking worden periodiek gemeld in een rapportage.

De rapportage bevat op het gebied van integriteit de volgende elementen:

- Een opsomming per organisatieafdeling van alle geïdentificeerde en vastgelegde integriteitrisico's.
- Per integriteitrisico een vermelding van de geïmplementeerde beheersingsmaatregel(en).
- Per integriteitrisico het resultaat van de toetsing van de werking van de bijbehorende beheersingsmaatregel(en).

Het voorgaande impliceert dat periodiek elk risico expliciet moet zijn bekeken; ook als er niets bijzonders is te melden zal dat moeten worden gerapporteerd. Op deze manier blijft er permanent awareness met betrekking tot de in de bedrijfsprocessen aanwezige integriteitrisico's.

Het -gedetailleerde- format van de rapportage wordt centraal voorgeschreven. Dit geeft de afdelingen guidance met betrekking tot de te verrichten werkzaamheden op het gebied van integriteit. Aldus heeft het format een dubbele functie: kaderstelling (vooraf) en verantwoordingsdocument (achteraf).

Het sluitstuk van de operatie is dat de (centrale) compliance functie al dan niet steekproefsgewijs controleert of het gestelde in de aangeleverde rapportages juist is.

Bijzondere integriteitrisico's

Al het voorgaande heeft betrekking op managementlagen die fulltime bij een organisatie zijn betrokken, en zich dus in beginsel te allen tijde op het juiste detailniveau kunnen laten informeren alvorens een beslissing te nemen.

Dit ligt anders bij organisaties die een parttime bestuur 'op afstand' hebben, zoals pensioenfondsen. Bij deze instellingen hebben sociale partners (werkgevers- en werknemersvertegenwoordigers) van oudsher een dominante rol in de governance. Niettemin zijn zij, afhankelijk van de omvang en complexiteit van de organisatie en afhankelijk van de functie, slechts enkele dagen per maand actief betrokken. Gedurende de resterende tijd vervullen deze personen vaak meerdere vergelijkbare functies. Deze structuur brengt ten minste twee integriteitrisico's met zich mee.

Vermenging van belangen

In de eerste plaats is er het risico van vermenging van belangen. Zoals gesteld hebben de hier bedoelde bestuurders veelal een aantal vergelijkbare functies, waarbij dezelfde typen problemen spelen. Enerzijds is dat positief, omdat de brede kennis en ervaring die hierbij worden opgedaan op meerdere plaatsen kunnen worden gebruikt. Anderzijds bestaat het gevaar dat bedrijfsgevoelige informatie van pensioenfonds A (onbewust) wordt aangewend om problemen bij pensioenfonds B op te lossen. En dat is natuurlijk niet de bedoeling; hier dienen integriteitrisico's zich aan.

Besluitvorming/standpuntbepaling gebaseerd op te weinig of verkeerde informatie

Een voor bestuurders veel lastiger vraagstuk is hoe te komen tot verantwoorde besluitvorming. Het bestuur van een pensioenfonds is eindverantwoordelijk voor alles wat zich afspeelt binnen het fonds. Op de bestuurstafel liggen vaak complexe dossiers ter besluitvorming. Gedacht kan worden aan bijvoorbeeld de vaststelling van de pensioenpremie of het goedkeuren van ingewikkelde vermogensbeheerconstructies. Een belangrijke vraag daarbij is steeds op basis van welke informatie en kennis het bestuur verantwoord een beslissing kan nemen. Een veelgehoorde opmerking uit bestuurskringen is dat de techniek iets is voor actuarissen, vermogensbeheerders en dergelijke, en dat het bestuur dan maar beslist op hun gezag. Dit is de verkeerde instelling! Een bestuur dat zo acteert kan worden verweten niet of onvoldoende integer te zijn.

Verantwoorde standpuntbepaling

Hoe kan een verantwoorde standpuntbepaling in zijn werk gaan? Uiteraard zullen part-time bestuurders in het algemeen niet alle technische details overzien. Dat hoeft ook niet, daarvoor kunnen zij gebruik maken van de kennis van experts (de genoemde actuarissen en vermogensbeheerders of anderen). Zij zullen zich door deze deskundigen moeten laten voorlichten over de verschillende keuzes die kunnen worden gemaakt met betrekking tot een bepaald vraagstuk. Bij die keuzemogelijkheden dienen de (maatschappelijke) implicaties van de verschillende keuzes integer en begrijpelijk in beeld te worden gebracht. Indien de bedoelde bestuurders de voorgelegde keuzes en de daarbij behorende maatschappelijke implicaties volledig doorzien kan een verantwoord standpunt worden genomen. Voorwaarde is uiteraard wel dat de informatiebronnen (de deskundigen) integer zijn. In dit

verband wordt daarmee bedoeld dat de informatieverschaffing objectief is, en niet gekleurd door (persoonlijke) voorkeuren.

Belangrijk in deze is dat de integriteit hiervan volledig transparant is door te zorgen dat de besluitvorming zichtbaar tot stand komt via dossiervorming. Zodat een bestuur ook daadwerkelijk kan laten zien aan een toezichthouder of een externe accountant waar en hoe het tot zijn besluit is gekomen.

Bij de standpuntbepaling is het dus van belang dat deze plaatsvindt via een transparant en evenwichtig proces. Transparant betekent dat alle ins en outs van de keuzemogelijkheden tijdens de bespreking van het voorstel ter tafel komen, zodat eenieder daarvan kennis kan nemen. Evenwichtig betekent dat de opbouw van de discussie logisch is (niet te snel 'jumping to conclusions'), en dat zoveel mogelijk wordt voorkomen dat een of enkele deelnemers aan de discussie een te dominante rol spelen. Het verdient aanbeveling een sterke gespreksleider te hebben (dat zal afhankelijk van de setting de bestuursvoorzitter of een ander zijn).

Indien het proces van standpuntbepaling zich afspeelt langs bovenbeschreven lijnen kan met een gerust hart worden gesteld dat de oordeelsvorming op een integere wijze heeft plaatsgevonden, ondanks het feit dat lang niet alle technische details worden begrepen.