De Integere Organisatie 2:

handreiking
voor een sluitend vangnet
voor ongewenst gedrag

Deze studie werd mogelijk gemaakt door subsidies van:
het Verbond van Verzekeraars
de Vereniging NCW, Centrum voor maatschappij-betrokken management van
de Vereniging VNO-NCW
het Ministerie van Justitie
het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Over de onderzoekers van Ethicon (www.ethicon.nl):
Muel Kaptein is docent aan de Faculteit Bedrijfskunde, directeur van Ethicon,
Centrum voor ethiekmanagement, Erasmus Universiteit Rotterdam,
en senior consultant bij een organisatieadviesbureau voor ethiek en integriteit.
Femke Buiter is als onderzoekster verbonden aan Ethicon.

Uitgave van:
Stichting Beroepsmoraal en Misdaadpreventie
Bezuidenhoutseweg 12
Postbus 93002
2509 AA Den Haag
Tel. 070 3490 400
www.npc-web.nl

De Stichting Beroepsmoraal en Misdaadpreventie functioneert onder auspiciën van het Nationaal Platform Criminaliteitsbeheersing en heeft als doel: vergroten van de alertheid en weerbaarheid tegen externe en interne criminaliteit in organisaties. Het bevorderen van integriteit speelt daarin een sleutelrol.
Eerder publiceerde de Stichting onder meer:
De Integere Organisatie: Het nut van een bedrijfscode.

Druk: Den Haag media groep, Rijswijk
Vormgeving: René Obertop, Zoetermeer

ISBN 90-5771-067-6

Een sluitend intern vangnet brengt samenhang tussen vertrouwenswerk, compliance, beveiliging en overige staffuncties die meldingen krijgen van ongewenst gedrag.

Dit boekje is met name bestemd voor:

Ondernemers en directeuren

Hoofden Personeelszaken, Juridische zaken en Kwaliteit

Vertrouwenspersonen

Bedrijfsbeveiligers

Compliance officers

Leden van ondernemingsraden

Leden van klachtencommissies en

Overige staffunctionarissen die meldingen (kunnen) krijgen van ongewenst gedrag.

Inhoudsopgave

pag.

In kaders genoemde organisaties:

Voorwoord

Integriteit loont. In een integere organisatie gaan mensen zorgvuldig om met de hun toevertrouwde bedrijfsmiddelen, er heerst onderling respect en met externe belangen wordt daadwerkelijk rekening gehouden. Diefstal, fraude en criminaliteit komen er minder voor en er is minder sprake van (seksuele) intimidatie, machtsmisbruik en andere ongewenste omgangsvormen. Een integere organisatie trekt loyale werknemers aan, geniet vertrouwen bij leveranciers en afnemers en heeft een streepje voor bij kapitaalverstrekkers. Kortom, integriteit loont.

U kunt integriteit managen. Een eerste stap in integriteitmanagement is dat u een code opstelt waarin u verantwoordelijkheden, waarden en normen vastlegt die gelden voor uw organisatie. Een noodzakelijke tweede stap is dat u dilemma's en schendingen signaleert en bespreekbaar maakt. In principe kan dat via de lijnorganisatie. Er dient echter tevens een vangnet te bestaan waar werknemers problemen die zij zien en ervaren, kunnen aankaarten.

In onze eerdere publicatie *De integere organisatie: het nut van een bedrijfscode* deden wij suggesties voor het ontwikkelen van een code. In dit boekje krijgt u een handreiking hoe u een vangnet op maat kunt inrichten. Daarvoor worden u enkele modellen aangereikt en treft u voorbeelden aan van bedrijven die stappen in deze richting hebben gezet.
Grotere organisaties kunnen voor een vangnet aanknopen bij de staffunctionarissen die thans al een belangrijke rol vervullen bij de signalering van ongewenst gedrag, te weten de vertrouwenspersoon, de afdeling Beveiliging en de *compliance officers*. Naar onze mening kunnen deze functionarissen hun werkzaamheden meer afstemmen, bijvoorbeeld door het inrichten van een *Helpdesk Integriteit* of het benoemen van een *integriteitcoördinator*. Kleinere organisaties kunnen een *integriteitfunctionaris* aanwijzen die misstanden en dilemma's signaleert en kanaliseert.

Ik denk dat dit boekje een goede aanzet kan vormen om intern het gesprek aan te gaan over het interne vangnet - met name met de hierboven genoemde functionarissen -. Wij zijn overigens zeer benieuwd naar uw ervaringen.

Ik wil hier Muel Kaptein en Femke Buiter, de onderzoekers van de Erasmus Universiteit, bedanken die het onderzoek hebben uitgevoerd, alsook de organisaties en experts die hebben meegewerkt aan dit rapport door hun informatie en visie te geven. Dit boekje zou niet verschenen zijn zonder de steun van:

- het Verbond van Verzekeraars,
- de Vereniging NCW, Centrum voor maatschappij-betrokken management van de Vereniging VNO-NCW,
- het Ministerie van Justitie, en
- het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

mr. Hans Tromp
voorzitter bestuur Stichting Beroepsmoraal en Misdaadpreventie

april 2001

Samenvatting

Leeswijzer

De lezer die geen tijd heeft, kan zich het beste beperken tot deze samenvatting en deel III (hoofdstuk 5, 6 en 7). Deel III beschrijft handvatten voor het opzetten en implementeren van een geïntegreerd intern vangnet om integriteitinbreuken te signaleren en aan te pakken. Deel I (hoofdstuk 1 en 2) toont waarom een dergelijk intern vangnet noodzakelijk is. Deel II (hoofdstuk 3 en 4) bespreekt de instanties die onderdeel vormen van een gangbaar vangnet.

Dit boekje biedt organisaties handvatten om te doordenken of de huidige organisatie voldoende alert is op normafwijkend gedrag. Een goede organisatie beschikt over een sluitend vangnet voor medewerkers om misstanden buiten de lijn aan de orde te stellen. Vanzelfsprekend dienen incidenten zoveel mogelijk binnen de lijn te worden opgelost. Toch ervaren medewerkers dikwijls drempels om laakbaar gedrag aan te kaarten. Dit leidt tot de volgende risico's:

- de incidenten gaan zich herhalen;
- de cultuur verziekt langzamerhand en de goede medewerkers zoeken een andere werkgever;
- het vertrouwen dat klanten, leveranciers, kredietverschaffers en politiek stellen in uw organisatie daalt met alle financiële gevolgen vandien; en
- medewerkers gaan met de incidenten naar de media.

Een open organisatie daarentegen 'leert' van incidenten en fouten, geniet vertrouwen bij stakeholders, krijgt lagere boetes in geval van wetsovertredingen van medewerkers en kan meer incasseren indien ongewenst gedrag zich voordoet. Bovendien werkt een open organisatie preventief doordat ongewenst gedrag wordt voorkomen.

In dit boekje wordt uitgewerkt hoe u een vangnet kunt inrichten. U krijgt enkele modellen aangereikt en zult voorbeelden aantreffen van bedrijven die stappen in deze richting hebben gezet. Hierna volgt een samenvatting per hoofdstuk.

Hoofdstuk 1: Het belang van integriteitmanagement

In een integere organisatie gaan management en medewerkers zorgvuldig om met de bedrijfsmiddelen, met elkaar en met de belangen van externen. Integriteitmanagement is noodzakelijk vanuit juridische overwegingen (‘het moet’), maar het is ook kostenbesparend (‘het loont’) en het verbetert het imago van de organisatie naar haar omgeving en het eigen personeel (‘het behoort’).

Hoofdstuk 2: Openheid als sleutelfactor

Het is beter om integriteitinbreuken te voorkomen dan te genezen. Toch zijn inbreuken niet volledig te voorkomen. Doen zich inbreuken voor, dan is het wenselijk dat de lijn dan wel de direct betrokken collega’s het incident signaleren, bespreken en waar nodig corrigerende acties ondernemen. Openheid is derhalve een belangrijk kenmerk van de integere organisatie. Interne openheid kan voorkomen dat medewerkers extern de spreekwoordelijke klok luiden over interne wanpraktijken. Als gevolg van de cultuur en structuur van Nederlandse organisaties wordt laakbaar gedrag niet altijd binnen de lijn gecorrigeerd en is een vangnet naast de lijn wenselijk.

Hoofdstuk 3: Loketten binnen huidige vangnetten

Veel organisaties beschikken over een intern vangnet naast de lijn in de persoon van bedrijfsmaatschappelijk werkers, bedrijfsartsen, ondernemingsraadsleden, vertrouwenspersonen, compliance officers, beveiligers, auditors en juristen. Ook staf-afdelingen als Inkoop, Milieu en Informatisering zijn dikwijls loketten waar medewerkers incidenten (kunnen) melden.

Hoofdstuk 4: Effectiviteit huidige vangnetten

De verschillende loketten zijn dikwijls onvoldoende op elkaar afgestemd waardoor er geen sluitend vangnet is voor misstanden en medewerkers van het kastje naar de muur worden gestuurd. Daarnaast heeft het management dikwijls te weinig zicht op de aard en omvang van de meldingen en wordt er te weinig geleerd van incidenten.

Hoofdstuk 5: Uitgangspunten en beslispunten voor een effectief vangnet

Voor het goed organiseren van een vangnet is het zaak om eerst na te gaan welke uitgangspunten de organisatie wenst te hanteren. Enkele van de in totaal negen besproken uitgangspunten luiden: laagdrempeligheid voor het melden van incidenten, duidelijke structuur van het vangnet, leren van incidenten en professionele afhandeling van meldingen. Daar waar deze uitgangspunten onderling conflicteren,

dienen organisaties keuzes te nemen. Enkele van de in totaal dertien besproken keuzes zijn: één loket of een loket per vraagstuk; centraal loket en/of decentrale loketten; een intern meldpunt en/of een extern meldpunt; toegankelijk voor medewerkers en/of voor externen; anoniem melding of met naam en toenaam?

Hoofdstuk 6: Modellen voor een geïntegreerd vangnet

Iedere organisatie dient te doordenken tot wie medewerkers zich buiten de lijn kunnen wenden om (vermeende) incidenten te melden op het gebied van bijvoorbeeld criminaliteit, misbruik van bedrijfsmiddelen en ongewenste omgangsvormen (de rol van meldpunt en hulpverlener). Daarnaast dient doordacht te worden wie onderzoek verricht naar de aard en ernst van de melding (de rol van onderzoeker) en wie advies uitbrengt aan de lijn over de te nemen maatregelen (de rol van adviseur).

Vertrouwenspersonen vormen een goed aanspreekpunt voor *slachtoffers* van ongewenste omgangsvormen. Met een vertrouwenspersoon kunnen slachtoffers het incident bespreken en in overleg bepalen welke vervolgstappen kunnen worden genomen (bijvoorbeeld bemiddeling of een klacht indienen bij de klachtencommissie). Voor *slachtofferloze incidenten* is de afdeling Beveiliging of een compliance officer meer voor de hand liggend om incidenten te melden. Juist binnen grote organisaties is, vanwege de specifiek benodigde deskundigheid, een diversiteit aan compliance officers wenselijk (bijvoorbeeld op het gebied van voorwetenschap, corruptie, privacy, nevenactiviteiten, internet, inkoop en verkoop).

Er zijn ten minste drie modellen denkbaar voor een geïntegreerd vangnet:

- *model 1*: een enkelvoudig vangnet waarbij medewerkers zich voor alle inbreuken kunnen wenden tot één persoon (*de integriteitfunctionaris*);
- *model 2*: een *meervoudig vangnet* waarbij per type inbreuk een ander loket is (waarbij de afstemming achter de schermen plaatsvindt door een *integriteitcoördinator*);
- *model 3*: een centraal meervoudig vangnet waarbij één centraal meldpunt zorg draagt voor de eerste opvang van melders en nagaat wie vervolgstappen neemt op de melding (het *Meldpunt Integriteit* of de *Helpdesk Integriteit*).

Met name voor grote organisaties is het wenselijk om de mogelijkheid te bezien van een *Helpdesk Integriteit* (model 3) waartoe alle medewerkers en managers zich kunnen wenden voor alle vermeende misstanden, dilemma's, kritiek en hulp. Het model van de Helpdesk Integriteit kenmerkt zich door een goede bereikbaarheid, lage drempels en een eenvoudige meldingsstructuur, waarbij medewerkers op een consistente wijze worden geholpen en adequate bewaking en rapportage mogelijk is. Bij een centrale helpdesk vindt er na de centrale intake een gedifferentieerde behandeling plaats op basis van het type incident. In het model van de helpdesk blijven de afzonderlijke instanties ook direct benaderbaar. Het functioneren van de *Integriteit-*

functionaris (model 1) is sterk afhankelijk van de persoonlijke kwaliteiten van de functionaris maar is minder anoniem dan de helpdesk. Dit biedt zowel voor- als nadelen. Het *meervoudige vangnet* (model 2) heeft als voordeel dat de rollen in het vangnet voor medewerkers duidelijk van elkaar worden gescheiden. De kwaliteit van de afstemming tussen de verschillende instanties staat of valt echter met de kwaliteit van de integriteitcoördinator. De drie modellen zijn ook te verbreden tot meldingen van externen over ongewenst gedrag van de organisatie en/of haar medewerkers.

Hoofdstuk 7: Implementatie van vangnet

De volgende factoren bevorderen de effectiviteit van een vangnet: het commitment van het management, een gedragscode voor de organisatie, adequate procedures voor bijvoorbeeld onderzoek, taakafbakening tussen de onderdelen van het vangnet, bescherming van de melders en daders, periodieke communicatie, rapportage aan het management en effectiviteitsmetingen onder bijvoorbeeld het personeel.

Gebruik van checklisten

Ieder hoofdstuk kent een eigen checklist die als bijlage in dit boekje is opgenomen. De hoofdstukken zijn zo geordend dat door achtereenvolgens de zeven checklisten in te vullen een plan ontstaat voor een effectief intern vangnet. De checklist kan worden ingevuld door de personen die verantwoordelijk zijn voor bijvoorbeeld integriteit, beveiliging of personeelszaken. Ook kan een projectteam worden samengesteld met daarin de functionarissen die vanuit hun staffunctie misstanden krijgen gemeld, aangevuld met ten minste één leidinggevende en iemand van de werkvloer. Het is veelal wenselijk om de checklisten één voor één te bespreken waarbij de projectteamleden eerst zelf de vragen beantwoorden en deze antwoorden vervolgens met elkaar bespreken. Vooral voor *Checklist 2, 5 en 6* is dit wenselijk.

Checklist 1 behandelt het nut en de noodzaak van integriteitzorg voor een organisatie: Waarom zou een organisatie aandacht aan integriteit moeten besteden? Wat zijn de kosten en de baten?
Checklist 2 helpt om de openheid binnen een organisatie in kaart te brengen: Wat is het zelfregulerend vermogen van afdelingen ten aanzien van integriteitinbreuken? Welke drempels ondervinden medewerkers als zij elkaar en hun leidinggevende aanspreken?
Checklist 3 biedt handvatten voor het beschrijven van het eigen huidige vangnet: Tot welke interne en externe instanties wenden medewerkers zich momenteel?

Met *Checklist 4* kan de effectiviteit van het huidige vangnet zichtbaar worden gemaakt: Wat zijn de sterke en zwakke kanten van het interne vangnet? Wat zijn de risico's? Welke meldingen blijven liggen?

Checklist 5 en 6 betreffen het vormgeven van de structuur van een eigen vangnet: Wat is voor een organisatie het meest geëigende interne vangnet? *Checklist 5* helpt bij het formuleren van de uitgangspunten en het maken van de belangrijkste keuzen. *Checklist 6* helpt bij het kiezen van het te hanteren model.
Checklist 7 reikt handvatten aan voor het effectief implementeren van het vangnet binnen een organisatie.

De checklisten zijn ook als bestand te downloaden vanaf www.npc-web.nl zodat ze eenvoudig te bewerken of te versturen zijn naar bijvoorbeeld leden van een werkgroep.

Deel I

De wenselijkheid van een intern vangnet

1 Het belang van integriteitmanagement

Bij integriteitmanagement binnen organisatie gaat het om het voorkomen van corruptie, misbruik en onzorgvuldig gebruik van bedrijfsmiddelen (zoals werktijd, bedrijfsinformatie, bedrijfsvoertuigen en communicatiemiddelen) en ongewenste omgangsvormen (zoals seksuele intimidatie, agressie en geweld). Dit hoofdstuk bespreekt waarom integriteitmanagement belangrijk is en welke rol een gedragscode daarbij vervult. Vanaf hoofdstuk twee zullen we zien op welke wijze organisaties kunnen omgaan met geconstateerde integriteitinbreuken.

Variatie in laakbaar gedrag

Recente onderzoeken tonen aan dat zich binnen Nederlandse organisaties allerlei vormen van laakbaar gedrag voordoen. Van fraude en diefstal tot discriminatie, lekken van vertrouwelijke informatie en ongewenste nevenactiviteiten. Geen enkele organisatie is brandschoon. Het is dikwijls niet de vraag óf zich laakbaar gedrag voordoet, maar in welke mate en met welke gevolgen. Een voorbeeld: In elk politiekorps komt seksuele intimidatie voor. Maar waar in het ene korps 19 procent van de medewerkers seksuele intimidatie in het eigen team constateert, geldt in een ander korps een percentage van 10.[1] Een vergelijking tussen 25 bedrijven leert dat roekeloos gebruik van bedrijfsmiddelen binnen ieder bedrijf voorkomt. Gemiddeld 57% van de medewerkers neemt dit in hun directe werkomgeving waar. Maar de bandbreedte (het verschil tussen de twee uitersten) is wel 75%![2]

Structuur en cultuur

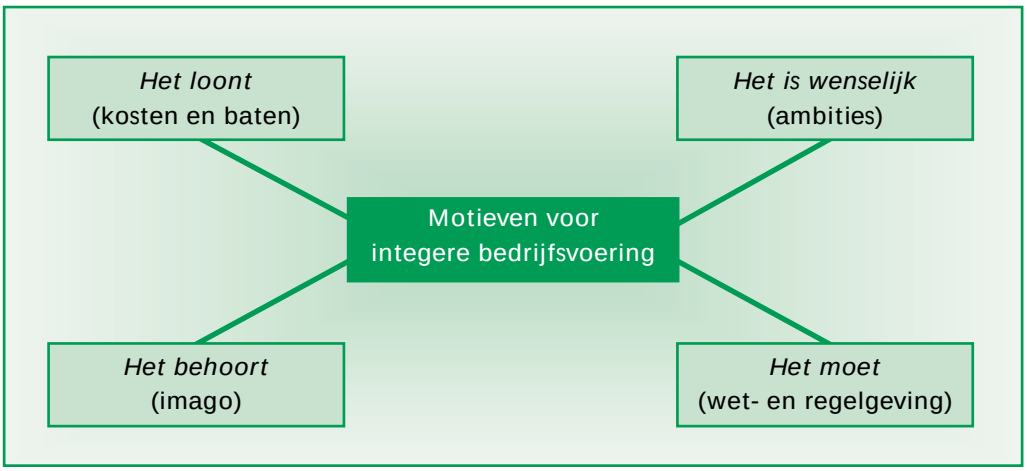
Enerzijds is laakbaar gedrag ook binnen organisaties onvermijdelijk. Anderzijds is laakbaar gedrag deels te voorkomen. De mate waarin schendingen binnen organisaties voorkomen, wordt sterk bepaald door het beleid dat een organisatie heeft ontwikkeld. Een gedragscode, functiescheiding en -roulatie, beveiliging en registratie van bedrijfsmiddelen zijn belangrijke maatregelen om laakbaar gedrag te voorkomen. De Luchthaven Schiphol constateerde 6 maanden na de introductie van haar bedrijfscode dat de schade aan bedrijfsvoertuigen met 19 procent was gedaald. Een

Rotterdams bedrijf bleek in staat om na een interne campagne de voorraadverschillen bijna te halveren. Zo komt in bedrijven waar een goed uitgewerkt beleid tegen seksuele intimidatie bestaat minder vaak seksuele intimidatie voor.[3] Daarnaast speelt de cultuur van een organisatie een minstens zo belangrijke rol. Geeft het management het goede voorbeeld? Gelden er realistische en ondubbelzinnige verwachtingen ten aanzien van de prestaties die medewerkers moeten leveren? Is binnen afdelingen bespreekbaar wat *done* en *not-done* is?

Vier redenen voor aandacht integriteit

Er zijn grofweg gesproken vier redenen waarom organisaties aandacht aan integriteit besteden. Aandacht aan integriteit vindt plaats vanuit (1) financiële, (2) immateriële/imago, (3) juridische en/of (4) persoonlijke motieven.

I. Motieven voor integere bedrijfsvoering



1. Financiële schade

Het geheel aan activiteiten en maatregelen dat een organisatie treft om laakbaar gedrag te voorkomen en moreel gewenst gedrag te stimuleren, is te vatten met de term integriteitmanagement. Integriteitinbreuken zijn dan die vormen van laakbaar gedrag waarbij evidente morele normen en waarden worden geschonden. Tabel II geeft een overzicht van de frequentie en consequentie van enkele integriteitinbreuken binnen Nederlandse organisaties.

II. Overzicht gevolgen van enkele integriteitinbreuken

Integriteitinbreuk	***Frequentie***	***Consequentie***
Interne criminaliteit	53% van de middelgrote bedrijven is de afgelopen drie jaar geconfronteerd met criminaliteit van eigen werknemers.[4]	Crimineel gedrag van medewerkers kost een middelgroot bedrijf gemiddeld *ƒ* 13.000 per jaar per organisatie.[5]
Fraude	Ruim 75% van bedrijven ervaart fraude als een belangrijk probleem voor de eigen organisatie.[6]	Gemiddeld schadebedrag van fraude voor de organisatie is *ƒ* 37.000.[7]
Privé-gebruik internet	19% van de werknemers constateert dat er op hun afdeling regelmatig tot vaak onder werktijd privé-gebruik gemaakt wordt van internet.[8]	5% van de werktijd gaat verloren aan privé-gebruik van internet.[9]
Agressie en geweld	36% van werknemers is op het huidige werk geconfronteerd met agressie en geweld.[10]	Agressie en geweld leiden tot verdubbeling van het verloop.[11]
Sexuele intimidatie	10% van werknemers is op het huidige werk geconfronteerd met sexuele intimidatie.[12]	Intimidatie leidt tot verdubbeling van het verloop.[13]
Pesten	16% van werknemers is op het huidige werk gepest.[14]	Een slachtoffer van pesterijen kost de organisatie gemiddeld *ƒ* 56.000 (bijvoorbeeld door lagere arbeidsproductiviteit, ziekte en verloop).[15]
Discriminatie	19% van werknemers constateert aanzienlijke discriminatie binnen de eigen afdeling.[16]	Discriminatie leidt tot stijging van ziekteverzuim met ruim 25%.[17]

Uit tabel II blijkt dat integriteitinbreuken geld kosten. Een adequaat integriteitprogramma voorkomt inbreuken en reduceert de daarmee gepaard gaande schade.

2. De immateriële baten

Bij integriteitzorg gaat het niet alleen om het reduceren van financiële schade. Belangrijke drijfveer is dikwijls het imago van de organisatie dat in het geding is. Het imago van een betrouwbare werkgever waar medewerkers niet het slachtoffer worden van ongewenste omgangsvormen. Het imago van een betrouwbaar beleggingsfonds, waar medewerkers niet op basis van voorkennis in aandelen handelen. Of bijvoorbeeld het imago van een betrouwbare afnemer, waar inkopers zich niet laten leiden door de leverancier die hen het meest fêteert. 73 procent van de Nederlandse bedrijven ontwikkelt anti-corruptiebeleid vanuit imago-overwegingen.[18] 80 procent van de Nederlandse consumenten laat zich bij de aankoop van producten leiden door de mate waarin het bedrijf eerlijk zaken doet en maatschappelijk verantwoord onderneemt. De helft van de bedrijven met een integriteitcode wil daarmee tegemoetkomen aan de wensen vanuit de samenleving, aangeven waar het bedrijf voor staat en de betrouwbaarheid van de organisatie onderstrepen.[19] 40 procent van de gemeenten stelt een code op om het imago naar derden te verbeteren.[20]

3. Wettelijke verplichtingen

Naast het feit dat integriteitinbreuken tot financiële schade kunnen leiden en integriteit bijdraagt aan een betrouwbaar imago, wordt aandacht voor integriteit ook ingegeven door de wet. Zo vereist de Arbo-wet sinds 1994 dat werkgevers een beleid ontwikkelen om werknemers te beschermen tegen seksuele intimidatie, agressie en geweld. Dit heeft tot gevolg gehad dat 18 procent van de Nederlandse organisaties in de daarop volgende vijf jaar beleid tegen seksuele intimidatie heeft ingesteld en 11 procent tegen agressie en geweld. Tabel III vermeldt voor uiteenlopende integriteitvraagstukken de relevante wetsartikelen.

Vraagstuk	***Wetsartikelen***
Fraude	'Hij die een geschrift dat bestemd is om tot bewijs van enig feit te dienen, valselijk opmaakt of vervalst, met het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken, wordt als schuldige aan valsheid in geschrifte gestraft, met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.' *(Wetboek van Strafrecht, art. 225 lid 1)* 'Hij die opzettelijk enig goed dat geheel of ten dele aan een ander toebehoort en dat hij anders dan door misdrijf onder zich heeft, wederrechtelijk zich toe-eigent, wordt, als schuldig aan verduistering, gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vijfde categorie.' *(Wetboek van Strafrecht, art. 321)*
Intimidatie / machtsmisbruik	'De werkgever voert, binnen het algemene arbeidsomstandighedenbeleid, een beleid tegen seksuele intimidatie en tegen agressie en geweld.' *(Arbeidsomstandighedenwet, art. 4 lid 2)*
Corruptie	'Het is den ambtenaar in zijn ambt verboden, anders dan met goedvinden van het bevoegd gezag, vergoedingen, beloningen, giften of beloften van derden te vorderen, te verzoeken of aan te nemen.' 'Het aannemen van steekpenningen is onvoorwaardelijk en ten strengste verboden.' *(ARAR, art. 64 lid 1 en 2)*
Discriminatie	'De werkgever mag geen onderscheid maken tussen mannen en vrouwen bij het aangaan van de arbeidsovereenkomst, het verstrekken van onderricht aan de arbeider, in de arbeidsvoorwaarden, bij de bevordering en bij de beëindiging van de arbeidsovereenkomst.' *(Burgerlijk Wetboek, art. 7A:1637ij)*
Nevenactiviteiten	'De ambtenaar is verplicht aan Onze Minister, op een door Onze Minister te bepalen wijze, opgave te doen van de nevenwerkzaamheden die hij verricht of voornemens is te gaan verrichten, die de belangen van de dienst voorzover deze in verband staan met zijn functievervulling, kunnen raken.' 'Het is de ambtenaar verboden nevenwerkzaamheden te verrichten waardoor de goede vervulling van zijn functie of de goede functionering van de openbare dienst, voorzover deze in verband staat met zijn functievervulling, niet in redelijkheid zou zijn verzekerd.' *(ARAR, art. 61 lid 1 en 3)*

III. Enkele relevante wetsartikelen (vervolg)

Vraagstuk	Wetsartikelen
Voorwetenschap	'Het is eenieder verboden om, beschikkende over voorwetenschap, in of vanuit Nederland een transactie te verrichten of te bewerkstelligen in a) effecten die zijn genoteerd aan een op grond van artikel 22 erkende effectenbeurs dan wel aan een buiten Nederland gevestigde en van overheidswege toegelaten effectenbeurs of effecten waarvan aannemelijk is dat deze spoedig aan een zodanige beurs zullen worden genoteerd; of b) effecten waarvan de waarde mede wordt bepaald door de waarde van onder a bedoelde effecten.' *(Wet toezicht effectenverkeer, art. 46 lid 1)*
Vertrouwelijke informatie	'Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.' *(Wetboek van Strafrecht, art. 272)*

4. Persoonlijke ambities

Ten slotte wordt in toenemende mate integriteitbeleid ontwikkeld omdat de ondernemer, directeur of de leidinggevende vanuit persoonlijke overtuiging een organisatie wil leiden die staat voor bepaalde normen. Een organisatie waarin men elkaar kan vertrouwen, waarin sprake is van respect en waarin zorgvuldig wordt omgegaan met toebedeelde verantwoordelijkheden en middelen. Een integere organisatie omdat men dat nu eenmaal wil en met minder geen genoegen neemt.

Persoonlijke integriteit

"Ik vind het ... heel belangrijk dat je normen hebt; dat je op een gegeven moment zegt: 'en dan maar niet'... Consistentie in je gedrag is heel erg belangrijk. Ik wil eigenlijk na elke transactie, zelfs een ontslag, iemand in de ogen kunnen kijken. Zo zelfs, dat we met elkaar nog een borrel kunnen drinken...Dat is voor mij een belangrijke *driver*".

Marten Pieters, lid van de Raad van Bestuur van KPN [21]

De bedrijfscode

Steeds meer organisaties ontwikkelen vanwege bovenstaande motieven beleid op het gebied van integriteit. Zo beschikte in 1999 38 procent van de grootste 100 bedrijven over een eigen code.[22] Ten minste 50 gemeentes hebben een eigen gedragscode.[23] 53 procent van de Nederlandse beroepsbevolking geeft aan dat de organisatie waarbij zij werkzaam zijn een gedragscode heeft.[24] In het boekje *De Integere Organisatie: Het nut van een bedrijfscode* wordt uiteengezet dat de meeste bedrijven die hun integriteit willen managen, een gedragscode als centraal instrument inzetten.[25] Een gedragscode verwoordt wat de verantwoordelijkheden van de organisatie jegens medewerkers en externe partijen zijn. Een code geeft dikwijls ook aan welke plichten medewerkers hebben om aan die verantwoordelijkheden gestalte te geven.

Eveneens wordt dikwijls belicht op welke wijze medewerkers dienen om te gaan met de bedrijfsmiddelen en met elkaar. “Wat zijn onze omgangsvormen?”, “Welke nevenactiviteiten zijn toelaatbaar?” en “Wat is ons beleid ten aanzien van geschenken?” zijn enkele vragen die dikwijls in een code worden aangesneden. Ook enkele ministeries (zoals het ministerie van VROM en SZW), de Nederlandse politie (het Integriteitstatuut), onderwijsinstellingen (zoals de Erasmus Universiteit Rotterdam) en beroepsgroepen (zoals inkopers en bedrijfsbeveiligers) hebben een eigen code. Ruim driekwart van de bedrijven met een bedrijfscode geeft aan dat zij daarmee de normen die voor de werknemers gelden, willen verduidelijken, bevestigen of bespreekbaar maken. De helft van de bedrijven met een code geeft aan dat zij werknemers daar ook echt op aan wil spreken.[26]

Met een code pogen organisaties integriteitincidenten te voorkomen. Immers, voorkomen is beter dan genezen. Tegelijk leert de praktijk dat ondanks goede voorzorgsmaatregelen zich toch incidenten kunnen voordoen. De vraag is dan ook op welke wijze men adequaat met deze incidenten om kan gaan. Het volgende hoofdstuk onderbouwt dat een open organisatie van groot belang is. Een code is daarbij dikwijls wel noodzakelijk, maar niet voldoende.

1 Gebaseerd op een integriteitenquête binnen politieregio's. Zie voor enkele achtergronden van dit onderzoek: P. van Reenen & M. Kaptein (1998), 'Ethiek en praktijk van politiewerk: wat weten we ervan?', In: Reenen, P. van (Red.), *De Geest van Blauw*, Politiestudies 23, Gouda Quint: 39-63.
2 Gebaseerd op een database van onderzochte bedrijven met behulp van een zogenaamde Integriteitthermometer. Zie voor beschrijving van deze Integriteitthermometer: M. Kaptein (1998), *Ethics Management*, Dordrecht: Kluwer Academic Publishers.
3 Dit blijkt uit een onderzoek dat de NIA in 1993 in opdracht van het Ministerie van SZW heeft uitgevoerd bij 50 bedrijven die minstens een jaar bezig zijn met een beleid tegen seksuele intimidatie.
4 Dit blijkt uit onderzoek van de Stichting Trendmeter onder ruim 400 algemeen directeuren van middelgrote Nederlandse ondernemingen (20-500 werknemers) in april 2000.
5 Stichting Trendmeter (2000), *Trendmeter van het Middenbedrijf*.
6 Wolde, J. ten (1997), Fraude: *Signaleren en voorkomen*. Controlling in de Praktijk 22. Kluwer Bedrijfsinformatie.
7 Wolde, J. ten (1997), Fraude: *Signaleren en voorkomen*. Controlling in de Praktijk 22. Kluwer Bedrijfsinformatie.
8 Kaptein, M. (2001), De Integriteitsbarometer: resultaten van een onderzoek naar de integriteit van Nederlandse organisaties, *Bedrijfskunde*.
9 *KPMG Fraude Onderzoek 2000*, (2000), KPMG Forensic & Integrity Services, Amstelveen: KPMG.
10 Ministerie van Sociale Zaken en Werkgelegenheid (2000), *Evaluatie Arbo-wet*.
11 Het ziekteverzuim bij lichamelijk geweld ligt per persoon 10,5 dagen per jaar hoger, bij ongewenste seksuele belangstelling is dit 17,3 ziektedagen. Zie TNO Arbeid (1999), *Geweld, Intimidatie en Discriminatie in de Europese Unie.*
12 Ministerie van Sociale Zaken en Werkgelegenheid (2000), *Evaluatie Arbo-wet over Seksuele Intimidatie, Agressie en Geweld en Pesten op het Werk.*
13 Zie TNO Arbeid (1999), *Geweld, Intimidatie en Discriminatie in de Europese Unie.*
14 Ministerie van Sociale Zaken en Werkgelegenheid (2000), *Evaluatie Arbo-wet over Seksuele Intimidatie, Agressie, Geweld en Pesten op het Werk.*
15 Walter, H. (1995), *Van Kwaad tot Erger: Pesterijen en psychoterreur op het werk*, Thema, Zaltbommel.
16 Kaptein, M. (2001), De Integriteitsbarometer: resultaten van een onderzoek naar de integriteit van Nederlandse organisaties, *Bedrijfskunde*.
17 TNO Arbeid (1999), *Geweld, Intimidatie en Discriminatie in de Europese Unie*.
18 Good Company (2000), *Opereren tussen macht en onmacht*, Ministerie van Economische Zaken.
19 Kaptein, M., Klamer, H., & Linden, ter J. (1999), *De Integere Organisatie: Het nut van een bedrijfscode*. NCW, KPMG en Stichting Beroepsmoraal en Misdaadpreventie, Den Haag Media Groep, Rijswijk.
20 Schumacher, G.M. (1997), *Gedragscodes in Gemeenten*, Afstudeerscriptie Erasmus Universiteit Rotterdam.
21 Graafland, J., Kaptein, M., Klamer, H., & Oorschot, A. (2000), *Binnenkamers: Ondernemers over dilemma's en geloof*, Meinema.
22 Zie noot 19.
23 Niemeyer, B., Huisman, W., & Beyers, G. (1997), *Gemeentelijk Integriteitsbeleid: Een blik op de praktijk*. Den Haag: VNG.
24 Op basis van onderzoek onder 1000 leden van de beroepsbevolking in 2000 door M. Kaptein.
25 Zie ook Kaptein, M., & Klamer, H. (2000), De bedrijfscode als effectief managementinstrument, *Holland Harvard Review*, 17(72): 22-27.
26 Zie noot 19.

2 Openheid als sleutelfactor

Horen, zien en bespreken (in plaats van zwijgen) kenmerken de integere organisatie. Niet alleen worden daarmee integriteitincidenten voorkomen, maar ook een omgeving geboden waarin incidenten adequaat opgepakt kunnen worden.

Risico's van gedogen

Al zullen integriteitinbreuken nooit geheel zijn te voorkomen, in alle gevallen is het van belang dat een organisatie incidenten vroegtijdig signaleert. Immers waar zicht ontbreekt, blijven maatregelen uit. Signalering kan ertoe leiden dat:

- *de nadelige gevolgen* van de overtreding of inbreuk worden beperkt. Door vroegtijdig te signaleren, kunnen mogelijkerwijs nog tegenmaatregelen of verzachtende maatregelen worden getroffen. Zo kan het vroegtijdig herkennen van een slachtoffer van intimidatie voorkomen dat de persoon wegens psychische klachten lange tijd uitgeschakeld raakt;
- de kans op *herhaling* door dezelfde persoon afneemt. Wanneer een overtreder niet wordt gepakt, neemt de kans op herhaling toe. De drempel wordt immers steeds lager;
- de kans op *overtredingen van meer ernstige aard* door dezelfde persoon afneemt. Een grote crimineel begint dikwijls als kruimeldief. Wanneer een overtreding wordt gedoogd, zal de overtreder minder morele bezwaren hebben om de volgende keer een overtreding van meer ernstige aard te begaan;
- wordt voorkomen dat het *klimaat verloedert*. Ongecorrigeerd laakbaar gedrag kan bij omstanders tot de opvatting leiden dat de organisatie kennelijk niet zo zwaar tilt aan de naleving van afspraken. De opvatting "En waarom zou ik mij moreler gedragen dan mijn collega?" opent de deur voor navolging;
- de overtredingen worden gecorrigeerd en daarmee de *organisatienorm wordt onderstreept*. Juist uit hetgeen gesanctioneerd wordt, blijkt welke normen de organisatie feitelijk hanteert. Een manager die zijn medewerkers aanspreekt op overmatig privé-bellen tijdens werktijd, creëert daarmee een norm. Daarentegen tasten ongecorrigeerde overtredingen de geloofwaardigheid van de betreffende normen juist aan;

- de kans op overtredingen afneemt. Adequate signalering en tegenmaatregelen werpen hun schaduw vooruit. Het besef dat normafwijkend gedrag niet alleen wordt gesignaleerd maar ook wordt aangepakt, werkt op zich al als *afschrikmiddel*. Veelal bekennen fraudeurs die tegen de lamp zijn gelopen, dat zij stellig van mening waren dat zij de dans wel zouden kunnen ontspringen;
- er *preventief beleid* kan worden gevoerd. Als er niet wordt geleerd van gemaakte fouten of tekortkomingen in de organisatie, blijft de kans bestaan dat soortgelijke incidenten zich ook op andere plekken binnen de organisatie voordoen.

Correctie vraagt structuur en cultuur

Structurele maatregelen zijn nodig om vroegtijdig laakbaar gedrag te signaleren. Voorbeelden van deze maatregelen zijn: controle op bijvoorbeeld kasverschillen, op privé-transacties van aandelen, internetgebruik, werktijden, verbruik bedrijfsmiddelen en op voorraadverschillen. Tegelijk zullen monitoringsystemen nooit een sluitend geheel zijn. Het is immers onmogelijk alle gedragingen van medewerkers op de voet of indirect te volgen. Bovendien is het dikwijls ook onwenselijk vanuit kostenoverwegingen en in strijd met het vertrouwen dat medewerkers verwachten. De organisatiecultuur is dan ook een noodzakelijke aanvulling op structurele maatregelen. Kenmerken van een dergelijke cultuur zijn zicht op elkaars handelen en bespreekbaarheid van laakbaar gedrag (transparantie).

Sociale controle

De rol van de leidinggevende is van cruciaal belang voor het vroegtijdig signaleren van normafwijkend gedrag. Een leidinggevende dient over vaardigheden te beschikken om signalen te herkennen. Daarnaast dient hij over capaciteiten te beschikken om mensen op de juiste wijze aan te spreken en dient hij het lef te hebben om desnoods sancties te nemen. Naarmate medewerkers zelfstandiger worden en taken verrichten die moeilijker door de directe leidinggevende te controleren zijn, wordt sociale controle steeds belangrijker. Over het algemeen zijn collega's beter op de hoogte van elkaars misstappen dan hun leidinggevende.[27] Daarom is het van belang dat medewerkers elkaar kunnen aanspreken op vermeend laakbaar gedrag. Dit vereist zowel een open houding bij degene die wordt aangesproken als moed en lef bij degene die aanspreekt.

ECT over openheid

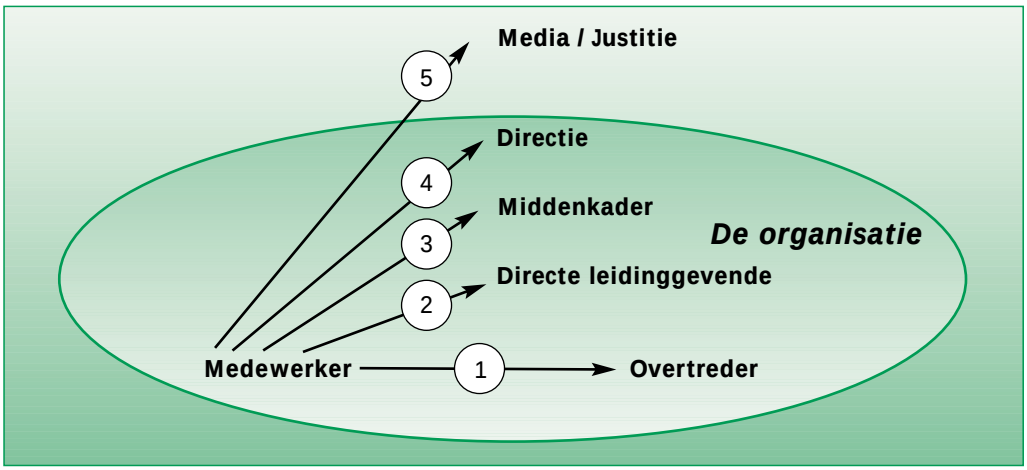
"...Alleen wie vervuld is van eigenwaan luistert niet naar anderen... We geven frank en vrij onze mening, omdat we weten dat er naar ons wordt geluisterd en dat onze eerlijke mening nooit 'tegen ons' zal worden gebruikt... Openheid wordt niet opgevat als een teken van zwakte, maar eerder van moed... Van kritiek kunnen we leren, mits we ons aangesproken voelen... Niemand hoeft bang te zijn voor negatieve consequenties, ook als mocht blijken dat hij zich bij het uiten van opbouwende kritiek heeft vergist."

ECT Gedragscode Correct

Hoe een incident bespreekbaar maken?

In de ideale situatie zal een medewerker indien hij laakbaar gedrag van een collega constateert, hem er direct op aanspreken. De gewenste code voor correctie van misstanden is dan ook dat (1) de direct betrokkene (gedupeerde dan wel getuige) eerst de overtreder zelf aanspreekt. Reageert deze niet naar wens, en gaat het om substantiële zaken waar gegronde twijfel over is, dan (2) wordt de direct leidinggevende op de hoogte gesteld. Blijft ook hierna de gewenste actie uit, dan (3) kan het middenkader worden gevraagd actie te ondernemen. Blijven acties uit, dan wordt (4) de top ingeschakeld. Blijft uiteindelijk ook de top in gebreke en gaat het om ernstige vergrijpen waar de medewerker gegronde vermoedens over heeft, dan is het moreel gezien niet alleen mogelijk maar ook wenselijk om (5) externen zoals de media op de hoogte te stellen. In die gevallen wordt extern de spreekwoordelijke klok geluid ('whistle blowing'). De cijfers bij deze vijf alternatieven zijn weergegeven in figuur IV.

IV. Code voor sociale correctie[28]

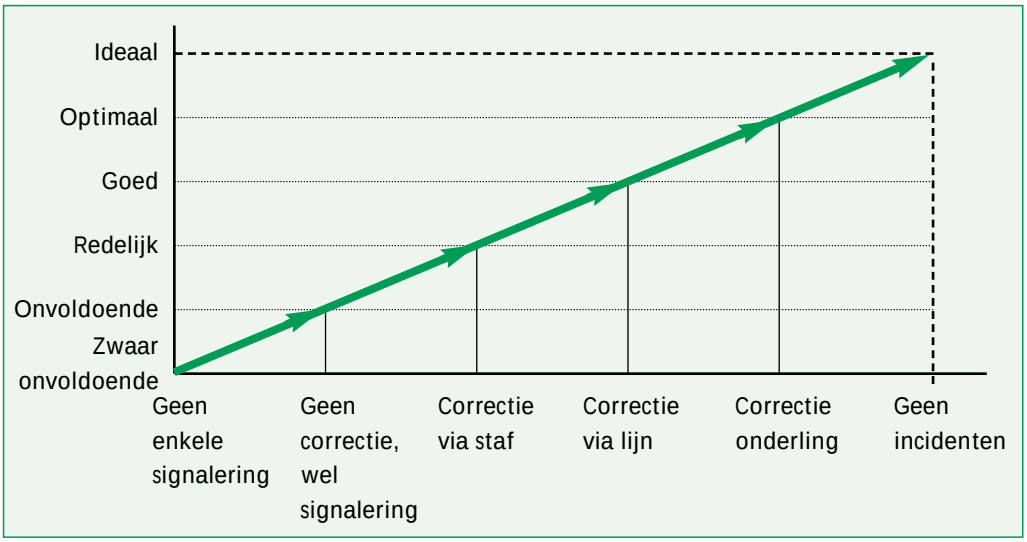


Naarmate laakbaar gedrag hoger in de organisatie wordt aangekaart, dient over het algemeen (a) de melder vrij zeker te zijn dat de vermeende overtreding zich feitelijk heeft voorgedaan en (b) de overtreding van ernstige aard te zijn. Een medewerker die constateert dat een collega regelmatig op zijn werk privé belt, kan dit bespreekbaar maken op zijn afdeling en eventueel bij het naast hogere echelon. Wanneer het slechts om bescheiden laakbaar gedrag gaat zonder aanzienlijke schade, is het niet nodig de directie hierover in te lichten. Gaat het echter om systematisch gesjoemel met omzetcijfers van een afdeling, dan ligt het eerder voor de hand de 'weg naar boven' langer te volgen. Kortom, openheid is wenselijk, maar wel onderbouwd en op het juiste niveau.

Niveaus van correctie

Op basis van de gewenste code voor correctie van misstanden is een zestal niveaus te onderscheiden in de mate waarin correctie plaatsvindt. Naarmate een organisatie meer naar rechts op de schaal zit, staat zij er beter voor.

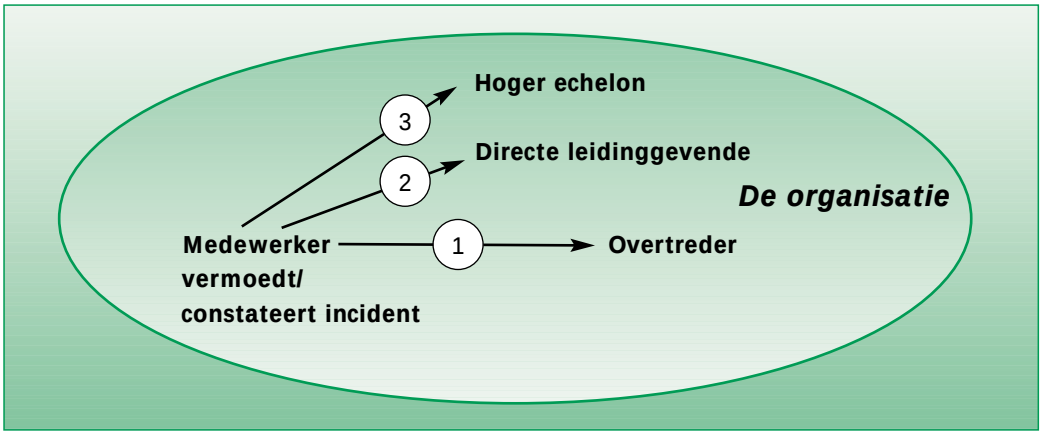
V. Zes niveaus van interne correctie



Drempels voor kritiek

Het is niet vanzelfsprekend dat de gewenste code voor interne correctie wordt gevolgd. Er kunnen drempels zijn om elkaar aan te spreken, bijvoorbeeld bij (1) de overtreder, (2) de directe leidinggevende en (3) het hogere echelon. Het gaat daarbij niet alleen om feitelijke drempels die er bestaan, maar juist ook om de perceptie van medewerkers dat er drempels bestaan.

VI. Drempels voor ventileren kritiek



1. Drempels naar de overtreder

Slechts één op de vier medewerkers zegt dat de overtreder reageert op de poging tot correctie.[29] Redenen die medewerkers daarvoor aandragen zijn onder meer:

- degene die aanspreekt wordt *weggewimpeld* als zijnde bemoeial, betweter of moralist (“Je bent zeker door de baas gestuurd?”);
- degene die aanspreekt krijgt direct de *bal terug* doordat de overtreder wijst op de balk in zijn eigen oog (“Als jij mij aanspreekt, dan weet ik ook nog wel het nodige over jou.”);
- de overtreder dreigt met *tegenacties* (“Als jij mij de maat neemt, dan zal ik jou daar zeer zeker betaald voor zetten.”);
- de overtreder is van mening dat *iedereen het doet* en hij niet de juiste geadresseerde is van de kritiek (“Als je mij aanspreekt, dan moet je iedereen aanspreken.”);
- de overtreder erkent wel dat hij niet netjes heeft gehandeld, maar *bagatelliseert* de gevolgen ervan (“Zo erg is dat toch niet? Waar maak je je nou druk om?”);
- de overtreder is van mening dat hij *recht heeft* op het toe-eigenen van de bedrijfsmiddelen (“Wie appelen vaart, die appelen eet.”).

2. Drempels naar direct leidinggevenden

Gevolg van bovenstaande reacties is dan ook dat kritiek in dit soort situaties in de kiem wordt gesmoord. Het vervolgens op de hoogte stellen van de leidinggevende valt echter ook niet altijd in goede aarde. Slechts één op de drie werknemers zegt dat zijn leidinggevende openstaat voor kritiek op het gedrag van een collega.

Redenen die werknemers daarvoor aandragen zijn onder andere:

- de werknemer wordt als *klikspaan* gezien (of denkt als klikspaan te worden gezien) en doorbreekt daarmee het saamhorigheidsgevoel van het team;
- de leidinggevende is van mening dat hij *zelf in staat* is signalen van niet-integer gedrag op te vangen en daarbij niet afhankelijk is van zijn medewerkers;
- de leidinggevende *stuurt de medewerker terug* met de opdracht het probleem zelf op te lossen (“Zeg maar dat ik achter je sta.”);
- de overtreder onderneemt *ondermijnende acties* of begint een tegenoffensief.
- de leidinggevende wil niet het risico lopen dat met dit voorval de beerput wordt opengetrokken;
- vanwege de *onduidelijkheid* over welke normen in het geding zijn, is er ook geen grond om de overtreder aan te spreken (“Zolang we er niets over hebben afgesproken, kan ik hem er ook niet op aanspreken.”);
- de leidinggevende is *mede schuldig* aan het incident en wil zichzelf buiten schot houden door de melding in de doofpot te stoppen;
- de leidinggevende is er *mede verantwoordelijk* voor dat het incident heeft kunnen plaatsvinden en wenst niet dat dit zichtbaar wordt.

3. Drempels naar een hoger echelon

Als ook de melding aan de direct leidinggevende niet het gewenste effect heeft gehad, kunnen medewerkers de inbreuken nog hoger in de lijn aan de orde stellen. Hier kunnen zij echter op onder andere de volgende drempels stuiten:

- het aan de orde stellen wordt als een *motie van wantrouwen* naar collega’s en leidinggevende opgevat (kennelijk is het team niet zelf in staat om het eigen schip schoon te houden);
- het aan de orde stellen wordt als *groepsverraad* beschouwd (de melder kiest voor het organisatiebelang en hangt de vuile was buiten);
- het naast hogere echelon verwijst de melder terug omdat het zich *niet verantwoordelijk* voelt voor de problemen van het lagere echelon;
- het naast hogere echelon *ontbreekt de tijd of de prioriteiten* om zich over dergelijke vraagstukken te buigen.
- met het buiten de afdeling aan de orde stellen van het incident, wordt het conflict *op scherp* gezet (er is dikwijls immers geen weg meer terug);

- naarmate de overtreding meer deel uit maakt van de *cultuur* van de organisatie, zal het hogere echelon minder ontvankelijk zijn voor overeenkomstige meldingen. Het tegen de stroom oproeien is dan ook voor de melder geen aanlokkelijk vooruitzicht;
- voor medewerkers is het dikwijls onduidelijk wat de relatie is tussen hun eigen leidinggevende en zijn/haar leidinggevende: zijn het vier handen op één buik of is het een vat dynamiet? In beide gevallen kan een melding een *averechts effect* hebben en ontbreekt de melder de zekerheid dat er op een zorgvuldige wijze met zijn melding wordt omgesprongen.

Amerikaanse wetgeving

Sinds 1991 gelden in Amerika de *U.S. Federal Sentencing Guidelines for Organizations*. Volgens deze richtlijnen geldt een adequaat integriteitprogramma ('compliance program') als verzachtende omstandigheid wanneer een onderneming schade veroorzaakt. Deze wet geldt ook voor Nederlandse bedrijven met vestigingen in de Verenigde Staten. Naast het hebben van een eigen code, geldt als één van de zeven verzachtende omstandigheden dat de organisatie beschikt over adequate interne meldingsprocedures voor misstanden die medewerkers in hun werkomgeving constateren. Een organisatie die aan de richtlijnen voldoet kan maximaal 95 procent vermindering van de boete krijgen.

Vertrouwen in zelfcorrectie?

Van belang voor een zelfcorrigerende organisatie is dat er een veilige cultuur is waarin medewerkers kritiek kunnen ventileren en vermoedens van laakbaar gedrag aan de orde kunnen stellen zonder te vrezen voor repercussies. Kunnen directeuren en managers er echter genoegzaam van uitgaan dat als hun geen incidenten via de lijn ter ore komen, dit ook inderdaad betekent dat alle incidenten zijn of worden opgelost? Kunnen directeuren en ondernemers vertrouwen op het zelfregulerend vermogen van de onderdelen? En kunnen onderdelen vertrouwen op het zelfcorrigerend vermogen van de afdelingen en teams? Het antwoord is ontkennend, zolang de bovenstaande drempels niet zijn geslecht.

Als de onderlinge sociale correctie en het aan de orde stellen in de directe lijn geen volledige waarborg biedt, is het dan wenselijk om naast de lijn een vangnet te hebben waar medewerkers incidenten kunnen melden? Het volgende hoofdstuk behandelt de vangnetten die momenteel binnen en buiten organisaties bestaan.

Klokkenluiderswetgeving in VS en het Verenigd Koninkrijk

De Verenigde Staten kent sinds 1989 wetgeving voor klokkenluiders. De zogeheten *Whistleblowers Protection Act* voorkomt sancties tegen ambtenaren die illegale activiteiten of bepaalde verkwistende activiteiten aan het licht brengen. De wet garandeert de bescherming van de klokkenluiders. Er is een speciale raad opgezet (de *U.S. Office of Special Council*) die onderzoeken verricht naar vergeldingsacties tegen klokkenluiders. Ook biedt de Raad een veilig kanaal waarlangs huidige en voormalige ambtenaren en sollicitanten misstanden aan het licht brengen van:

- een overtreding van wet of regelgeving;
- een grove kwestie van mismanagement;
- een grove verkwisting van gelden;
- machtsmisbruik; of
- een aanzienlijk en specifiek gevaar voor de volksgezondheid of veiligheid.

Het Verenigd Koninkrijk heeft sinds 1998 wetgeving voor de bescherming van klokkenluiders (de *Public Interest Disclosure Act*). Klokkenluiders worden beschermd wanneer zij informatie openbaar maken die verband houdt met onder andere een strafbaar feit, een rechterlijke dwaling of aantasting van de gezondheid, veiligheid en milieu. De wet heeft ook betrekking op personen die niet voor de overheid werken. De wet geeft vrij gedetailleerd aan onder welke omstandigheden openbaarmaking is toegestaan.

27 Kaptein, M. (2001), De Integriteitsbarometer: resultaten van een onderzoek naar de integriteit van Nederlandse organisaties, *Bedrijfskunde*.

28 Er (even) vanuitgaande dat er geen interne mogelijkheden zijn om buiten de lijn incidenten te melden.

29 Kaptein, M. (2001), De Integriteitsbarometer: resultaten van een onderzoek naar de integriteit van Nederlandse organisaties, *Bedrijfskunde*.

Deel II

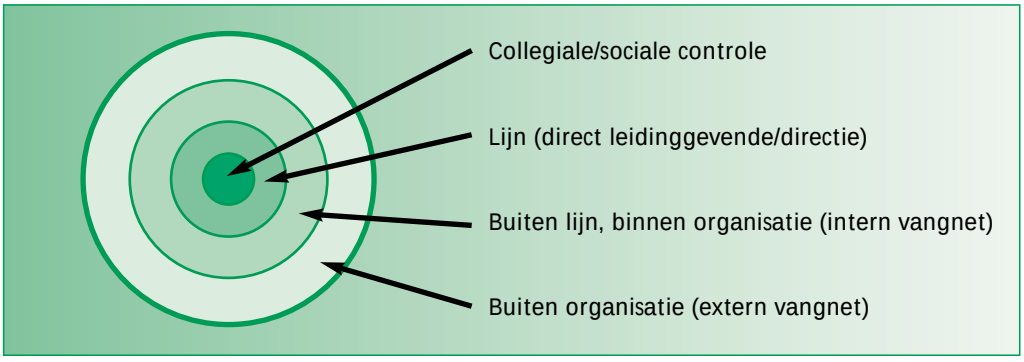
Gangbare vangnetten

3 Huidige vangnetten binnen en buiten organisaties

Voor het organiseren van integriteit is openheid van belang. Het elkaar kunnen aanspreken is noodzakelijk om gesignaleerde incidenten onderling te kunnen corrigeren. De praktijk wijst echter uit dat niet klakkeloos kan worden vertrouwd op het zelfcorrigerende vermogen van teams en afdelingen. Bovendien zijn medewerkers vervolgens ook terughoudend in het melden van incidenten aan het management en is het management ook niet altijd in staat adequaat op de melding te reageren. Schiet de openheid van organisaties tekort, dan lopen zij het risico dat een medewerker publiekelijk de klok luidt om zo aandacht voor het vraagstuk te krijgen. In bijna alle gevallen wijzen klokkenluiders op een tekortschietende interne organisatiecultuur. Het is dan ook van belang dat organisaties potentiële klokkenluiders niet monddood maken maar voldoende mogelijkheden bieden om hun bezwaren intern bespreekbaar te maken.

Het is derhalve wenselijk na te gaan op welke wijze organisaties een vangnet voor incidenten kunnen organiseren: een vangnet dat buiten de (hiërarchische) lijn valt, zodat medewerkers bij onvoldoende gehoor in de lijn niet direct op een instantie buiten de organisatie zijn aangewezen. In dit hoofdstuk gaat het om de vraag in hoeverre een intern vangnet bijdraagt aan de zelfcorrigerende werking van organisaties. Is het nuttig en noodzakelijk om een vangnet buiten de lijn in te richten? Of werkt dit juist ondermijnend op de lijn? Hoofdstuk 6 bespreekt enkele geïntegreerde modellen voor een intern vangnet.

VII. Vier routes voor melding van incidenten



Enkele voorbeelden van externe vangnetten voor medewerkers zijn:

- *Overkoepelende instanties*: sommige branches en beroepsgroepen (zoals de Vereniging voor Registerinformatici en de Registeraccountants) hebben een centraal meldpunt. Ook hebben de ministeries sinds januari 2001 een gezamenlijk meldpunt: de Commissie Integriteit Rijksoverheid.
- *Arbo-dienst (bedrijfsartsen, arbeids- en organisatiedeskundigen) en Arbeidsinspectie*: de Arbo-dienst adviseert over de preventie van onder andere ongewenste omgangsvormen en heeft in die zin ook een signalerende functie. Signaleringsmomenten zijn bijvoorbeeld de Risico Inventarisatie & Evaluatie en het Periodiek Arbeids Geneeskundig Onderzoek. Medewerkers kunnen zich met klachten over tekortschietende arbeidsomstandigheden wenden tot de Arbo-dienst. Zo heeft de Arbeidsinspectie in elke regio speciale vertrouwensinspecteurs aangesteld voor werknemers met klachten over ongewenste omgangsvormen. Deze inspecteurs kunnen slachtoffers eventueel verwijzen naar andere instanties voor de juiste hulp maar kunnen zelf geen daders aanspreken. Wel kan de Arbo-dienst de signalen melden aan het management tijdens het Sociaal Medisch Overleg.
- *Huisarts/Gak/psychologen/Algemeen Maatschappelijk Werk/RIAGG*: met name wanneer problemen binnen de organisatie tot fysieke of psychische klachten leiden kan een beroep op deze hulpverleners worden gedaan.
- *Vakbonden*: ook deze instanties staan open voor meldingen van hun leden. Zo heeft het CNV speciale vertrouwenspersonen voor eventuele vragen over keuringen en herkeuringen in verband met arbeidsongeschiktheid.
- *Accountants*: omdat accountants de financiële huishouding beoordelen en in dat kader ook gesprekken voeren met medewerkers en managers, kunnen financiële onregelmatigheden ook aan hen worden gemeld.
- *Milieu-inspectie*: medewerkers zouden milieudelicten kunnen melden aan de Milieu-inspectie die toeziet op de naleving en het bevorderen van de milieuregelgeving.
- *Belastingdienst en belastinginspectie*: medewerkers zouden ontduikingen van belastingverplichtingen die de organisatie begaat kenbaar kunnen maken bij de Belastingsdienst.
- *Politie/OM/CRI/Rijksrecherche* zijn instanties die kunnen worden benaderd inzake wetsovertredingen met vervolgmogelijkheden. De Binnenlandse Veiligheidsdienst heeft een speciaal meldpunt voor door bestuurders en ambtenaren begane (ernstige strafbare) overtredingen van (integriteit)regelingen.
- *Toezichthoudende organen*: ook deze instanties kunnen locaties zijn waar medewerkers incidenten melden. Daarbij valt te denken aan de Stichting Toezicht Effectenverkeer in het geval van bijvoorbeeld misbruik van voorwetenschap, de Algemene Rekenkamer voor de doelmatigheid van het overheidsbeleid en bijvoorbeeld de OPTA voor de telecomsector.
- *Certificerende instanties*: organisaties die keurmerken of certificaten toekennen

(bijvoorbeeld het ISO-certificaat en het SA-certificaat) kunnen gedurende hun onderzoek of als gevolg daarvan door medewerkers worden benaderd met incidenten op hun werkterrein.

- *NGO's* (non-gouvernementele organisaties) kunnen door medewerkers/managers worden benaderd wanneer de organisatie een bepaald belang schendt, zoals in het geval van milieuschade (Greenpeace), ondeugdelijke producten (Consumentenbond), corruptie (Transparancy International) en schending van de mensenrechten (Amnesty International).
- *Politici* (lokaal, provinciaal, nationaal): voor misstanden die tot maatschappelijke schade leiden.
- *Media*: met name overtredingen die een hoge media-attentie hebben.

Meldpunt Integriteitaantastingen Binnenlandse Veiligheidsdienst

'Bij het Meldpunt Integriteitsaantastingen kunnen incidenten met betrekking tot (veronderstelde) aantastingen van de integriteit van het openbaar bestuur ter kennis van de BVD worden gebracht. De BVD heeft een wettelijke verplichting tot geheimhouding van de identiteit van melders. De meldingen worden door de dienst beoordeeld op hun geloofwaardigheid, waarna wordt vastgesteld welke instantie in beginsel tot het instellen van een onderzoek bevoegd is. Tevens wordt vastgesteld of er sprake is van een melding die qua ernst BVD-onderzoek, zo nodig met inzet van bijzondere inlichtingenmiddelen, zou vorderen of rechtvaardigen. Het BVD-onderzoek naar (veronderstelde) aantastingen van de integriteit dient primair de doelstellingen waarheidsvinding/onzekerheidsreductie en het doen beëindigen van de integriteitsaantasting. Resultaten van onderzoeken kunnen tevens bijdragen aan verbetering van preventieve adviezen en aan mogelijkheden tot strafrechtelijk en/of disciplinair optreden.'

BVD Jaarverslag 1999

Zolang externe meldingsinstanties een verlengstuk zijn van de organisatie, geeft de organisatie de regie niet volledig uit handen. Dikwijls heeft de organisatie er echter geen zeggenschap over en is zij overgeleverd aan de aanpak van de betreffende instantie. Vooral als de instantie zelf weer een meldingsplicht heeft (politie, justitie, accountant) of leeft bij de gratie van publiciteit (media en in mindere mate NGO's), kunnen klokkenluiders de organisatie in diskrediet brengen of kostbare en tijdverslindende procedures veroorzaken. Om escalatie te voorkomen is het wenselijk een goed intern vangnet te hebben. Daarnaast is het mogelijk dat organisaties een eigen extern meldpunt inrichten (zie hoofdstuk 5). In alle gevallen is het wenselijk dat, waar mogelijk, de organisatie goede contacten onderhoudt met externe instanties waar medewerkers misstanden kunnen aankaarten. Naarmate de relatie beter is, wordt de kans op escalatie kleiner.

Commissie Integriteit Rijksoverheid

Per 1 januari 2001 is er een regeling voor rijksambtenaren die vermeende misstanden aan de kaak willen stellen, de zogenaamde klokkenluiders. In de regeling is beschreven dat vermeende misstanden binnen het eigen departement gemeld en afgedaan moeten worden. Het gaat hierbij om misstanden over bijvoorbeeld een ernstig strafbaar feit, het misleiden van justitie of het in gevaar brengen van de volksgezondheid. Wanneer de klokkenluider van mening is dat op zijn klacht niet adequaat intern wordt gereageerd, kan hij zich wenden tot een externe commissie. Deze Commissie Integriteit Rijksoverheid heeft tot taak een door een betrokkene gemeld vermoeden van een misstand te onderzoeken en daaromtrent het bevoegd gezag te adviseren. Hierbij zal indien gewenst het vertrouwelijke karakter van de informatie in acht worden genomen. Indien het gemeld vermoeden van een misstand ontvankelijk is, legt de Commissie zo spoedig mogelijk haar bevindingen neer in een advies, gericht aan het bevoegd gezag.

Intern vangnet

Binnen organisaties bestaat een veelheid aan instanties waar medewerkers buiten de lijn incidenten aan de orde kunnen stellen.

1. ‘Reguliere’ stafafdelingen

Als vanouds bieden stafafdelingen als Juridische Zaken, Personeelszaken en Audit mogelijkheden om vermeende misstanden te melden. Vanuit hun werkterrein zijn zij immers medeverantwoordelijk voor respectievelijk naleving van wet- en regelgeving, goed werkgeverschap en eerlijke verslaglegging. Ook recentelijker aangestelde staffunctionarissen, zoals op het gebied van milieu en IT, kunnen instanties zijn waarnaar medewerkers, al dan niet gestimuleerd, hun weg vinden voor respectievelijk milieuschade en misbruik van computers, software (downloaden van programmatuur waarop auteursrecht berust), internet en elektronische berichten (verzenden van aanstootgevende e-mail, virussen of pornografische afbeeldingen).

2. Beveiliging

De stafafdeling Beveiliging (security, veiligheidszaken) is in de jaren ’60 in opkomst gekomen. Een traditionele beveiligingstaak is het verzorgen van de fysieke beveiliging. Mede op basis van risicoanalyses wordt bepaald welke preventieve,

repressieve en opsporingsmaatregelen getroffen dienen te worden. Een veelvoorkomende taak van de afdeling Beveiliging is het onderzoek naar incidenten van inbraak, schade, criminaliteit, diefstal, corruptie en afpersing. In mindere mate behoren ook andersoortige incidentenonderzoeken, zoals verslaving, misbruik werktijden en machtsmisbruik tot haar takenpakket. Vanuit dien hoofde is de afdeling Beveiliging een loket waarbij medewerkers of managers incidenten kunnen melden.

De rol van beveiliging bij de Rabobank

De stafgroep Coördinatie Beveiliging (CoBRa) van de Rabobank Groep ziet er op toe dat medewerkers en externen zorgvuldig omgaan met materiële zaken die van de bank zijn of die de bank zijn toevertrouwd. Doelstelling van de stafgroep is het op economisch verantwoorde wijze beheersen van de risico's die de Rabobank-organisatie (Rabobank Nederland, aangesloten banken en meerderheidsdeelnemingen) bedreigen.

Ten aanzien van het begrip 'risico' is het onderscheid in commerciële en niet-commerciële risico's en risicofactoren relevant. De doelstelling van de stafgroep beperkt zich tot niet-commerciële risico's en risicofactoren.

Om de doelstelling te bereiken houdt de stafgroep zich bezig met:
- het voorbereiden, implementeren, bewaken en evalueren van een consistent risicomanagementbeleid;
- het formuleren en communiceren van procedures, normen en richtlijnen op basis van geaccepteerd risicomanagementbeleid;
- het beantwoorden van vragen over het beleid;
- het coördineren van alle beveiligingsactiviteiten binnen de organisatie;
- het coördineren en onderhouden van contacten met andere financiële instellingen en met de overheid;
- het oplossen van coördinatieproblemen met betrekking tot beveiligingsvraagstukken tussen de beveiligingseenheden onderling en met andere organisatieonderdelen;
- het maken van risicoanalyses, beveiligingsplannen en continuïteitsplannen en het geven van ondersteuning en adviezen op beveiligingsgebied;
- het centraal afsluiten van contracten met betrekking tot beveiliging;
- het fungeren als neutraal meldpunt voor het onder geheimhouding melden van ongebruikelijke transacties die men om welke reden dan ook niet volgens de gebruikelijke procedure kan of wil melden.

De stafgroep CoBRa heeft regelmatig overleg met de afdelingen Compliance, Juridische zaken en Audit om de afstemming ten aanzien van (meldingen van) incidenten te garanderen.

Het hoofd CoBRa heeft ook zitting in de Ethiek Commissie van Rabobank Nederland. Deze commissie geeft advies over ethische dilemma's en zorgt met name voor het bespreekbaar maken daarvan binnen de organisatie. Er wordt door de commissie niet beslist of een bepaalde actie wel of niet geoorloofd is; er wordt met name een algemene ethische lijn voor het hele bedrijf uitgestippeld. De stelregel blijft dat de beslissingbevoegdheid bij de lijn ligt; de staf kan desgewenst wel adviseren. De commissie ressorteert direct onder de Raad van Bestuur.

3. Bedrijfsmaatschappelijk werk e.a.

Bedrijfsmaatschappelijk werkers zijn met name betrokken bij problemen in de arbeidssituatie. Een bedrijfsarts is een daaraan flankerende professional die medewerkers met gezondheidsklachten en/of psychische klachten opvangt en helpt. Wanneer misstanden in de organisatie de oorzaak zijn van de klachten kunnen deze in de behandelingskamer ter sprake komen. De bedrijfsarts kan in het periodieke gesprek met het management de gedepersonaliseerde klachten en de organisatorische oorzaken daarvan aan de orde stellen.

4. Ondernemingsraad

Ook de Ondernemingsraad (OR) kan een kanaal zijn waarlangs medewerkers klachten van algemene aard ventileren. De drempel hierbij is laag omdat de leden van de OR vanuit de medewerkers zelf zijn gekozen. De OR is ook een orgaan dat onderwerpen als ongewenste omgangsvormen op de agenda van de organisatie kan zetten. Ook kan de OR zelf onderzoeken uitvoeren naar bijvoorbeeld ongewenste omgangsvormen.

5. Vertrouwenspersonen en klachtencommissie

Medio jaren tachtig is de 'Stichting Handen thuis' opgezet, een landelijk, door de Nederlandse overheid gesubsidieerd, expertisebureau voor ongewenste intimiteiten op het werk. Naar aanleiding van de aandacht die het onderwerp seksuele intimidatie ook in de jaren erna kreeg, formuleerde de Stichting van de Arbeid in 1990 aanbevelingen over seksuele intimidatie. In 1994 is in de Arbo-wet opgenomen dat werk-gevers verplicht zijn beleid te ontwikkelen ter bevordering van een veilige werk-omgeving en hun medewerkers zoveel mogelijk dienen te beschermen tegen seksuele intimidatie, agressie en geweld en de gevolgen ervan. De wijze waarop aan deze verplichting inhoud wordt gegeven, is voor organisaties volledig vrij. Veel

organisaties hebben als gevolg van de gewijzigde Arbo-wet een klachtenstructuur opgezet, doch deze is zelden (bij slechts 2% van de bedrijven[30]) vastgelegd in de CAO. Een klachtenstructuur bestaat over het algemeen uit één of meer vertrouwenspersonen, een klachtenregeling en een klachtencommissie. De klachtencommissie is een onafhankelijk orgaan dat onderzoekt of een klacht inzake ongewenste omgangsvormen ontvankelijk en gegrond is. Een vertrouwenspersoon kan onder andere zorgen voor de eerste opvang van de klager, het informeren en adviseren over de mogelijkheden voor verdere actie, het begeleiden in het oplossingstraject en het bieden van nazorg. In toenemende mate wordt de vertrouwenspersoon ook een bemiddelende rol toebedeeld. De vertrouwenspersoon tracht de klacht tussen het slachtoffer en dader onderling op te lossen zodat het niet tot een officiële klacht hoeft te komen. Naast de individuele vertrouwenspersonen kan er ook een centrale vertrouwenspersoon of -commissie bestaan. Hier kunnen individuele vertrouwenspersonen advies krijgen voor bij hen gemelde klachten. Ook managers kunnen bij deze centrale persoon of commissie terecht voor advies over de behandeling van concrete klachten. Een centrale vertrouwenscommissie is echter geen klachteninstantie en houdt zich dus niet bezig met individuele klachtenbehandeling. Medewerkers kunnen klachten dan ook niet ter beoordeling aan deze commissie voorleggen.

Klachtenrecht in CAO's

Op grond van sommige CAO's kan een medewerker een klacht indienen tegen een beslissing van zijn werkgever waardoor hij zich benadeeld voelt. De medewerker wendt zich, al dan niet met behulp van de vertrouwenspersoon, tot de directe manager met het verzoek om een maatregel te treffen (bijvoorbeeld een disciplinaire maatregel of een ordemaatregel ter voorkoming van herhaling). Als niet aan dit verzoek wordt voldaan, kan de betrokkene een klacht indienen bij de directeur die om advies vraagt aan de klachtencommissie. De klacht richt zich dus niet tegen de belager, maar tegen de werkgever die geen passende maatregelen neemt om het werkklimaat te verbeteren.

De vertrouwenspersonen bij ECT

Het Rotterdams havenbedrijf ECT heeft na een intensieve interne discussie in 1998 een bedrijfscode opgesteld en gedistribueerd onder alle 2200 medewerkers. Als gevolg daarvan rees de vraag tot wie medewerkers zich met vragen over de naleving van de code kunnen wenden. Sinds 1999 kent ECT drie vertrouwenspersonen en een klachtencommissie. Eveneens is er een deelcode ontwikkeld die beschrijft welke omgangsvormen als ongewenst kunnen worden beschouwd.
De vertrouwenspersonen zijn twee bedrijfsmaatschappelijk werkers en een mede-

werker van de afdeling Opleidingen. Het vertrouwenswerk vindt met name part-time plaats. Omdat het instituut bedrijfsmaatschappelijk werk al langer bestaat, hebben de betreffende personen een reputatie van vertrouwen opgebouwd bij het personeel. Het vertrouwenswerk en bedrijfsmaatschappelijk werk bijten elkaar in de praktijk af en toe. Bijvoorbeeld als blijkt dat iemand dreigt uit te vallen naar aanleiding van seksuele intimidatie. Indien dergelijke gevallen zich voordoen, zal de behandelend bedrijfsmaatschappelijk werker een collega vertrouwenspersoon vragen de zaak te behartigen. Eén van de vertrouwenspersonen fungeert als coördinator voor het vertrouwenswerk. De onderlinge afstemming tussen de vertrouwenspersonen gebeurt verder op een natuurlijke manier. Twee vertrouwenspersonen zijn vrouwelijk en één is mannelijk waarmee vergroting van de toegankelijkheid van de vertrouwenspersonen wordt beoogd. Het voordeel van meerdere vertrouwenspersonen is dat ingeval de objectiviteit en neutraliteit van een van de vertrouwenspersoon in het geding is, de andere vertrouwenspersoon de kwestie kan overnemen. Iedere vertrouwenspersoon is op een andere locatie gehuisvest. De vertrouwenspersonen staan ook open voor externen die zich op de terreinen van ECT bevinden. De vertrouwenspersonen staan open voor meldingen van in principe alle vormen van integriteitinbreuken. Afhankelijk van het type integriteitinbreuk wordt een procedure gevolgd die schriftelijk is vastgelegd. Naast de interne vertrouwenspersonen is het voor een verdachte ook mogelijk een externe partij in te schakelen.
Meldingen kunnen anoniem worden gedaan. Op het moment dat een melding uitloopt op een daadwerkelijke klacht, wordt de anonimiteit (van degene die de klacht indient én de verdachte) prijsgegeven. De klachtencommissie zal de klacht, die schriftelijk ingediend moet worden, daarna behandelen en de vertrouwenspersoon zal de klager bij dit traject blijven ondersteunen.

6. Compliance officers

De compliancefunctie (handhaving) is in de jaren dertig in de Verenigde Staten ontstaan. Veelal wordt deze functie in directe relatie met gebruik van voorwetenschap en andere vormen van beursgerelateerde fraude gezien. Met de nieuwe effectenwetgeving (zoals de Regeling Melding en Reglementering Transacties 1999 en de Nadere Regeling) is de aanwezigheid van de compliance officer bij aan de beurs genoteerde ondernemingen en financiële instellingen verplicht. In deze wet staat de compliance officer genoemd als interne toezichthouder op de naleving van externe wetten. Voor de financiële sector betekent dat onder meer de bestrijding van witwassen. De compliance officer is bevoegd een onderzoek te (laten) verrichten naar effectentransacties van managers en medewerkers. De compliance officer kan daartoe alle informatie over effectentransacties vragen. Medewerkers die als insider zijn

aangewezen, melden iedere door hen verrichte effectentransactie aan de compliance officer. In sommige instellingen heeft de compliance officer de bevoegdheid medewerkers te verbieden om gedurende een bepaalde periode in met name genoemde effecten te handelen. Sommige functieomschrijvingen van compliance officers geven een bredere taakomschrijving: het houden van toezicht op de integriteit van de organisatie. In toenemende mate worden ook compliance officers aangesteld op andere specifieke thema's, zoals een privacy officer, een corruptie officer en een mensenrechten officer. In de brede omschrijving van de compliancefunctie vallen dus alle functionarissen binnen een organisatie die belast zijn met het toezicht houden op de integriteit in algemene zin of een deelterrein ervan.

De compliance-functie bij de Fortis Bank Nederland

Fortis Bank Nederland heeft een uitgebreide compliancestructuur. Zij heeft een centraal compliance-bureau, waar twee officers werkzaam zijn. Deze compliance officers houden zich in de praktijk bezig met de implementatie van en toezicht op de interne en externe regelgeving en de ondersteuning van de decentrale compliance officers binnen de diverse business lines. Om het werk van het compliancebureau te faciliteren, is er een compliance-handboek, waarin de gedragscode en het compliancehandvest van de bank zijn opgenomen, evenals de diverse compliance-regelingen.
De eindverantwoordelijke compliance officer rapporteert periodiek aan de voorzitter van de Raad van Bestuur. Daarnaast is het compliancebureau ook verplicht om één keer per kwartaal aan de Stichting Toezicht Effectenverkeer (de STE) te rapporteren over het aantal compliance-incidenten en de aard daarvan.
Naast dit compliancebureau beschikt Fortis Bank Nederland over een aparte afdeling Veiligheidszaken, en over een Arbo-dienst met onder andere een aantal bedrijfsmaatschappelijk werkers. De afdeling Veiligheidszaken houdt zich bezig met interne en externe fraude, informatiebeveiliging en fysieke beveiliging.

VIII. Gangbare specifieke interne vangnetten

Instantie	Gangbaar werkterrein	Typische taken	Wettelijk kader	Toepassing
Beveiliging	Inbraak, diefstal, vandalisme, schade aan middelen, corruptie, afpersing, reputatierisico's	• Onderzoek naar misstanden • Rapporteren over de aard, omvang van de schade en de dader(s) • Adviseren over de maatregelen		
Bedrijfsmaatschappelijk werk/ Bedrijfsartsen/ Bedrijfspsychologen	Psychische en lichamelijke klachten	• Consultatie • Doorverwijzing • Medicatie		
Ondernemingsraad	Werknemersbelangen	• Behartiging van belangen	De *Wet op ondernemingsraden*: verplicht tot het instellen van personeelsvertegenwoordiging bij 50 werknemers of meer.	In 84% van de vestigingen met tenminste 50 werknemers is een OR ingesteld.[31]
Vertrouwenspersonen	Discriminatie, seksuele intimidatie, pesten, agressie en geweld	• Opvang van slachtoffers • Informeren en adviseren over de mogelijkheden van vervolgstappen • Begeleiden in oplossingstraject (bijvoorbeeld bij indienen van schriftelijke klacht en tijdens klachtenprocedure) • Informele bemiddeling • Bieden van nazorg	De Memorie van Toelichting op de *Arbo-wet* beveelt een vertrouwenspersoon voor ongewenste omgangsvormen aan.	34% van de bedrijven had in 1999 een vertrouwenspersoon (was 24 in 1995).[32] 54% van de Nederlandse beroepsbevolking heeft op het werk toegang tot een vertrouwenspersoon.[33] 52% had in 1999 een meldpunt voor seksuele intimidatie (was 33% in 1995).[34]

VIII. Gangbare specifieke interne vangnetten (vervolg)

Instantie	Gangbaar werkterrein	Typische taken	Wettelijk kader	Toepassing
Klachten-commissie	Ongewenste omgangsvormen en conflicten tussen werkgever en werknemer	• Onderzoeken van klachten • Adviseren over aanneembaarheid van klachten • Adviseren over maatregelen	De Memorie van Toelichting op de *Arbo-wet* beveelt een klachten-commissie aan.	17% van de bedrijven heeft een klachtenregeling in 1999 (was 7% in 1995).[35] In 2000 had 23% van de bedrijven met klachtenregeling een klachten-commissie.[36]
Compliance officers	Voorwetenschap, reputatierisico's, bestrijding van fraude en corruptie	• Signaleren en rapporteren • Dwingende regels opleggen • Identificeren van medewerkers die over (koers)gevoelige informatie beschikken • Nemen van beslissingen ten aanzien van de interpretatie van geldende regels • Het geven van aanwijzingen inzake de toepassing en interpretatie van regels • Adviseren inzake toepassing van sancties ingeval van overtreding • Onderzoek (laten) instellen tot bijvoorbeeld effecten-transacties	De *Regeling melding en regeling transacties in effecten 1999* en de *Nadere regeling 1999* voor effecten-instellingen en effectenkredietinstellingen verplicht. Voor beursondernemingen facultatief.	Financiële instellingen beschikken over een compliance officer. De compliance functie binnen beursgenoteerde ondernemingen is in opkomst.

Functies van het interne vangnet

Kenmerkend voor bovenstaande functies is dat zij min of meer een onafhankelijke positie hebben. Zij zijn niet verplicht om het lijnmanagement voor iedere stap toestemming te vragen en inzage te geven in wat zij hebben gehoord. Omdat het vangnet buiten de lijn is geplaatst, beschikken zij over het algemeen niet over bevoegdheden tot het nemen van sancties, maar adviseren zij de lijn over te treffen sancties.

Taken van een intern vangnet zijn:

1 *vragen beantwoorden* of informatie verstrekken over bijvoorbeeld hoe om te gaan met dilemma's en management;
2 *ondersteunen* van de melder, klager, slachtoffer (in termen van eerste opvang, coaching, luisterend oor en hulp);
3 *doorverwijzen* naar andere instanties;
4 *bemiddelen* in geval van overbrugbare conflicten tussen dader en slachtoffer of werknemer en werkgever;
5 *toestemmen/instemmen* met verzochte handeling;
6 *onderzoeken* van vermeende incidenten (reactief) of handelingen die risicovol zijn (pro-actief);
7 *verdedigen* en bijstaan in geval van conflict;
8 *adviseren* over te treffen sancties en arbeidsrechtelijke maatregelen;
9 *registeren en analyseren* van klachten, incidenten, meldingen, oorzaken en gevolgen;
10 *signaleren* van knelpunten en adviseren over te ontwikkelen beleid aan het management, gevraagd dan wel ongevraagd;
11 *stimuleren* van het bewustzijn van management en medewerkers omtrent integer gedrag;
12 *nazorg verlenen* aan degenen die betrokken zijn geweest bij een incident;
13 *bewaken* van realisatie van gedane toezeggingen en gemaakte afspraken (bijvoorbeeld ten aanzien van de afwikkeling van een klacht).

Rollen binnen vangnet bij Ministerie van SZW

Het Ministerie van Sociale Zaken en Werkgelegenheid houdt zich onder meer bezig met voorbereiding en bewaking van wetgeving en regels op het gebied van arbeid, arbeidsaspecten en arbeidsomstandigheden. Het ministerie heeft onlangs een onderzoek laten uitvoeren naar het functioneren van vertrouwenspersonen en klachtencommissies seksuele intimidatie binnen organisaties.
Het ministerie beschikt voor het eigen personeel over:

1 bedrijfsmaatschappelijk werkers (wanneer uitval van personeel dreigt);
2 een interne ombudsman (voor klachten over arbeidsomstandigheden, de inhoud van het werk of de manier waarop men door de chef en/of collega's is behandeld);
3 vertrouwenspersonen seksuele intimidatie. (De taken zijn met name de melder, klager of slachtoffer te ondersteunen en door te verwijzen naar andere instanties);
4 een klachtencommissie seksuele intimidatie;
5 een integriteitfunctionaris (voor zaken als fraude);
6 een extern beveiligingsbedrijf.

Er zijn drie vertrouwenspersonen seksuele intimidatie aangesteld. In de praktijk blijken er weinig meldingen van ongewenst gedrag bij de vertrouwenspersonen binnen te komen. Hieruit mag niet de conclusie worden getrokken dat ongewenste bejegeningen niet voorkomen in de SZW-organisatie. Daarom is naar aanleiding van het geringe aantal meldingen een onderzoek uitgevoerd naar de risicofactoren inzake ongewenste intimiteiten en ongewenste omgangsvormen van de SZW-kerndepartementorganisatie en haar fysieke omgeving. Deze zogenaamde scan is in het 4e kwartaal 1999 uitgevoerd.
De resultaten van dit onderzoek geven geen aanleiding tot ingrijpende maatregelen. In vervolg erop worden wel de nodige vragen opgenomen in het belevingsonderzoek dat in 2001 wordt gehouden in het kader van de RI&E (Risico-inventarisatie en evaluatie). Wellicht zal dan blijken dat één van de oorzaken van het geringe aantal meldingen de te hoge drempels zijn. Hoge drempels zijn het gevolg van weinig communicatie. Seksuele intimidatie blijft toch voor velen een moeilijk bespreekbaar onderwerp. En vanwege het kleine aantal meldingen is men al snel geneigd communicatie als onnodig te beschouwen. Daarmee is de cirkel rond.

30 Ministerie Sociale Zaken en Werkgelegenheid (2000), *Regelingen inzake een individueel klachtenrecht van werknemers in bedrijven*.
31 Bruin, E. & Huijgen, F. (2000), *Naleving van de Wet op de Ondernemingsraden: Stand van zaken begin 2000*, Ministerie van Sociale Zaken en Werkgelegenheid, Den Haag: Elsevier Bedrijfsinformatie.
32 Zie noot 31.
33 M. Kaptein, presentatie tijdens het congres 'De Aanpak van ongewenste omgangsvormen op het werk', georganiseerd door het Studiecentrum voor Bedrijf en Overheid op 7 februari 2001. Het cijfer is gebaseerd op een onderzoek onder de Nederlandse beroepsbevolking in 2000.
34 Zie noot 31.
35 Zie noot 31.
36 Zie noot 31.

4 Effectiviteit van huidige vangnetten binnen organisaties

Een vangnet functioneert onder andere als een ventiel. Het voorkomt overdruk doordat medewerkers met hun problemen altijd intern ergens terechtkunnen. Dit voorkomt weer dat de kans dat informatie op straat geraakt, afneemt. Voor het goed organiseren van een vangnet voor incidenten, klachten en dilemma's is het van belang te weten welke voor- en nadelen momenteel in de praktijk worden ondervonden. Recentelijk zijn daarom diverse onderzoeken verricht naar het functioneren van het vangnet voor klachten en incidenten binnen Nederlandse organisaties. Met name het functioneren van vertrouwenspersonen ten aanzien van omgangsvormen is belicht.

IX. Onderzoeken naar functioneren intern vangnet

Door	Jaar	Naar	Resultaten
ABVAKABO	1999	Loyaliteitsproblemen bij ambtenaren	Een derde van de ambtenaren heeft wel eens een loyaliteitsdilemma (misstand binnen de eigen organisatie houden of in de publiciteit brengen).
Ministerie van Sociale Zaken en Werkgelegenheid	2000	Knelpunten omtrent praktijk en beleid Arbowet	Het merendeel van de slachtoffers van ongewenste omgangsvormen meldt zijn ervaringen aan een persoon of instantie die actie kan ondernemen na een dergelijke melding. Desondanks verandert er niets op het werk of voor het slachtoffer persoonlijk.
Ministerie van Sociale Zaken en Werkgelegenheid	2000	Regelingen inzake een individueel klachtenrecht	Werknemers ervaren een hoge drempel om een klacht in te dienen bij een daarvoor ingestelde klachtencommissie. Werknemers ervaren een minder hoge drempel als de klacht wordt ingediend bij interne vertrouwenspersonen.

IX. Onderzoeken naar functioneren intern vangnet (vervolg)

Door	Jaar	Naar	Resultaten
NISSO	2000	Knelpunten die vertrouwenspersonen omgangsvormen binnen de politie ervaren	Eén op de tien medewerkers die last ondervinden van seksuele intimidatie maakt daarvan intern melding.
KPMG & Vrije Universiteit Amsterdam	2000	Effectiviteit vertrouwensstructuur	De effectiviteit van het vertrouwenswerk wordt met name bepaald door het belang dat het management hecht aan omgangsvormen.
Ernst & Young	2000	Complianceprocedures bij financiële instellingen	De positie van 'klokkenluider' is niet beschermd binnen het overgrote deel van de financiële instellingen in Nederland.

Knelpunten afzonderlijke instanties binnen vangnetten

In tabel X staan de belangrijkste knelpunten opgesomd die in de praktijk door de loketten zelf dan wel door werknemers en management geregeld tot vaak worden ervaren. Deze bevindingen zijn gebaseerd op onder andere een onderzoek onder de Nederlandse beroepsbevolking, een onderzoek onder leden van het vangnet, managers en medewerkers binnen organisaties en consultatie van experts.

X. Huidige specifieke knelpunten van afzonderlijke vangnetten

Instantie	Ervaren knelpunten binnen organisaties
Staf	• Geen vast aanspreekpunt ("De secretaresse van de stafafdeling helpt mij alleen als ik eerst de klacht aan haar vertel.") • Staat ver van werkvloer af. • Belang van de organisatie staat voorop, hetgeen de onafhankelijkheid aantast. • Ontbreken van procedures voor meldingen en bescherming van melder. ("Ze zien me daar al aankomen. Het eerste wat ze waarschijnlijk doen is mijn verzoek op de mail naar iedereen van de stafafdeling zetten met de vraag wie mij kan helpen.")

X. Huidige specifieke knelpunten van afzonderlijke vangnetten (vervolg)

Instantie	Ervaren knelpunten binnen organisaties
Vertrouwenspersonen	• Vanwege de incident- en slachtofferbenadering van de vertrouwenspersonen worden de oorzaken niet aan de orde gesteld. • Meldingen bij vertrouwenspersonen worden niet teruggekoppeld aan de betreffende managers omdat de klager daarvoor geen toestemming geeft of de melding geen officiële klacht wordt. Zolang het management onwetend blijft, kan het ook geen acties ondernemen om het probleem in de toekomst te voorkomen. • Geen of weinig ervaring. ("In de twee jaar dat ik nu vertrouwenspersoon ben, heb ik nog geen vraag gekregen. Eigenlijk weet ik ook nog steeds niet of ik wel geschikt ben voor deze functie.") • Beperkt zich tot vraagstukken op het gebied van ongewenste omgangsvormen, of zelfs alleen seksuele intimidatie. ("Voor vragen op het gebied van bijvoorbeeld vriendjespolitiek ben ik niet thuis.") • Ontbreken centrale/coördinerende vertrouwenspersoon ("Als vertrouwenspersoon hang ik er maar een beetje bij. Soms heb ik het idee dat ik mijzelf tussen hemel en aarde bevind.") • Vanwege de regiefunctie van de klager wordt de klager in zijn rol van slachtoffer bevestigd. Dikwijls zal de klager een eigen inbreng hebben gehad in de ontstane situatie. Er vindt zogenaamde verslachtoffering van de klager plaats. De klager wordt lijder in plaats van leider.[37] Van de vertrouwenspersoon wordt in zekere zin alleen maar verwacht dat deze opkomt voor de belangen van de klager. Er vindt verharding van het probleem plaats. • Bij afwikkeling van incidenten ligt de nadruk op het juridisch proces in plaats van op de inhoud van het probleem.
Ondernemingsraad	• Vanwege het vele contact met het management ontstaat de angst dat er onder één hoedje wordt gespeeld. • Het in vertrouwen melden aan één lid van de Ondernemingsraad kan ertoe leiden dat de zaak in de gehele raad wordt besproken waardoor de kans op anonimiteit afneemt. ("Wie verzekert mij dat mijn naam toch niet na verloop van tijd door de organisatie gaat zingen?") • Een melding over een incident kan snel ontaarden terwijl, in het geval van bijvoorbeeld miscommunicatie tussen twee personen, de gevoelens gemakkelijk te sussen zouden zijn geweest.
Beveiliging	• Management heeft geen grip op werkzaamheden van Beveiliging (bijvoorbeeld wanneer en naar wie onderzoek wordt verricht). • Management houdt zich afzijdig. ("Mijn management wil zijn handen niet vuil maken. Geen bericht is voor hen goed bericht. Wat niet weet wat niet deert.") • Wordt als de politie van de organisatie gezien en daarmee een zwaar middel om soms kleine misstanden op te lossen. ("Als iemand van Beveiliging bij ons de gang opkomt, sluit iedereen zijn deur.")
Compliance officer	• Staat aan de kant van de directie. • Weinig vertrouwen van personeel omdat compliancefunctie primair gericht is op correctie. ("Telkens als ik intern iets over mijn werkzaamheden vertel, krijg ik achterdochtige vragen.") • Beperkt tot interne naleving van externe wetten: sterke juridische insteek.

Naast bovenstaande knelpunten worden ook knelpunten genoemd die voor meerdere loketten tegelijk gelden, zoals:

- onvoldoende *bevoegdheden* en draagvlak van het management. (“Hoe harder ik roep, des te dover het management wordt”);
- *selectieve toepassing* van het werkterrein (“Ik word geacht alleen tegen medewerkers in actie te komen. Het management acht mij naar hen toe overbodig.”);
- onvoldoende *draagvlak* bij personeel. (“Ik word gewoon uitgelachen of iedereen sluit zijn deur als ik langs wil komen.”);
- onvoldoende *middelen* (tijd, budget en gespreksruimte) (“Ik ben al blij als ik het eerste telefoongesprek adequaat kan afhandelen.” En: “We hebben nog niet eens een budget voor een dossierkast.”);
- reguliere *omgang* met collega’s verandert zodat voeling met de praktijk afneemt. (“Sinds ik deze functie heb, passen collega’s toch op wat zij in mijn nabijheid zeggen.”);
- onvoldoende *opleiding* of voorbereiding. (“Van de één op de andere dag moest ik maar even de vertrouwenspersoon spelen.”);
- geïsoleerde *positie* binnen de organisatie. (“We zitten niet alleen letterlijk maar ook figuurlijk in de uithoek van de organisatie.”);
- *onduidelijke normen*. Een onduidelijke gedragscode bemoeilijkt niet alleen het onderling aanspreken en het melden, maar ook het vervolgens door het vangnet aankaarten van het gedrag bij de overtreder;
- zware *emotionele belasting* die onvoldoende door de organisatie wordt erkend. (“Helaas is er voor de vertrouwenspersoon geen vertrouwenspersoon. Ik ben mijn eigen vertrouwenspersoon.”);
- *buitenproportionele activiteiten*. Wanneer na lange tijd eindelijk een melding binnenkomt, overreageert het loket door zich helemaal op de melding te storten en het probleem van het slachtoffer over te nemen of de overtreding tot op het bot uit te zoeken om zichzelf te bewijzen;
- *onbereikbaarheid* van de loketten. (“Toen ik de compliance officer belde met het verzoek teruggebeld te worden, kreeg ik een week later zijn secretaresse aan de lijn met de mededeling dat hij geen kans meer had gezien mij te bellen en dat hij nu drie weken op vakantie was.”);
- onduidelijkheid over de *taken* van de verschillende loketten bij werknemers;
- *onbekendheid* met personen die de loketten bemensen. (“Zolang ik me er geen gezicht bij kan voorstellen, ga ik ook mijn hebben en houwen niet aan zo iemand toevertrouwen.”);
- *onveranderbaarheid*. Meldingen leiden niet tot veranderingen van de organisatie. (“Ik moet nog zien dat de eerste gegronde klacht ook echt leidt tot aanpassing van het beleid.”);
- *afschuiving* van verantwoordelijkheden. Leidinggevenden schuiven lastige gevallen ten onrechte af op het vangnet.

De *Ethics Officer Association* in de VS

Sinds 1992 bestaat er in Amerika een vereniging voor ethiekfunctionarissen. Ethiekfunctionarissen zijn personen die binnen hun organisatie verantwoordelijk zijn voor het opzetten, implementeren en/of controleren van de ethiek van de organisatie. De vereniging telt momenteel ongeveer 720 leden, afkomstig uit zowel profit- als non-profit-organisaties. Het doel van de vereniging is ethisch gedrag te bevorderen door middel van het uitwisselen van informatie. De vereniging organiseert frequent allerlei educatieve programma's.

In 1997 heeft deze vereniging onder haar leden een enquête uitgezet over de inbedding van *ethics officers* binnen organisaties. Enkele bevindingen zijn:

- 61% van leden is fulltime *ethics officer* en 39% parttime. Bij de grote organisaties werkt 87% van de *ethics officers* fulltime. Van de parttime officers besteedt 36% meer dan de helft van hun tijd aan ethische zaken.
- De *ethics officers* vallen onder de volgende afdeling: 23% Personeelszaken; 23% Administratie; 19% Juridische Zaken; 12% Interne Audit en 11% Financiën/ Accounting. Bij kleine organisaties heeft 37% een personeelsachtergrond.
- Over het algemeen waren de *ethics officers* al 16,3 jaar in dienst bij hun huidige werkgever. De functie van ethics officer bestaat gemiddeld al 5,3 jaar.
- Van de *ethics officers* rapporteert direct aan de top.
- Gemiddeld gezien hebben de ethics officers 960 meldingen over het voorgaande jaar gehad. De parttime officers kregen gemiddeld 96 meldingen en de fulltime officers 1486. De meldingen betroffen met name:
  - Belangenverstrengeling 62%
  - Cadeaus 53%
  - Misbruik van middelen 47%
  - Fraude met tijdschrijven 31%
  - Privé-werkzaamheden tijdens het werk 28%
- De omvang van de ethiekafdeling is gemiddeld 8 personen, hetgeen met name wordt bepaald door de grootte van de organisatie.
- Van de *ethics officer*s heeft 69% regelmatig contact met de juridische afdeling, 64% met Personeelszaken, 57% met Audit, 32% met de Security en 30% met de Financiële afdeling.
- Gemiddeld 64% van de leden heeft naast een *ethics officer* een ethische commissie.
- De *ethics officers* zijn verantwoordelijk voor de volgende taken:
  - Toezien op hotline/gedragscode/interne rapportage 85%
  - Voorbereiden en geven van interne presentaties 83%
  - Identificeren van knelpunten/zwakke punten 80%
  - Organisatiebrede communicatie 79%
  - Toezien op onderzoek naar overtredingen 77%

- Beoordelen van succes van initiatieven	75%
- Direct beheren van hotline/gedragscode/interne rapportage	75%
- Communicatie met (senior) management	73%
- Voorbereiden en geven van externe presentaties	72%
- Ontwikkeling van trainingsprogramma's	70%
- Geven van trainingen	58%
- Uitvoeren van onderzoek naar overtredingen	56%

Knelpunten gehele vangnet

Knelpunten van het gehele vangnet kunnen zijn:

- *Ondoorzichtigheid*. Er zijn vele interne instanties waar medewerkers incidenten kunnen melden waardoor zij door de bomen het bos niet meer te zien is. Het is niet duidelijk met welke vraag men zich tot welke instantie kan wenden.
- *Onvoldoende dekking* van vangnet voor incidenten. Slechts voor een beperkt aantal overtredingen beschikt de organisatie over een vangnet. Sommige meldingen raken vanwege deze witte vlekken tussen wal en schip.
- Ontoereikende *afstemming* tussen loketten. Soms weten bijvoorbeeld vertrouwenspersonen elkaar nog niet eens te vinden. ("Ik zou niet weten wie de andere vertrouwenspersonen binnen deze organisatie zijn.") De afdeling Beveiliging of Audit consulteert te weinig de vertrouwenspersoon indien bijvoorbeeld een fraudezaak ook aspecten van ongewenste omgangsvormen kent. In de praktijk blijkt juist dat geregeld fraudezaken worden gemeld omdat er sprake is van ontaarde omgangsvormen. Melding van fraude vindt plaats omdat bijvoorbeeld de melder geïntimideerd is door de fraudeur. In een groot Nederlands bedrijf bleek dat de vertrouwenspersonen relatief weinig werk hadden omdat de bedrijfsbeveiligers een groot deel van de eerste opvang en begeleiding van slachtoffers van ongewenste omgangsvormen naar zich toe trokken zonder dat de vertrouwenspersonen hiervan op de hoogte waren.
- Onvoldoende *aansturing*. De top heeft onvoldoende zicht op het gehele vangnet en stuurt ook als zodanig het vangnet niet aan. Zo zijn er nauwelijks organisaties waarbij er sprake is van een geïntegreerde rapportage over alle incidenten. Bewaking van het vangnet vindt niet plaats.

Weinig organisaties hebben een doordachte, samenhangende visie op hun vangnet. Het vangnet is te vaak en te veel versnipperd. Het volgende hoofdstuk bespreekt de overwegingen voor een goed vangnet en de beslissingen die daarbij dienen te worden genomen.

38 *Het Groot Arbowerk*, Alphen a/d Rijn: Samsom (o.a. van der Zwet, P.J. (2000), Vertrouwenswerk: het organisatiebelang voorop, B8030-1 t/m B8030-16).

Deel III

Handvatten voor een effectief geïntegreerd intern vangnet

5 Uitgangspunten en beslispunten voor een intern vangnet

In de vorige hoofdstukken is gebleken dat het noodzakelijk is dat voor een effectief vangnet doordacht moet worden welke kanalen daar voor open staan, welke rol iedere betrokkene heeft en hoe afstemming plaatsvindt tussen de betrokkenen. Deel III geeft een handreiking hoe het interne vangnet ingericht kan worden. De wijze waarop een vangnet wordt georganiseerd, hangt af van de uitgangspunten die de organisatie hanteert. Juist situaties waarbij uitgangspunten met elkaar conflicteren, zijn bepalend voor de vormgeving van het vangnet. Dit hoofdstuk bespreekt eerst negen uitgangspunten. Vervolgens worden uiteenlopende beslispunten besproken die bepalend zijn voor de vormgeving van het vangnet en waarbij telkens twee of meer uitgangspunten op gespannen voet met elkaar staan.

Uitgangspunten voor intern vangnet

Voor het goed organiseren van een vangnet is het zaak eerst na te gaan welke uitgangspunten de organisatie wenst te hanteren. Het gewicht dat de organisatie vervolgens aan ieder van deze uitgangspunten toekent, bepaalt vervolgens de wijze waarop een vangnet voor incidenten gestalte krijgt. In tabel XI staan negen uitgangspunten beschreven.

XI. Uitgangspunten voor vormgeving intern vangnet

1. Eigen verantwoordelijkheid van het slachtoffer of de getuige
2. Verantwoordelijkheden van de lijn
3. Verantwoordelijkheden van de staf
4. Duidelijke structuur om incidenten te melden
5. Lage drempels om incidenten te melden
6. Professionele aanpak
7. Efficiënte en daadkrachtige organisatie
8. Geloofwaardigheid en integriteit van vangnet
9. Organisatiebrede lering van incidenten

1. Eigen verantwoordelijkheid van het slachtoffer of de getuige

De wijze waarop het vangnet vorm krijgt, hangt af van het gewicht dat wordt toegekend aan de eigen verantwoordelijkheid van het slachtoffer of de getuige. Een vangnet dat volledig is geënt op de eigen verantwoordelijkheid van de medewerker, behelst dat de medewerker volledig de regie houdt en zelf op de genomen stappen aanspreekbaar is. Sommige deskundigen zijn van mening dat het slachtoffer de regie gedurende het gehele traject in eigen handen dient te houden. Zo is het aan de melder om te bepalen of hij zelf de melding op een officiële klacht uit wil laten lopen. In eerste instantie is het aan het slachtoffer of de getuige om de overtreder zelf aan te spreken en waar mogelijk het probleem op te lossen. Ook als de overtreder niet adequaat reageert, is het aan het slachtoffer of de getuige om zelf naar de lijnmanager te stappen om het probleem op die manier aan te kaarten. Ook als dat niet het gewenste effect heeft, is het aan het slachtoffer of de getuige om de misstand bij het hogere echelon aan te kaarten of buiten de lijn aandacht voor het probleem te vragen. Het slachtoffer neemt steeds zelf de eerste stap.

2. Verantwoordelijkheden van de lijn

Het is primair de taak van de direct leidinggevende om de incidenten die zich binnen zijn afdeling of onderdeel voordoen op een adequate manier op te lossen. Bij het instellen van een vangnet moet dan ook met name worden voorkomen dat de leidinggevende te snel of zelfs bij voorbaat meldingen doorverwijst naar het vangnet. Een vangnet heet niet voor niks een vangnet (voor de lijn). Sommige organisaties zien het instellen van een vertrouwenspersoon daarom als tijdelijke oplossing totdat de lijn zelf in staat is de problemen binnen de afdelingen adequaat op te lossen. Soms blijkt ook dat organisaties ervoor kiezen dat alleen de leidinggevende het vangnet mag consulteren.

3. Verantwoordelijkheden van de staf

Stafafdelingen zijn gecreëerd ter ondersteuning van het management (bijvoorbeeld in het geval van juridische zaken) en ter vergroting van de efficiency (bijvoorbeeld de salarisadministratie). Stafafdelingen beschikken over specifieke deskundigheid en beogen een uniforme werkwijze in de organisatie. Zo is Personeelszaken de aangewezen instantie voor omgangsvormen op de werkvloer, Juridische Zaken voor wetsovertredingen en Financiën voor fraude. Doordat stafafdelingen ook niet in een hiërarchische relatie tot de klagers staan, is de drempel om incidenten aan te kaarten lager. Daarnaast geldt dat hoe groter de verantwoordelijkheid van de staf, des te meer zelfstandig zij kan bepalen hoe met verzoeken van klager en management om te gaan. Ook dit kan de drempel tot melden verlagen.

4. Duidelijke structuur om incidenten te melden

Voor alle leden van de organisatie moet het duidelijk zijn bij wie welke meldingen kunnen worden gedaan en welke vervolgstappen tot de mogelijkheden behoren. Vragen waarop een integere organisatie antwoord dient te geven, zijn: “Voor welke incidenten kan ik me tot welke personen richten?”, “Tot wie kan ik mij wenden voor dilemma’s, vragen, kritiek en klachten?” en “Welke procedure geldt er voor de verschillende typen meldingen?”.

De vertrouwenspersoon bij Shell Nederland

Bij de introductie van de *Herziene Verklaring van Algemene Beleidsuitgangspunten* in 1997 heeft Shell een managementsysteem voor implementatie, handhaving en rapportage geïntroduceerd. Onderdeel hiervan is een jaarlijks verslag door de *Country Chairman* aan het *Committee of Managing Directors*. Dit heeft betrekking op de implementatie en handhaving van de Verklaring van Algemene Beleidsuitgangspunten, de zogeheten *Business Principles*. Deze *Business Principles Annual Letter* gaf aanleiding tot de aanstelling van een vertrouwenspersoon voor de Nederlandse Shell bedrijven in Nederland in 1999. Deze parttime vertrouwenspersoon is gehuisvest op het hoofdkantoor in Den Haag.
Bij voorkeur worden informatie en/of vermoedens van situaties, ontwikkelingen of voorvallen die in strijd (kunnen) zijn met de *Algemene Beleidsuitgangspunten* besproken met de lijn. Wanneer dit in bepaalde omstandigheden niet gepast of wenselijk is, kan contact worden opgenomen met de vertrouwenspersoon. Dit geldt voor alle medewerkers van Shell in Nederland. Dit houdt in dat bijvoorbeeld werknemers van de NAM en mensen van Shell Nederland Chemie in strikt vertrouwen bij de vertrouwenspersoon terechtkunnen. De functie van de vertrouwenspersoon is om de waarheid omtrent eventuele schendingen van de code boven tafel te krijgen. Vervolgens geeft de vertrouwenspersoon de melding door aan de hoogst verantwoordelijke lijnmanager zodat hij actie kan ondernemen. Indien nodig zal de vertrouwenspersoon de melding bespreken met de Shell-veiligheidsadviseurs, -juristen en/of -accountants. De vertrouwenspersoon informeert de *Country Chairman* ieder kwartaal en - indien nodig - ad hoc over alle meldingen en de genomen acties en maatregelen. De vertrouwenspersoon ziet het ook als zijn functie om de *Verklaring van Algemene Beleidsuitgangspunten* nogmaals onder de aandacht van alle medewerkers te brengen.

5. Lage drempels om incidenten te melden

Het moet medewerkers zo gemakkelijk mogelijk gemaakt worden om incidenten die zonder succes in de lijn zijn aangekaart, buiten de lijn aan de orde te stellen. Hoe hoger de drempel, des te meer incidenten tussen wal en schip raken, hoe groter de kans op escalatie van het incident en hoe groter de kans op extern klokkenluiden.

6. Professionele aanpak

In elke fase dient een melder op professionele wijze te worden geholpen: van het aanhoren van de melding, het interpreteren ervan, het bepalen van de vervolg-aanpak, het eventueel in gang zetten van onderzoek en het trekken van conclusies tot aan het zorgen voor een follow-up.

Klokkenluider bij een ministerie

"Een anonieme klokkenluider, in dienst van een ministerie, zond de secretaris van de Rekenkamer een brief waarin hij zijn zorg uitsprak over de gelijktijdige vervulling van twee naar zijn opvatting onverenigbare functies door een hoge ambtenaar bij dat ministerie. De secretaris legde de brief aan mij voor. Ik gaf aan dat deze functies naar mijn mening in beginsel inderdaad niet verenigbaar waren, maar dat het wel van belang was te weten of die ambtenaar eventueel zelf al maatregelen had genomen om feitelijke belangenverstrengeling te voorkomen. Het onderzoekbureau van de Rekenkamer bij het betreffende ministerie kon informatie verstrekken over deze compenserende maatregelen. Op basis daarvan kon de secretaris concluderen dat actie niet noodzakelijk was. Aldus werd recht gedaan aan de waarde van *betrouwbaarheid* (fair play), in dit geval in relatie tot de gecontroleerde."

Jaarverslag 1999 Vertrouwenspersoon Integriteit van de Algemene Rekenkamer

7. Efficiënte en daadkrachtige organisatie

In veel gevallen is het wenselijk snel actie te ondernemen om escalatie van het probleem te voorkomen en om sowieso duidelijk te maken dat het probleem serieus genomen wordt. Vanuit efficiency-overwegingen is het ook wenselijk dat het vangnet tegen zo laag mogelijke kosten wordt vormgegeven.

8. Geloofwaardigheid en integriteit van vangnet

Het oordelen over oorzaken en schuldigen dient op een onafhankelijke wijze, dus ongeacht de personen in kwestie en de context, plaats te vinden. Ongeacht de status van de persoon dient overal met dezelfde maat gemeten te worden. De melder dient er ook vertrouwen in te hebben dat er integer met zijn informatie wordt omgesprongen. Voor een vertrouwensstructuur is het dodelijk, de naam zegt het eigenlijk al, wanneer de medewerkers onvoldoende vertrouwen hebben in de integriteit van betrokken functionarissen en de wijze waarop er met in vertrouwen medegedeelde informatie wordt omgesprongen. Ook degene die beschuldigd wordt van laakbaar gedrag, dient er vertrouwen in te hebben dat er zorgvuldig met zijn belangen omgesprongen wordt.

9. Organisatiebrede lering van incidenten

Om te voorkomen dat soortgelijke incidenten zich op andere plekken in de organisatie wederom voordoen, is het zaak dat er organisatiebreed van incidenten geleerd wordt.

Beslispunten

Daar waar de bovenstaande uitgangspunten conflicteren, moeten keuzes worden gemaakt. Deze keuzes bepalen de uiteindelijke inrichting van het netwerk. Dertien belangrijke beslispunten worden hieronder beschreven.

XII. Beslispunten voor vormgeving vangnet

	Beslispunten	**Conflicterende uitgangspunten**
1	Het voorkomen van onnodige meldingen of het signaleren van alle relevante meldingen?	Efficiency versus effectiviteit
2	Een intern meldpunt en/of een extern meldpunt?	Lage drempels (blijft binnen de eigen organisatie) versus lage drempels (anonimiteit) en geloofwaardigheid (onafhankelijkheid)
3	Eén loket of een loket per vraagstuk?	Lage drempels (gemakkelijk bereikbaar) en duidelijke structuur versus efficiency en geloofwaardigheid (verstrengeling van rollen uitgesloten)
4	Centraal en/of decentraal?	Efficiency en professionaliteit versus lage drempels (meldpunt binnen eigen onderdeel kan vertrouwelijker zijn)

XII. Beslispunten voor vormgeving vangnet (vervolg)

	Beslispunten	Conflicterende uitgangspunten
5	Voor medewerkers en/of voor externen?	Efficiency en geloofwaardigheid versus effectiviteit en geloofwaardigheid
6	Fulltime of parttime?	Professionaliteit en lage drempels (geen mogelijke vermenging met andere taken) versus lage drempels (naar verhouding meer functionarissen) en efficiency
7	Eén voor allen of één op één?	Efficiency versus effectiviteit
8	Onderzoek door leidinggevende en/of door staf?	Eigen verantwoordelijkheid lijn versus professionaliteit en verantwoordelijkheid staf
9	Centrale en/of decentrale registratie?	Organisatiebreed leren versus eigen verantwoordelijkheid lijn
10	Centrale melding van incidenten of zelfreiniging van afdelingen?	Eigen verantwoordelijkheid lijn versus professionele aanpak
11	De functie van toezichthouder en vraagbaak scheiden of verenigen?	Geloofwaardigheid versus efficiency
12	Anoniem melden of identificeren?	Effectiviteit versus eigen verantwoordelijkheid medewerker
13	Klachtencommissie of niet?	Efficiency (flexibiliteit) versus geloofwaardigheid

1. Voorkomen onnodige meldingen of signaleren alle relevante meldingen?

Hoe hoger de drempel, des te minder meldingen er bij het meldpunt zullen binnenkomen en des te groter de kans dat ernstige incidenten niet bekend worden. Naarmate echter de drempel tot een meldpunt lager wordt, zal de kans toenemen dat het meldpunt ook voor onbenulligheden benaderd wordt (het zogenaamde stofzuigereffect; het zuigt alle problemen naar binnen, ongeacht de gegrondheid en ernst) en zuigt zo verantwoordelijkheden bij de lijn weg.

2. Intern meldpunt en/of extern meldpunt?

Met name voor kleine organisaties kan het wenselijk zijn om een meldpunt buiten de organisatie te hebben. Een dergelijk meldpunt kan worden georganiseerd door een aantal bedrijven op dezelfde locatie, in dezelfde regio of branche. Zo biedt KPMG Ethics & Integrity Consulting sinds 2000 ter ondersteuning aan organisaties een zogenaamd supportdesk aan. Dit kan voor organisaties niet alleen goedkoper

zijn, maar op deze manier kan de behandeling ook op een professionele wijze plaatsvinden en kan bereikbaarheid worden gegarandeerd. Juist in kleine organisaties is het moeilijk om de betrouwbaarheid van de melding te garanderen omdat iedereen elkaar kent ('ons-kent-ons'). Een extern meldpunt biedt meer kans op een onbevooroordeelde behandeling en op betrouwbaarheid en anonimiteit. Mogelijke nadelen van een extern meldpunt zijn dat er geen (interne) kennis van de organisatie en de cultuur aanwezig is, de vertrouwenspersoon relatief onbekend is en het moeilijk is voor de vertrouwenspersoon om het vertrouwen van de medewerkers te winnen.

3. Eén loket of een loket per vraagstuk?

Een belangrijk voordeel van één enkel loket is dat er voor de medewerkers duidelijkheid is over waar ze met hun melding heen kunnen. De bereikbaarheid en functies van een dergelijk loket zijn gemakkelijk te communiceren en door medewerkers eenvoudig te onthouden. Bovendien kan één loket kostenbesparend zijn doordat er geen dubbel werk wordt gedaan. Met behulp van één loket is ook gemakkelijker een centraal overzicht te verkrijgen van de gemelde incidenten. Nadeel van één enkel loket is dat de kans op een stofzuigerwerking toeneemt. Bovendien wordt er veel kennis en kunde verwacht van de medewerkers die het ene loket bemensen. Eveneens bestaat het gevaar dat naarmate het centrale loket door minder mensen wordt bezet, bepaalde informatie moeilijker te scheiden is. Bijvoorbeeld als er zowel een melding van incidenten binnenkomt als een verzoek van de betreffende verdachte om gesteund te worden bij zijn verdediging.

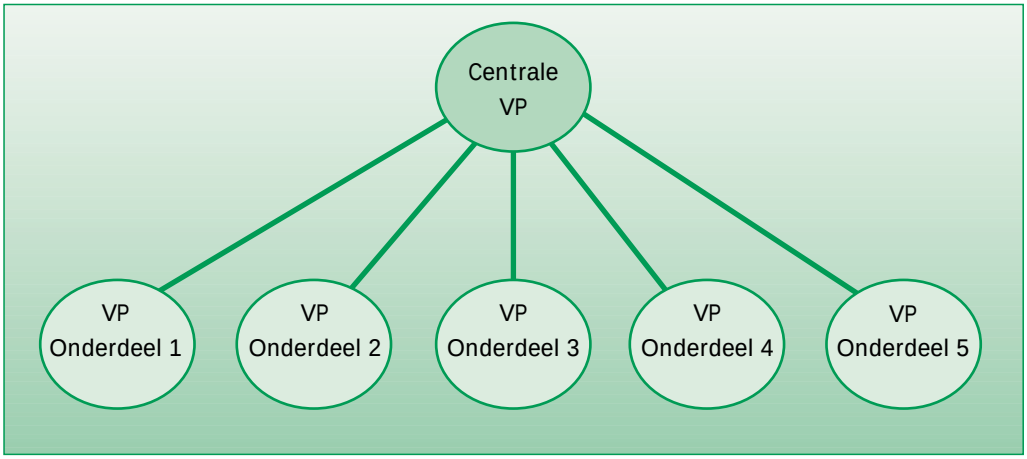
Soorten vertrouwenspersonen bij het Ministerie van Verkeer en Waterstaat

In 1996 heeft het Ministerie van Verkeer en Waterstaat een actiepakket ethiek samengesteld. Daarin wordt onder andere de eenheden verzocht een vertrouwenspersoon in te stellen. Er zijn momenteel twee typen vertrouwenspersonen per eenheid werkzaam: een vertrouwenspersoon voor economische incidenten en een vertrouwenspersoon voor sociale incidenten. Bij de grotere eenheden is de vertrouwenfunctie voor sociale incidenten ook nog opgesplitst in een vertrouwenspersoon voor seksuele intimidatie en een vertrouwenspersoon voor overig ongewenst gedrag. Eén van de eenheden beschikt zelfs over een heel team van vertrouwenspersonen, die ieder hun expertise hebben (bijvoorbeeld op het gebied van pesten, machtsmisbruik, ongewenst fysiek contact). De vertrouwenspersonen zijn geen verantwoording verschuldigd aan de directie van hun eenheid, maar direct aan de secretaris-generaal. Wel vindt regelmatig rapportage plaats aan de directie over de verrichte activiteiten.

4. Centraal of decentraal?

Een gedecentraliseerd vangnet (bijvoorbeeld per onderdeel) komt de herkenbaarheid bij medewerkers en de affiniteit met de situatie ten goede. Bovendien legt het daarmee de verantwoordelijkheid voor toezicht op het vangnet bij het management van het betreffende onderdeel. De onafhankelijkheid van bijvoorbeeld een centrale vertrouwenspersoon zal door medewerkers sneller in twijfel getrokken worden: “Hij/zij is niet één van ‘ons’, maar een handlanger van het management”. Hoe meer verschillende vertrouwenspersonen qua hiërarchisch niveau (en ook etnische achtergrond en sekse) des te meer recht wordt gedaan aan de diversiteit binnen het personeelsbestand en des te lager de drempel tot melden. Hoe hoger de meldingsfunctionaris geplaatst wordt, des te meer gewicht deze naar het management toe zal hebben. Door de decentrale plaatsing bestaat de kans dat de vertrouwenspersonen geen ervaring kunnen opdoen. Dit leidt ertoe dat wanneer zich een casus voordoet, de vertrouwenspersoon vanuit goedbedoelde betrokkenheid te ver gaat in zijn of haar hulpverlening en wellicht onbewust de rol van ‘redder’ opneemt. Bovendien leert de ervaring dat hoe meer vertrouwenspersonen er zijn, des te groter de kans dat deze in een geïsoleerde positie raken.

XIII. Mogelijke structuur voor vertrouwenspersonen (VP)



5. Voor medewerkers en/of externen?

Een andere vraag die bij het instellen van een vangnet naar boven komt, is de vraag of het meldpunt ook bereikbaar moet zijn voor externen. Sommige incidenten zullen eerder door externen worden opgemerkt (juist wanneer zij het slachtoffer zijn) dan door collega’s. Bovendien maakt de organisatie met de aanwezigheid van een meldpunt voor externen naar de omgeving duidelijk dat zij er alles aan doet om

laakbaar gedrag van de medewerkers te voorkomen en te bestrijden. Daarnaast kunnen meldingen van externen waardevolle adviezen voor de organisatie bevatten. Een mogelijk nadeel van het openstellen van een vangnet voor externen is dat bij externen de suggestie kan worden gewekt dat de organisatie onvoldoende in staat is zelf laakbaar gedrag te signaleren en te voorkomen. Bovendien zijn er hogere kosten verbonden aan een meldpunt voor externen (hogere bezetting, meer communicatie, hogere telefoonkosten bij een gratis nummer en ook meer telefoontjes van stalkers). Een ander nadeel is dat met het openstellen van een meldpunt voor externen, ook verwachtingen bij externen worden gewekt die, wanneer die niet kunnen worden gerealiseerd, het imago van de organisatie des te meer kunnen aantasten. Waar een organisatie juist al beschikt over bijvoorbeeld een ombudsman of een meldpunt voor consumenten, kunnen de ervaringen en faciliteiten goed worden benut om een intern meldpunt in te stellen.

General Electric over het melden van problemen

"Het is werknemers van GE in welke functie dan ook verboden om vergeldingsmaatregelen te nemen tegen iemand omdat hij een probleem heeft gemeld dan wel informatie heeft verschaft over een probleem met betrekking tot onze gedragsregels. Indien u denkt dat dit is gebeurd, meldt u dit dan aan een manager of bel de informatielijn van uw bedrijfsonderdeel of van General Electric Corporate ... of bel/schrijf de ombudsman/vrouw. De achterliggende gedachte is dat u uw mening moet kunnen uiten. Stel uw problemen aan de orde. Schuif ze niet terzijde."

General Electric *Onze Verklaring naar Letter en Geest*

6. Fulltime of parttime?

Bij de meeste organisaties blijkt dat het vertrouwenswerk uit kostenoverwegingen als een extra taak aan iemand binnen een bepaalde afdeling gegeven wordt. De parttime vertrouwenspersoon blijft op deze manier deel uitmaken van het bedrijf en blijft verbonden met de praktijk en de gang van zaken op de werkvloer. Eveneens is de drempel tot een parttimer lager omdat de persoon door het personeel als 'één van de onzen' wordt gezien. Mogelijke nadelen van een parttime vertrouwensfunctie zijn de verminderde bereikbaarheid en de geringere onafhankelijkheid. Een vakantie van de betreffende persoon betekent een even lange sluiting van het loket. De onafhankelijkheid van de vertrouwenspersoon komt vervolgens in het geding wanneer zijn andere taken conflicteren met de vertrouwenstaak. Bij een inkoopbedrijf was de secretaresse van de directeur de enige vertrouwenspersoon. Toen een klacht binnenkwam over de directeur belandde de secretaresse in een moeilijk parket. Sindsdien

is er een tweede vertrouwenspersoon aangesteld. Een ander risico van parttime werk is dat de werkzaamheden ten behoeve van het vangnet onvoldoende tijd krijgen wanneer andere taken veel aandacht opeisen. Een secretaris van de Raad van Bestuur die compliance officer voor aandelentransacties is, zal zich vanwege de veelheid aan functies moeilijker kunnen vrijmaken voor spoedeisende verzoeken dan een medewerker die geheel voor deze compliancefunctie is vrijgesteld.

7. Eén voor allen of één op één?

De capaciteit aan vertrouwenspersonen loopt per organisatie sterk uiteen. Het aantal vertrouwenspersonen (teruggerekend in het aantal *fulltime equivalents* (fte)) varieert van 1 op de 90 tot 1 op de 100.000 medewerkers. Ook het aantal instanties loopt per organisatie sterk uiteen. Veel organisaties hebben alleen een vertrouwenspersoon seksuele intimidatie. Er zijn ook organisaties waarin naast een vertrouwenspersoon omgangsvormen, een vertrouwenspersoon economische integriteit, een bedrijfsmaatschappelijk werker, een beveiligingsfunctionaris, een compliance officer voor voorkennis en één voor ICT zijn ingesteld. Hoe meer instanties en personen, des te fijnmaziger de structuur en in principe des te beter bereikbaar. Tegelijk neemt bij de toename van het aantal instanties, de kans op ontoereikende afstemming toe. Het ideale aantal vertrouwenspersonen is echter moeilijk te bepalen. Het aantal is immers mede afhankelijk van het aantal medewerkers, de geografische spreiding van de medewerkers, de verscheidenheid van interne culturen, de sociaal-culturele achtergrond van de personeelsleden, de aard van de werkrelatie (detachering of werkzaam bij de officiële werkgever) en de aard en omvang van de problemen.

De *Corporate Review Committee* bij Philips

Bij de invoering van de algemene gedragscode in 1998, heeft Philips een *Corporate Review Committee* ingesteld dat wereldwijd toezicht houdt op de naleving van de gedragscode. Om nog meer nadruk te leggen op het belang en de naleving van de code heeft elke landenorganisatie en elke divisie van Philips een compliance officer ingesteld. Overtredingen van de gedragscode dienen te worden gemeld aan de compliance officer. De *Review Committee* heeft een boek samengesteld met daarin allerlei cases over inbreuken op de gedragscode. Dit caseboek is via de HRM-managers binnen de Philips-organisatie verspreid. De gedragscode maakt in Nederland onderdeel uit van het arbeidscontract.

8. Onderzoek door leidinggevende en/of staf?

Of leidinggevenden zelf onderzoek naar incidenten mogen uitvoeren, bepaalt mede de inrichting van het vangnet. Een leidinggevende die zelf onderzoek verricht, maakt duidelijk dat hij zijn eigen verantwoordelijkheid serieus opneemt. Bovendien kan dit de snelheid van het onderzoek ten goede komen en voorkomt dit een mogelijke escalatie van het incident of conflict. Naarmate een manager meer complexe onderzoeken verricht, neemt de kans op een onprofessionele aanpak echter toe. Een leidinggevende op onderzoekspad onder zijn eigen mensen loopt daarnaast het risico de onderlinge relaties blijvend te beschadigen en daarmee het vertrouwen dat hij geniet aan te tasten. De staf die wel een professionele aanpak kan garanderen, loopt echter het risico onvoldoende affiniteit te hebben met de specifieke situatie van het voorval.

9. Centrale en/of decentrale registratie?

Door alle incidenten centraal te registeren wordt de kans op organisatiebreed leren vergroot. Zo kunnen trends eerder worden gesignaleerd en incidenten ook met elkaar in samenhang worden gebracht. Registratie kost echter tijd en geld. Daarnaast is het de vraag wat dan precies moet worden geregistreerd en hoe de vertrouwelijkheid kan blijven gewaarborgd. In het uiterste geval zou een leidinggevende ieder incident en iedere maatregel moeten registeren.

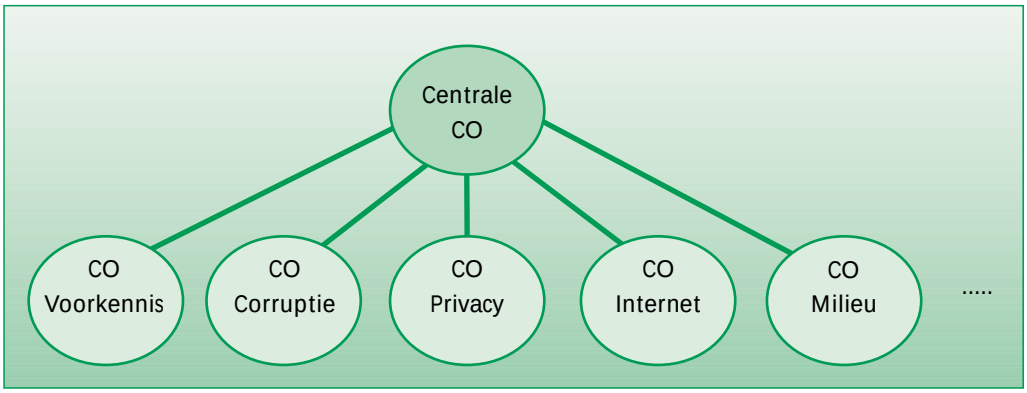
10. Centrale melding van incidenten of autonomie van afdelingen?

Hoe directer en dichter het incident bij de bron kan worden aangepakt, des te beter. Tegelijk zullen er uiteenlopende soorten overtredingen zijn, waarbij de directie niet zal toestaan dat dit één op één op de werkvloer wordt opgelost. Ernstige vormen van seksuele intimidatie, fraude, grove schendingen van interne richtlijnen en (aanzienlijke) overtredingen van de wet dienen daarnaast in de top bekend te zijn.

11. De functie van toezichthouder en vraagbaak scheiden of verenigen?

Sommige compliance officers fungeren zowel als vraagbaak en als toezichthouder. Enerzijds is dat wenselijk omdat vragen input kunnen zijn voor nieuw beleid. Anderzijds wordt van de vrager een kwetsbare opstelling gevergd. De vrager zal informatie moeten verstrekken over zijn probleem. Het is voor de compliance officer moeilijk om bij het verrichten van onderzoek, de informatie die hem als vraagbaak ter ore is gekomen, opzij te zetten. Met andere woorden, openheid kan ertoe leiden dat je eerder object van onderzoek wordt.

XIV. Mogelijke compliancestructuur



12. Anoniem melden of identificeren?

Het anoniem kunnen melden van incidenten verlaagt de drempels. De risico's op loze meldingen, telefoonterreur en medewerkers die met het telefoontje zich vervolgens van iedere verantwoordelijkheid ontdoen, nemen echter toe.

Gedragscodecommissie RET

"Als je alleen je verhaal kwijt wilt aan een vertrouwenspersoon gebeurt er verder niets. Niemand komt te weten wat jullie besproken hebben. Als je een officiële klacht indient, kan dat natuurlijk niet anoniem. Je moet je klacht schriftelijk indienen bij de gedragscodecommissie. Als je wilt, helpt de vertrouwenspersoon je daarbij. De gedragscodecommissie gaat je klacht onderzoeken. Ze kan jou en degene waarover je klaagt oproepen voor een gesprek. Vanzelfsprekend blijft alles vertrouwelijk. Binnen zes weken nadat je je klacht hebt ingediend brengt de gedragscodecommissie een advies uit aan de directeur over de klacht en de te nemen maatregelen. Op grond hiervan neemt hij binnen zes weken daarna een beslissing." *Gedragscode RET*

13. Klachtencommissie of niet?

Ongeveer een kwart van de bedrijven met een klachtenregeling heeft een klachtencommissie. De aanwezigheid van een klachtencommissie kan benadrukken dat de klachtenregeling/-procedure serieus wordt genomen. Bij de klachtencommissie komen in principe geen directe meldingen binnen en er worden door de klachtencommissie geen sancties getroffen. Een klachtencommissie bestaat over het algemeen uit een brede vertegenwoordiging van werknemers, wat mede de objectiviteit kan bevorderen. De aanwezigheid van een klachtencommissie kan er echter ook voor zorgen dat de effectiviteit en flexibiliteit van het proces afneemt.

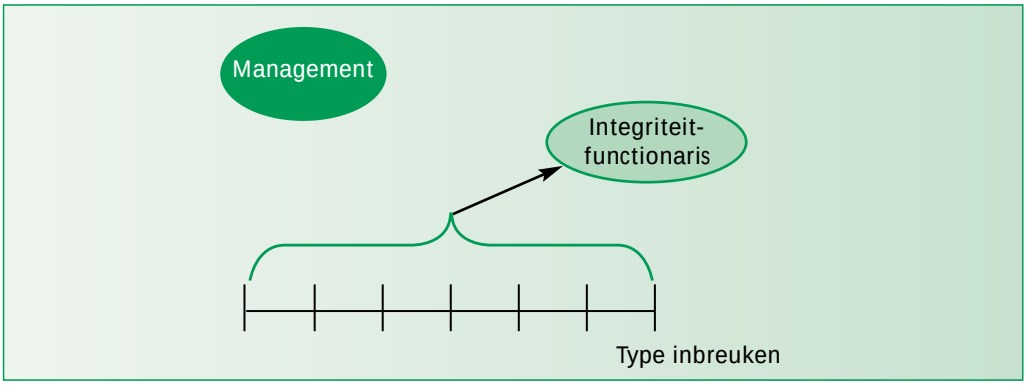
6 Drie modellen voor een geïntegreerd intern vangnet

In hoofdstuk 4 is gewezen op de risico's van een tekortschietende afstemming tussen de loketten van een intern vangnet. Een goed geïntegreerd intern vangnet zorgt ervoor dat medewerkers altijd met hun melding bij het vangnet terechtkunnen, dat er een goede follow-up is op de melding en dat het management erop toeziet dat het vangnet goed functioneert. Dit hoofdstuk schetst drie modellen voor een geïntegreerd vangnet.

Drie modellen

Er zijn grofweg drie modellen te onderscheiden voor een geïntegreerd intern vangnet.

XV. Model 1: Enkelvoudig vangnet met een integriteitfunctionaris



Bij een enkelvoudig vangnet is er voor alle type inbreuken één functionaris tot wie medewerkers zich kunnen wenden. Variaties op dit model zijn, afhankelijk van de keuzes ten aanzien van de beslispunten in hoofdstuk 5, centrale en decentrale functionarissen, intern of extern en bijvoorbeeld fulltime of parttime. Deze *integriteitpersoon* kan ook worden aangeduid met de term 'ethics-officer', 'vertrouwens-

persoon', 'vertrouwenspersoon integriteit' of 'compliance officer'. Het nadeel van de term 'compliance officer' is dat het takenpakket verder reikt dan louter het toezicht houden op de naleving van de gewenste integriteit. Mogelijk nadeel van de term 'vertrouwenspersoon integriteit' is dat medewerkers het onderscheid met de gangbare 'vertrouwenspersonen ongewenste omgangsvormen' die vooral opkomen voor de belangen van het slachtoffer, moeilijk kunnen begrijpen.

Met name in kleine organisaties verdient dit model al snel de voorkeur. Iemand buiten de lijn wordt tot integriteitpersoon aangesteld waarbij medewerkers zowel terechtkunnen voor sociale als voor financiële integriteitschendingen. De integriteitpersoon bepaalt (in overleg met de melder) vervolgens wat er met de melding wordt gedaan en wie eventueel daarbij betrokken zal worden.

De Vertrouwenspersoon Integriteit bij de Algemene Rekenkamer

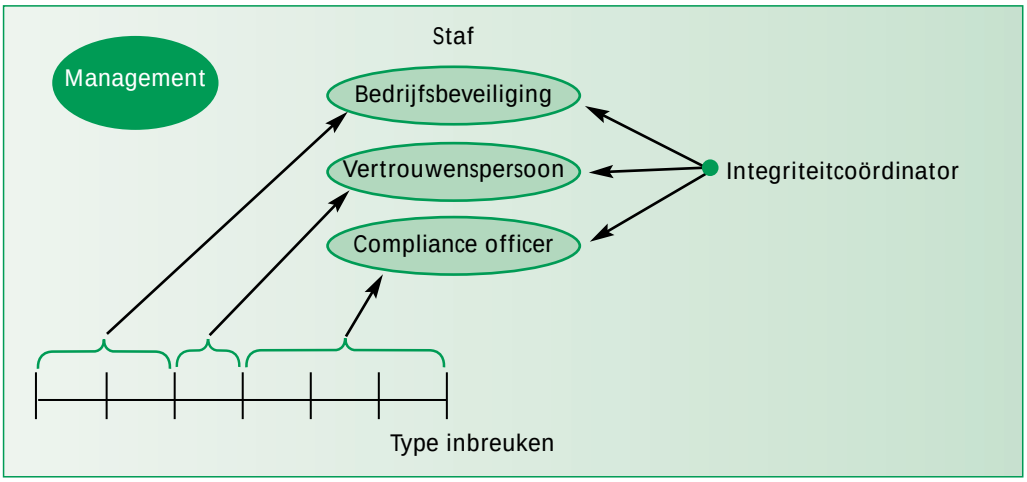
In het in 1996 verschenen rapport *Integriteitbeleid bij de overheid* geeft de Algemene Rekenkamer de ministeries het advies tot het aanstellen van een vertrouwenspersoon voor meldingen van (vermoede) aantasting van de integriteit. Een jaar daarvoor had de Algemene Rekenkamer in een interne nota al het voorstel gedaan voor het aanstellen van een vertrouwenspersoon integriteit binnen de Rekenkamer zelf.
De vertrouwenspersoon integriteit is via een formeel aanstellingsbesluit benoemd zodat daarmee het belang van de functie wordt onderstreept. De taken van de vertrouwenspersoon zijn:

- het geven van adviezen in meer algemene en in concrete situaties ter voorkoming van corruptie en machtsbederf;
- meldpunt voor gesignaleerde frauduleuze en/of corruptieve handelingen;
- het op grond van nader onderzoek beoordelen of een gemelde zaak aan het bevoegd gezag moet worden gerapporteerd;
- het verzorgen van een jaarverslag dat aan alle medewerkers ter beschikking wordt gesteld.

De vertrouwenspersoon integriteit is ook betrokken geweest bij het opstellen van de gedragscode.
In het aanstellingsbesluit van de vertrouwenspersoon integriteit is ook duidelijk omschreven dat de vertrouwenspersoon niet verplicht kan worden vertrouwelijke informatie vrij te geven en dat de vertrouwenspersoon een zelfde ontslagbescherming geniet als de leden van de Ondernemingsraad. De meldingen worden door de vertrouwenspersoon dan ook strikt vertrouwelijk behandeld. Een melding moet anoniem kunnen worden gedaan en ook anoniem kunnen blijven, zodat er geen repercussies volgen wanneer meldingen onterecht blijken te zijn. Om de

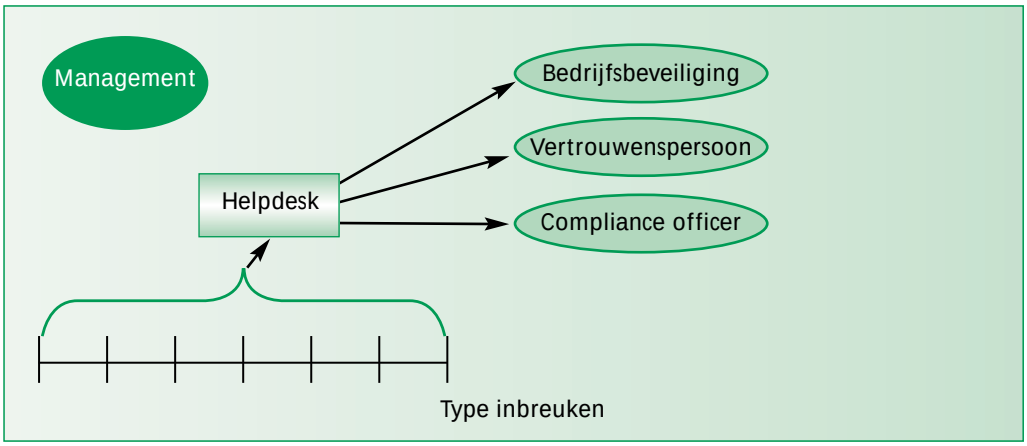
drempel zo laag mogelijk te houden, is er geen formele meldingsprocedure. In het jaarverslag van 1999 staat onder andere beschreven wat de taken van de vertrouwenspersoon zijn, wat de ervaringen met de taakvervulling zijn en een opsomming van diverse zaken die de vertrouwenspersoon ter behandeling heeft gehad. De vertrouwenspersoon wordt met name "ingeschakeld als *second opinion* over een bepaalde handelwijze. Over het algemeen bestond er bij de aanvragers van de adviezen al een vrij helder beeld omtrent de te maken keuze of te ondernemen actie, maar was er behoefte aan een klankbord om de gemaakt afwegingen aan voor te leggen."

XVI. Model 2: Meervoudig vangnet met een integriteitcoördinator



Bij een meervoudig vangnet zijn er verschillende loketten voor verschillende typen inbreuken. Wanneer de mogelijke vraagstukken van medewerkers duidelijk van elkaar te onderscheiden en te scheiden zijn, kunnen verschillende loketten goed naast elkaar bestaan. Goede communicatie over de reikwijdte van de verschillende loketten en afstemming tussen de loketten zijn daarbij belangrijk. De *integriteit-coördinator* heeft vervolgens de taak om (achter de schermen) erop toe te zien dat de verschillende instanties goed op elkaar zijn afgestemd.

XVII. Model 3: Geïntegreerd meervoudig vangnet met een helpdesk of meldpunt



Bij een geïntegreerd meervoudig vangnet is er één centraal loket voor alle typen inbreuken, waarachter alle relevante functionarissen zitten (al dan niet fysiek). Het *Meldpunt Integriteit* beslist op welke wijze de melding een vervolg krijgt. De term *Helpdesk Integriteit* nodigt medewerkers ook uit om zich met vragen en dilemma's hiertoe te wenden. Deze benaming benadrukt ook de eigen verantwoordelijkheid van werknemers op een positieve wijze (het helpaspect). Tegelijk erkent de organisatie ook haar eigen verantwoordelijkheid (bij de helpdesk ligt de taak om medewerkers naar de juiste instantie door te verwijzen). De medewerkers kunnen zich bijvoorbeeld ook direct tot de vertrouwenspersoon wenden, maar deze laatste dient de melding dan wel weer terug te koppelen naar de helpdesk.

De helpdesk zegt net als de integriteitfunctionaris toe voor iedere integriteitinbreuk open te staan. Het is de verantwoordelijkheid van de helpdesk om de melder verder te helpen. Als er voor een bepaald type melding geen loket is, dient de helpdesk te zoeken naar een goede opvolging van de melding en de melder niet aan zijn lot over te laten. Vooral bij grotere organisaties waar zich een veelheid aan inbreuken kan voordoen en er dikwijls een veelheid aan loketten is ontstaan, heeft de geïntegreerde meervoudige aanpak de voorkeur.

De werkwijze voor een Helpdesk Integriteit is als volgt:

1. *Intakefase*. De beller wordt een klankbord geboden waarbij een klacht, dilemma of vraag kan worden besproken. Aandachtspunten in de intakefase zijn onder andere een eerste inzicht te krijgen in de casus, het luisteren naar de gevoelens van de melder, het opbouwen van vertrouwen, en het uitleggen van de werkwijze en mogelijkheden van de Helpdesk Integriteit. De helpdesk medewerker is echter niet de persoon die vervolgens de vertrouwenstaken of compliancetaken uitvoert.

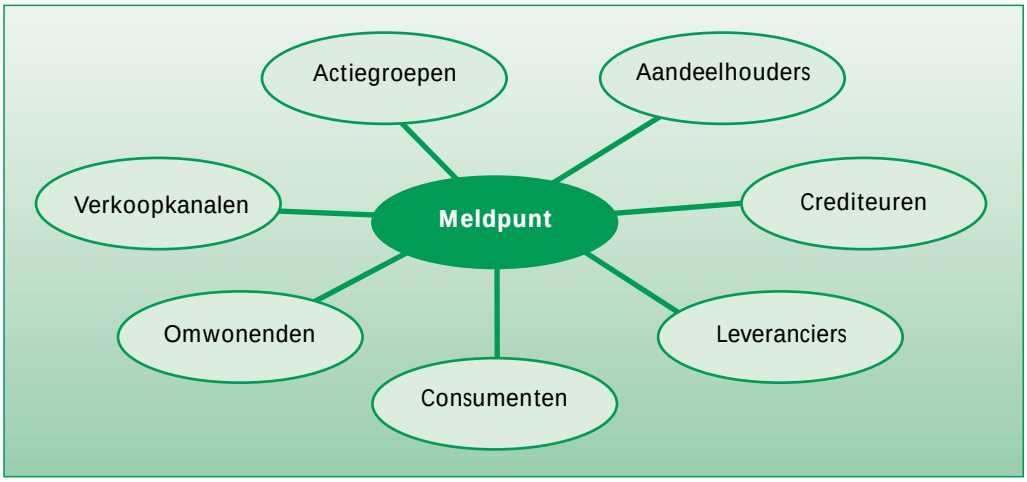
2. *Registratiefas*e. De helpdeskmedewerker registreert de melding in het daarvoor beschikbare systeem.
3. *Doorverwijsfase*. Vervolgens wordt het probleem in kaart gebracht, worden de mogelijkheden verkend en wordt de melder verwezen naar de meest geschikte functionaris binnen de organisatie. Hiertoe beschikt de helpdesk-medewerker over een 'code kaart' van de organisatie, die aangeeft welke functionaris het best voor welke meldingen kan worden geraadpleegd. De functionarissen zijn in principe altijd bereikbaar of bellen binnen vier uur terug.
4. *Bewakings-/follow-upfase*. De helpdeskmedewerker maakt in overleg met de melder afspraken over het vervolg van de begeleiding: onder andere door wie en wanneer er contact zal worden opgenomen met de melder. De helpdesk medewerker ziet erop toe dat de melder in contact komt met de desbetreffende functionaris. Eveneens houdt de helpdesk de voortgang van het proces in de gaten. De functionarissen zijn er zelf ook verantwoordelijk voor dat de direct aan hen gerichte verzoeken worden geregistreerd door de helpdesk. Periodiek rapporteert de helpdesk aan het management van de verschillende onderdelen en de directie. De compliance officers en vertrouwenspersonen krijgen de voor hen relevante geaggregeerde data ter beschikking.

De *ethics hotline* van Sara Lee/DE

In Amerika staat Business Ethics al veel langer op de agenda van de werkgever dan in Nederland. Sara Lee/DE is sinds 1977 gelieerd met het Amerikaanse bedrijf Sara Lee Corporation en besteedt daarom al lang aandacht aan ethiek en integriteit. Sara Lee/DE beschikt over *Global Business Standards* die voor de Nederlandse medewerkers zijn samengevat in 'De Gids voor Integer Werken'. Het bedrijf beschikt over een organisatie voor meldingen van integriteitinbreuken en vragen omtrent de interpretatie van haar regels. Deze organisatie wordt gevormd door de afdeling Personeel en Organisatie, de *Business Practices Officers* van de werkmaatschappijen/divisies en de *Business Practices Officer* van Sara Lee/DE op het niveau van de Raad van Bestuur. Als 'vangnet' is er een gratis telefoonlijn waar medewerkers terechtkunnen met meldingen. Door middel van deze telefoonlijn kan iedereen op elk moment (24 uur per dag) al dan niet anoniem melding maken van klachten.
Omdat de codes een wezenlijk onderdeel vormen van het functioneren van het bedrijf, is constante aandacht vereist. Juist omdat normen en waarden na verloop van tijd kunnen veranderen of anders kunnen worden geïnterpreteerd, vindt er een constante dialoog plaats tussen de *Business Practices Officers*. De *Business Practice Officers* ondernemen ook vele acties om medewerkers te wijzen op hun verantwoordelijkheden en het bestaan van de *Business Practices* organisatie inclusief de gratis telefoonlijn.

De bovenstaande modellen zijn ook gemakkelijk uit te breiden tot meldingen van externen over het gedrag van de onderneming in het algemeen of een of enkele medewerkers in het bijzonder. Juist omdat het voor buitenstaanders moeilijk te achterhalen is wie verantwoordelijk is voor bepaald beleid dan wel gedrag van een betreffende medewerker, kan een centraal punt de toegankelijkheid aanzienlijk verbeteren. Het centrale punt draagt vervolgens de verantwoordelijkheid om de externe persoon met de juiste interne persoon in contact te brengen en erop toe te zien dat er adequate follow-up wordt gegeven. Een meldpunt voor externen kan mede gestalte geven aan het beleid op het gebied van maatschappelijk verantwoord ondernemen en daarbij informatie verschaffen voor externe rapportage.[38]

XVIII. Meldpunt voor externen



Type incident bepaalt wijze van aanpak

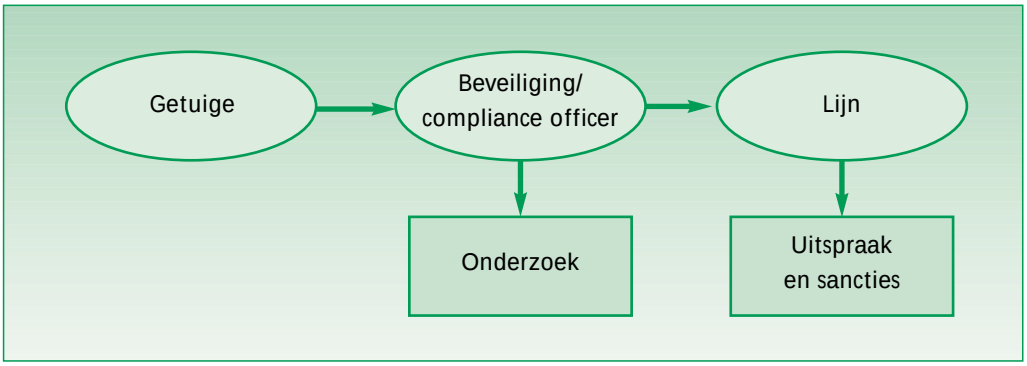
De wijze waarop de instanties in het vangnet aan elkaar zijn gerelateerd is afhankelijk van het type incident. Het maakt bijvoorbeeld verschil uit of er sprake is van een slachtoffer of niet, of de melding tot doel heeft corrigerende maatregelen te treffen of louter preventie beoogt, en of er sprake is van een lichte overtreding dan wel grove schendingen. Drie soorten meldingen zijn te onderscheiden die cruciaal zijn voor de afstemming van de rollen in het vangnet.

1. Overtredingen zonder duidelijk slachtoffer

Bij misbruik van bedrijfsmiddelen is er meestal geen persoon die daardoor direct gedupeerd raakt. Er is dan ook geen slachtoffer dat vanuit zijn eigenbelang de schending aan de orde stelt. Er zijn slechts getuigen of medewerkers met vermoe-

dens van een incident. Wanneer de lijn niet ontvankelijk is voor de melding, kan de getuige zich direct wenden tot de onderzoekende instantie dan wel indirect via de helpdesk/ meldpunt. In veel gevallen is de beveiligingsfunctionaris dan wel een andere compliance officer gerechtigd tot het doen van onderzoek. De betreffende functionaris start een onderzoek, dikwijls na toestemming van de bevoegde manager en doet op basis daarvan voorstellen voor maatregelen, waar de lijn verder over beslist.

XIX. Aanpak voor overtredingen zonder slachtoffer

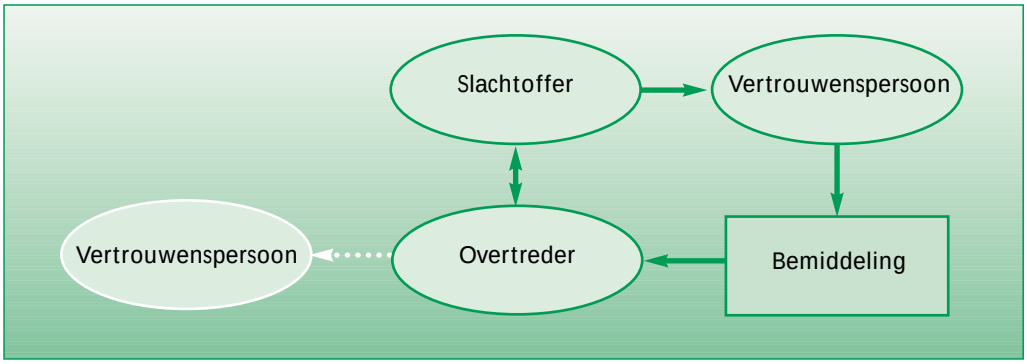


Het is onwenselijk dat een vertrouwenspersoon een meldpunt is voor misbruik van bedrijfsmiddelen en vervolgens zelf het onderzoek uitvoert. Eveneens is het onwenselijk dat een vertrouwenspersoon de melding overneemt en vervolgens zelfstandig in bijvoorbeeld de directie het incident aan de orde stelt. Vooral in een klein bedrijf zal de melding die door de vertrouwenspersoon wordt geventileerd, al snel terug zijn te voeren tot de betreffende medewerker. Temeer wanneer de medewerker zelf al eerder intern de lijn heeft benaderd om misstanden aan de orde te stellen. Bovendien bestaat de kans dat een vertrouwenspersoon die regelmatig het management op de hoogte stelt van concrete incidenten, al snel het draagvlak bij het management verliest. Als periodieke brenger van het slechte nieuws is het geen gemakkelijke opgave om steeds weer aandacht voor het incident te vragen. Juist daarom dient een vertrouwenspersoon in een klein bedrijf medewerkers die binnen de lijn melding willen doen van misstanden, te coachen om deze op een goede manier aan de orde te stellen. Zijn de condities om dit te doen afwezig, dan kan de vertrouwenspersoon hooguit de afwezigheid van deze condities in het management aan de orde stellen. Een dergelijke aanpak is minder bedreigend omdat er niet op de persoon wordt gespeeld en niet een concreet incident centraal staat. Juist in dergelijke situaties heeft de vertrouwenspersoon de taak om activiteiten te ontplooien om de openheid binnen de organisatie te waarborgen. Is de lijn of staf niet geëquipeerd of te veel partij in het zelf uitvoeren van onderzoek, dan is het wenselijk een externe onderzoeksinstantie in te schakelen.

2. Lichte overtredingen met slachtoffer

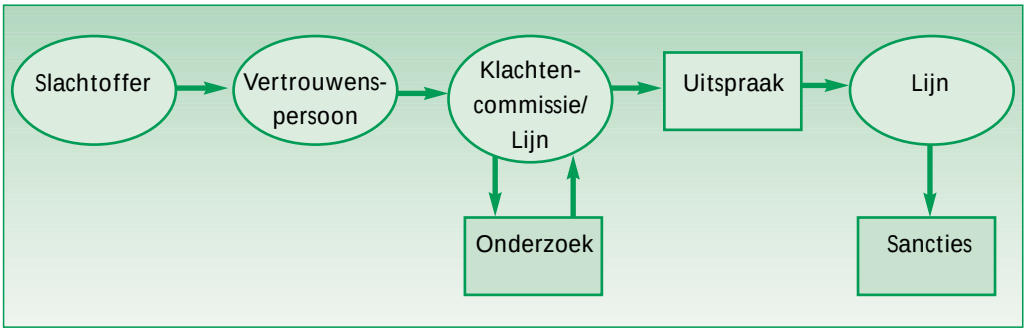
In geval van lichte overtredingen ten nadele van een medewerker gaat het er veelal om relaties voor de toekomst te herstellen, verschillen van opvattingen te verhelderen of systemen en structuren in het bedrijf te verbeteren zodat incidenten zich minder snel kunnen voordoen. Het is de taak van de vertrouwenspersoon om op verzoek te bemiddelen tussen het slachtoffer en de overtreder en ervoor te zorgen dat het conflict onderling wordt bijgelegd. Indien de vermeende dader erop staat, kan deze ook gebruikmaken van een andere vertrouwenspersoon of zelfs de bemiddeling laten plaatsvinden door een derde vertrouwenspersoon. Als bemiddeling niet gewenst is of niet tot het gewenste resultaat leidt, kan een onderzoek worden gestart.

XX. Aanpak voor lichte overtredingen met slachtoffer



3. Ernstige schendingen met slachtoffer

Is het slachtoffer zo ernstig gedupeerd (bijvoorbeeld aanranding of verkrachting) dat daarom correctieve acties noodzakelijk zijn, dan is bemiddeling niet meer op zijn plaats. Immers met de excuses van de overtreder en welgemeende beloftes voor de toekomst kan het slachtoffer niet tevreden worden gesteld. In dit geval zal, na overleg met de vertrouwenspersoon, de stap naar de eventueel aanwezige klachtencommissie worden genomen of een andere (interne dan wel externe) onderzoeksinstantie door het management worden gevraagd de feiten boven tafel te brengen. Vanwege de gewenste objectiviteit en professionaliteit van de vertrouwenspersoon dient deze het onderzoek niet zelf te verrichten. De klachtencommissie voert zelf het onderzoek uit of laat dat uitvoeren, op basis waarvan zij vervolgens tot een oordeel over de situatie komt. Het is dan aan de directie om vervolgens sancties te treffen. Een getuige van een overtreding waarvan een medewerker slachtoffer is geworden, zal over het algemeen geen stappen kunnen ondernemen zonder toestemming van het slachtoffer.



Het is wenselijk dat een organisatie per item uit haar code doordenkt wie binnen de staf verantwoordelijk is voor de naleving. Deze personen zijn in zekere zin allen te beschouwen als compliance officers. Deze rol moet niet worden verward met die van vertrouwenspersonen. Waar vertrouwenspersonen met name slachtoffers van inbreuken bijstaan en geen onderzoeker zijn, is een compliance officer onafhankelijker en wel geautoriseerd tot het instellen van een onderzoek. Compliance officers hebben doorgaans een veel actievere rol ten aanzien van het toezicht op en de handhaving van de integriteit binnen de organisatie dan een vertrouwenspersoon.

De *hotline* van Philips

Sinds 1 januari 2001 beschikt Philips Nederland over een interne meldlijn. De medewerkers zijn onder andere als volgt op de hoogte gesteld:
"In uw werk wordt u geconfronteerd met gedragingen die overduidelijk in strijd zijn met de Philips Gedragscode. U ergert zich er mateloos aan, vindt dat dit echt niet door de beugel kan en belt de Hotline. Het gratis nummer (0800-XXXXXX) verbindt u buiten de bedrijfscentrale om met een antwoordapparaat (24 uur per dag in bedrijf), dat tevens dienst kan doen als faxapparaat (let op: op een fax staat vaak de afzender vermeld; wilt u anoniem blijven, maak dan niet van deze mogelijkheid gebruik), en dat ergens in Eindhoven in een afgesloten ruimte staat. De compliance officer en de *ethics assistant* zijn de enigen die erbij kunnen. U spreekt de melding in en dezelfde dag of een dag later maakt de ethics assistant daar een transcript van. Heeft u uw naam genoemd, dan volgt binnen enkele dagen een ontvangstbevestiging. De compliance officer heeft het transcript dan al gelezen (en weer veilig opgeborgen), de melding geanalyseerd en zijn onderzoek in gang gezet. Kan hij dat laatste niet zelf, dan wordt een andere discipline ingeschakeld, bijvoorbeeld Internal Audit, Security of een collega-compliance officer bij een productdivisie. Verwijzing naar een lokale personeelsdienst of vertrouwenspersoon gebeurt alleen als de aanmelder (die in dit geval bekend moet zijn)

daarmee akkoord gaat. Afhankelijk van de complexiteit van de zaak moet de eindrapportage binnen vier tot zes weken klaar zijn. De aanmelder (wederom: mits bekend) krijgt dan te horen of gevolg kan worden gegeven aan zijn melding en zo ja wat er gaat gebeuren."

Philips Magazine, januari 2001

Rollen in vangnet

Vanwege de verschillende rollen die er in een vangnet zijn, is het wenselijk te doordenken welke instantie welke rol op zich neemt. In tabel XXII staan de rollen van de mogelijke instanties weergegeven. Tabel XXIII beschrijft drie ondersteunende rollen aan het vangnet.

XXII. Rollen in vangnet

	Rollen in vangnet	IF	IC	HD	VP	CO	KEC	STAF	LIJN
1	Vraagbaak/informatie-punt	x	x	x	x	x	x	x	x
2	Coach (steun/toeverlaat)	x			x				
3	Verwijzer	x	x	x	x	x		x	x
4	Bemiddelaar/facilitator	x			x		x		x
5	Goedkeurder	x				x		x	x
6	Onderzoeker	x				x	x	x	x
7	Ondersteuner bij verdediging	x			x				
8	Adviseur van maatregelen/sancties	x			x	x	x	x	
9	Registrator	x	x	x	x	x	x	x	x
10	Signaleerder en adviseur van beleid ter preventie (gevraagd/ongevraagd)	x	x	x	x	x	x	x	x
11	Aanjager	x	x	x	x	x	x	x	x
12	Nazorgverlener	x			x		x		
13	Bewaker	x	x	x	x	x	x	x	x

IF = Integriteitfunctionaris, IC = Integriteitcoördinator, HD = Helpdesk/Centraal Meldpunt, VP = vertrouwenspersoon, CO = compliance officer, KEC = klachtencommissie dan wel ethische commissie, STAF = overige stafafdelingen, LIJN = lijnmanagement

XXIII. Ondersteunende rollen voor vangnet

	Ondersteunende rollen in vangnet	STAF	LIJN
14	Normsteller/codeerder		x
15	Beslisser van sancties/scheidsrechter		x
16	Controleur	x	

Alhoewel niet alle rollen formeel behoeven te worden toegewezen, is het in alle gevallen wenselijk dat het management zich afvraagt wie zich binnen de organisatie op natuurlijke wijze de bovenstaande rollen heeft eigen gemaakt.

KPN Helpdesk Security & Integriteit

Mede in het kader van het onderzoek voor dit boekje, is bij KPN Telecom nagegaan in hoeverre een Helpdesk Integriteit wenselijk en haalbaar is. In samenwerking met onder andere de afdeling Security en Personeelszaken van KPN is een geïntegreerde helpdesk ontwikkeld en geïmplementeerd.
KPN beschikt sinds 1999 over een Helpdesk Security voor de beveiligingsvraagstukken waarmee management en medewerkers worden geconfronteerd (zoals diefstal, schade en calamiteiten en adviezen ter preventie). Bij de introductie van de KPN bedrijfscode 'Wat ons bindt', najaar 2000, is de helpdesk verbreed tot een helpdesk voor allerhande integriteitvraagstukken. De helpdesk sluit aan bij de wens van de Raad van Bestuur om intern te beschikken over een sluitend vangnet voor de naleving van de gehele code. In de code wordt daarom vrij uitvoerig verwezen naar de Helpdesk. "Binnen KPN kunnen medewerkers worden geconfronteerd met problemen, incidenten en vragen aangaande de naleving van de code. Indien het niet mogelijk is deze problemen in de lijn en/of met de direct betrokkenen op te lossen, dan kunnen medewerkers terecht bij de KPN-Helpdesk Security & Integriteit" aldus de bedrijfscode. Denkbare vraagstukken waarmee medewerkers zich tot de helpdesk kunnen wenden, lopen uiteen van het lekken van vertrouwelijke informatie, ongeautoriseerd gebruik van passwords, dupering van externen, belangenverstrengeling, (seksuele) intimidatie en bijvoorbeeld alcoholmisbruik. Leidinggevenden kunnen eveneens bij de helpdesk terecht voor ondersteuning bij het oplossen van integriteitvraagstukken die zich binnen hun afdeling of onderdeel voordoen.
De helpdesk is via een gratis 0800-nummer 24 uur per dag en zeven dagen per week voor iedere manager en medewerker bereikbaar. Er zijn acht medewerkers en een manager werkzaam bij de helpdesk. Zij zorgen voor de eerste opvang van de medewerker, registratie van de melding en doorverwijzing naar een functiona-

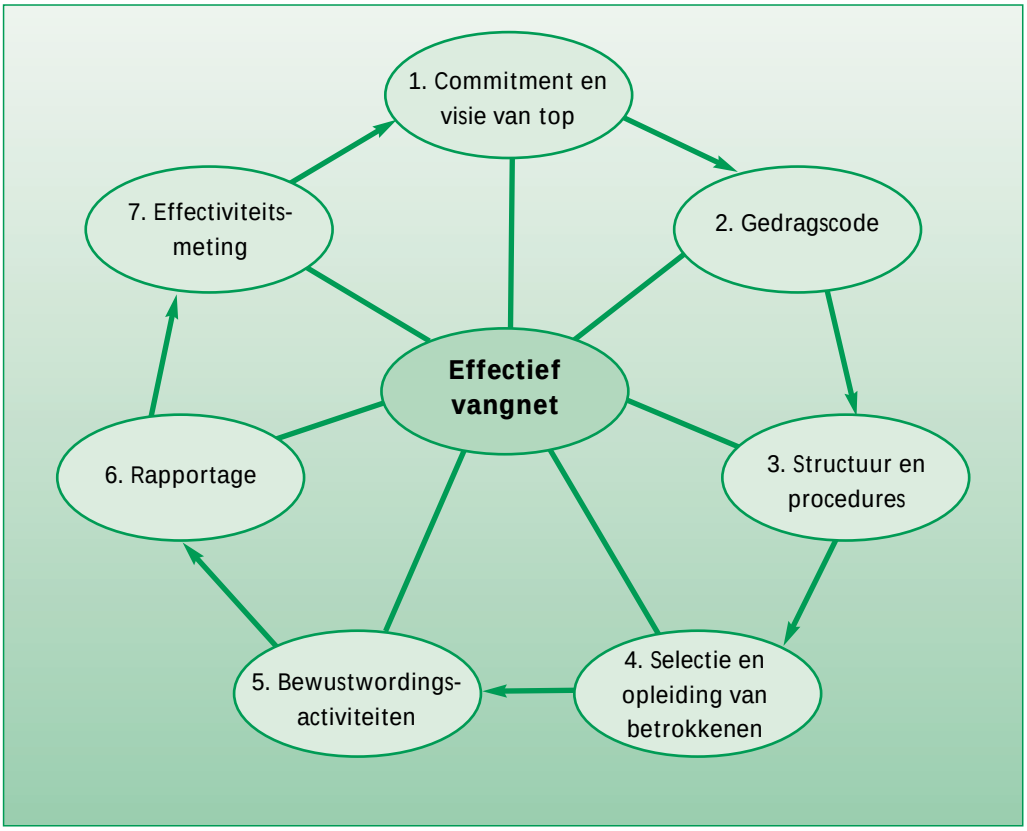
ris die de medewerker kan helpen. Functionarissen die de achterwacht vormen zijn onder andere de vertrouwenspersonen voor ongewenste omgangsvormen, de integriteitconsultants die incidenten onderzoeken en de compliance officers die toezicht houden op (interne en/of externe) regels en daarvoor als vraagbaak fungeren (zoals voor privacy, voorkennis, bedrijfsmiddelen en IT). Medewerkers kunnen zich ook direct wenden tot de vertrouwenspersoon binnen het eigen onderdeel of de betreffende compliance officer. Het hoofd Security verstrekt de voorzitter van de Raad van Bestuur alsmede de directeuren van de bedrijfsonderdelen periodiek informatie over de aard en omvang van de binnengekomen verzoeken bij de helpdesk. Drie analisten verzorgen de rapportages daarvoor. Via onder andere brochures, factsheets en berichten op de intra-site wordt het personeel voorgelicht over de werking van de helpdesk.

38 Zie Wempe, J., & Kaptein, M. (2000), *Ondernemen met het Oog op de Toekomst: Integratie van economische, sociale en ecologische verantwoordelijkheden*. Stichting Maatschappij en Onderneming.

7 Effectief implementeren van een intern vangnet

Een goed intern vangnet staat of valt met de structuur waarmee het vangnet wordt vormgegeven. Daarnaast zijn er verschillende andere factoren van belang die de effectiviteit van een vangnet bepalen. Het doel is een vangnet waarbij meldingen op een adequate wijze worden opgevangen en opgelost. Deze factoren zijn in figuur XXIV weergegeven.

XXIV. Model voor effectiviteit van intern vangnet



1. Commitment en visie van top

Uit onderzoek is gebleken dat de belangrijkste succesfactor van een vangnet het commitment van het management is.[39] Zo is het niet alleen belangrijk dat het management besluit een vangnet te creëren, maar juist ook dat het management hier verantwoordelijkheid voor blijft dragen en er ook bij betrokken blijft. Als het personeel het idee heeft dat het vangnet slechts een middel voor het management is om zijn verantwoordelijkheid te ontlopen, dan verminderen het gebruik en de effectiviteit ervan. Eveneens is het belangrijk dat het personeel het vangnet niet opvat als een motie van wantrouwen van de top naar de medewerkers of als een kliklijn om elkaar een 'oor aan te naaien'.

Drempelscan

Het verrichten van een drempelanalyse is een van de methoden om het management van een organisatie het belang van een vangnet te laten inzien. Via een enquête wordt (een deel van) het personeel gevraagd naar de drempels die zij ervaren bij het in de lijn aan de orde stellen van ongewenst gedrag. Iedere manager wordt voorafgaand aan dit onderzoek gevraagd een inschatting te geven van de eindresultaten op iedere vraag uit de enquête. Deze inschatting van het management biedt vervolgens de mogelijkheid om op basis van het onderzoek onder het personeel te bepalen in hoeverre het management goed zicht heeft op de drempels die medewerkers ervaren. Dikwijls blijkt het management een positiever beeld van de situatie te hebben. Het gebrek aan inzicht bij het management in de drempels die medewerkers ervaren is dikwijls juist de grootste drempel tot een open organisatie! Door in een bijeenkomst van het management het verschil in percepties te bespreken, wordt een begin gemaakt met het slechten van de drempels en dikwijls de noodzaak gevoeld voor een vangnet naast de lijn.

2. Gedragscode

Een gedragscode is het fundament voor een vangnet. Zonder code is er geen basis voor medewerkers om zich tot het vangnet te wenden. En zonder code heeft het vangnet (zelfs als het vangnet wordt uitbesteed) geen grond om medewerkers aan te spreken. In een code dient niet alleen te zijn opgenomen welke gedragingen wenselijk zijn dan wel verboden. Een code dient juist de openheid van de organisatie te onderstrepen. Openheid om elkaar onderling en desnoods het management aan te spreken, zodat het interne vangnet geen vervanging wordt voor de lijn. Dit vereist ook dat de code onderstreept dat medewerkers nooit schade zullen ondervinden als

zij weloverwogen en welgezind incidenten aan de orde stellen. Juist ook in het midden- en kleinbedrijf is een code/huisregels een waardevol instrument om de integriteit van de organisatie te communiceren. Het gaat daarbij niet zozeer om een glossy folder of boekwerk, maar om bij wijze van spreken een A4'tje dat verwoordt waar de organisatie voor staat.

Om de gedragscode tot leven te brengen, dient aandacht te worden besteed aan de implementatie ervan. Het gaat er daarbij om dat medewerkers zelf de vertaalslag maken naar wat de code voor hen betekent. Bijvoorbeeld "Wat betekenen zuivere omgangsvormen voor mijn functioneren?" en "Wat betekent het zorgvuldig omgaan met vertrouwelijke informatie in mijn werk?". Door binnen de afdeling de code bespreekbaar te maken wordt als het ware geoefend met sociale correctie en wordt ook inzicht gekweekt in de integriteitsrisico's van de werkzaamheden die worden uitgevoerd. Het boekje *De Integere Organisatie: het nut van een bedrijfscode* geeft enkele handvatten voor de implementatie van een code.[40] Juist bij de implementatie van de code kunnen de functionarissen van het vangnet zich presenteren. Zo kunnen bijvoorbeeld vertrouwenspersonen enkele dilemma's over omgangsvormen in het afdelingsoverleg aan de orde stellen en kan de compliance officer tekst en uitleg geven over enkele regels.

KPN

"...De bovenstaande waarden en verantwoordelijkheden horen bij KPN. Werken bij KPN betekent dan ook dat alle medewerkers, van 'laag' tot 'hoog', persoonlijk aanspreekbaar zijn op de wijze waarop de code wordt vertaald in hun gedrag en werkveld. Leidinggevenden zorgen er daarom voor dat de code bekend is bij hun medewerkers. Managers zijn er op gericht een open klimaat te scheppen waarin medewerkers en leidinggevenden elkaar aanspreken op naleving van de code."

KPN Bedrijfscode "Wat ons bindt"

3. Structuur en procedures

Voor een effectief vangnet is het wenselijk dat de verantwoordelijkheden en taken van de betrokken instanties en de procedures schriftelijk worden vastgelegd. Een dergelijk document geeft niet alleen bescherming aan de leden van het vangnet zelf, maar ook aan de medewerkers die betrokken raken bij het vangnet (zowel slachtoffer, klager, getuige als verdachte). Zaken als geheimhouding, verschoningsrecht, onafhankelijkheid, zorgvuldigheid, bescherming van de klokkenluider tegen represailles en mogelijkheden tot verweer dienen daarbij te worden behandeld. Ook

dient bijvoorbeeld duidelijk gemaakt te worden dat de melder serieus wordt genomen, maar de melding niet klakkeloos wordt aangenomen.

Klachtenregeling seksuele intimidatie burgerlijk rijkspersoneel

"...De klacht wordt uiterlijk binnen twee jaar na de confrontatie ingediend. De vertrouwenspersoon is met inachtneming van de nodige vertrouwelijkheid bevoegd de beklaagde of andere betrokkenen binnen de dienst te horen en informatie in te winnen, voor zover dit voor de uitvoering van de taken noodzakelijk is... De klager en de beklaagde kunnen zich tijdens het horen door een raadsman of -vrouw laten bijstaan... De vergaderingen van de klachtencommissie zijn niet openbaar... Het bevoegd gezag biedt de vertrouwenspersonen en de leden van de klachtencommissie de faciliteiten die nodig zijn voor de uitvoering van de opgedragen taken..."

4. Selectie & opleiding

Niet iedereen kan zomaar de functie van bijvoorbeeld een vertrouwenspersoon op zich nemen. Enerzijds dient een goede vertrouwenspersoon van nature een aantal eigenschappen te bezitten, zoals de gave om naar anderen te luisteren en invoelingsvermogen. Anderzijds dient door middel van training een aantal vaardigheden te worden aangeleerd, zoals het stellen van de juiste vragen om volledige informatie te krijgen. Adequate selectie, opleiding en periodieke training zijn dan ook noodzakelijk. Afhankelijk van de rol in het vangnet, zijn benodigde kwaliteiten die al snel over het hoofd worden gezien onder andere:

- communicatievaardigheden (spreken en met name luisteren);
- bemiddelingsvaardigheden;
- onderzoeksvaardigheden;
- organisatievaardigheden om het incident in de context te plaatsen;
- adviesvaardigheden (inzicht in adequate sancties en maatregelen teneinde ook volwaardige discussiepartner voor het management te zijn).

Om de motivatie van de direct betrokken functionarissen te behouden en afstemming tussen de werkzaamheden te verzekeren is het wenselijk dat er regelmatige bijeenkomsten plaatsvinden van de betrokkenen bij het vangnet. Tijdens een dergelijk overleg kunnen bijvoorbeeld pijnlijke en positieve ervaringen worden uitgewisseld en kan van actuele cases worden nagegaan hoe daarmee het best kan worden omgegaan. Vooral bieden dergelijke bijeenkomsten de mogelijkheid om de afstemming tussen de loketten binnen het vangnet te verbeteren.

Vertrouwensteam Parity Solutions

Parity Solutions is een ICT-organisatie met 180 medewerkers. De organisatie beschikt sinds medio 2000 over twee vertrouwenspersonen en een klachtencommissie. Eén van de twee vertrouwenspersonen is lid van het managementteam waarmee het bedrijf wil aangeven het vertrouwenswerk serieus te nemen. Tegelijkertijd beoogt men laagdrempeligheid door ook iemand die niet lid is van het managementteam vertrouwenspersoon te laten zijn. Medewerkers zijn kort na de installatie van de vertrouwenspersonen door middel van een brief op de hoogte gebracht van wat ongewenste omgangsvormen zijn en wat er gedaan kan worden als men ermee te maken krijgt. Daarnaast is er een uitgebreide beschrijving gemaakt van de taken van de vertrouwenspersonen en de klachtencommissie en is er een officiële klachtenprocedure opgesteld. Het bijzondere aan de procedure is dat er ook met name aandacht wordt besteed aan de drempels tot melding die men kan ondervinden. Door deze van tevoren al te identificeren en ze indien mogelijk te ontkrachten, wordt de procedure voor de medewerkers toegankelijk. Doordat de medewerkers vrijwel allemaal gedetacheerd zijn bij andere bedrijven is het voor het bedrijf echter lastig te bepalen in hoeverre medewerkers de code en procedures naleven.

5. Bewustwordingsactiviteiten

De aanwezigheid van een vangnet betekent nog niet dat dit algemene bekendheid en vertrouwen geniet. Communicatie over de functies en werkwijze van het vangnet is dan ook wenselijk. Medewerkers moeten niet alleen weten waar zij aan toe zijn als zij het vangnet consulteren, maar ook met welke kwesties zij zich al dan niet tot het vangnet kunnen wenden. Een vangnet dat bekendheid blijft genieten, vergt regelmatige communicatie. Tal van instrumenten zijn daarvoor aanwezig:

- toolbox (met bijvoorbeeld een discussiemethodiek, video en casuïstiek);
- posters;
- presentaties;
- interviews en artikelen in bedrijfsblad;
- een interne site;
- e-mail;
- succesverhalen.

Het is ook belangrijk voor de functionarissen van het vangnet dat zij bekend en gekend worden. Actieve betrokkenheid (bijvoorbeeld *by walking around*) is dan ook cruciaal.

De Bestuursdienst van de Gemeente Amsterdam

Bij de gemeente Amsterdam zijn 22.000 ambtenaren werkzaam verdeeld over 13 stadsdelen en 40 diensten. Binnen ieder stadsdeel en elke dienst is in principe een vertrouwenspersoon aangesteld.
De Bestuursdienst beschikt over een parttime vertrouwenspersoon, een klachtencommissie en een ombudsman die zich bezighoudt met klachten van externen.
De vertrouwenspersoon bij de Bestuursdienst functioneert met name als een soort psycholoog. Hij staat open voor vrijwel alles wat de medewerkers van de dienst persoonlijk raakt en waar zij over willen praten. Dit zorgt voor een lage drempel tot melden. De activiteiten van de vertrouwenspersoon hebben in de praktijk vooral te maken met meldingen over ongelijke behandeling, onheuse bejegening door leidinggevenden en seksuele intimidatie.
Om het belang van het vertrouwenswerk te onderstrepen, geeft de vertrouwenspersoon tweemaal per jaar een presentatie over zijn werk tijdens een introductiebijeenkomst voor nieuwe medewerkers. De vertrouwenspersoon ervaart dat naarmate hij meer tijd aan het vertrouwenswerk besteedt, het beroep dat op hem wordt gedaan toeneemt.

Belastingdienst

"De elf vertrouwenspersonen die in 1989 over de Belastingdienst waren verspreid, hielden zich intensief bezig met voorlichting, het maken van voorlichtingsmateriaal, verzorgen van publicaties en het op de agenda zetten van het thema. Achteraf overziend had een aantal zaken anders moeten worden aangepakt. De elf vertrouwenspersonen zijn weliswaar goed opgeleid, maar zijn vervolgens zonder voldoende ondersteuning van bovenaf, te veel alleen gelaten. Bovendien zagen we onszelf toch wel een beetje als idealisten, we hadden een missie. Wij werden de vertolkers van de boodschap. Maar wij waren niet de beleidsmakers, wij waren de uitvoerders van het beleid. Bovendien hadden wij ons te veel gericht op de medewerkers, waardoor de leidinggevenden buiten schot bleven. Inmiddels zijn er op dit gebied al een aantal zaken veranderd.
In de eerste jaren, 1989 en 1990, kwamen er in totaal 10 klachten binnen bij de vertrouwenspersonen. Over 1999 zijn er 75 klachten en 127 meldingen geregistreerd. Onder meldingen verstaat de Belastingdienst zaken die worden gemeld aan de vertrouwenspersoon, maar waar verder geen actie op is ondernomen."

M. Krom, vertrouwenspersoon bij de Belastingdienst

6. Registratie en rapportage

Registratie en rapportage bieden mogelijkheden tot leren en bijsturen. Vragen die zich hierbij voordoen zijn:

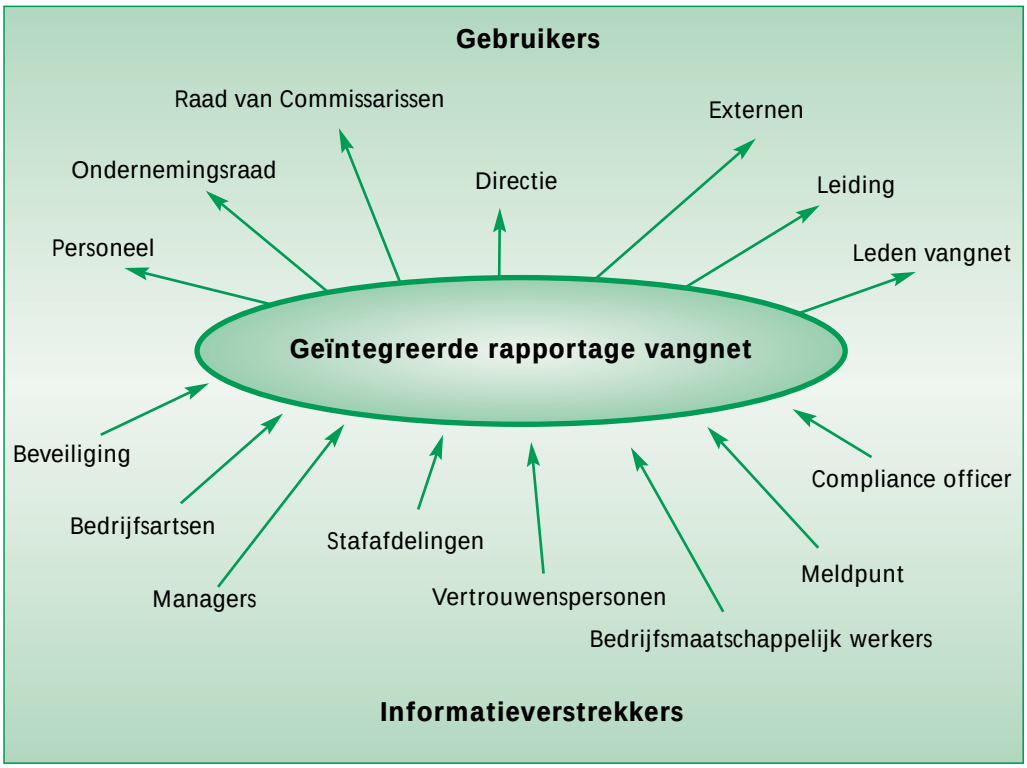
- Wat wordt geregistreerd?
- Hoe vindt registratie plaats?
- Op welke wijze wordt de geregistreerde informatie geanalyseerd?
- Wat is het aggregatieniveau waarop wordt gepresenteerd?
- Wie ontvangt de rapportage?
- Wat is de frequentie van de rapportage?
- Wordt de rapportage gecontroleerd en, zo ja, door wie?

ICC Business Charter for Corporate Citizenship

De Internationale Kamer van Koophandel (ICC) heeft in november 2000 een conceptcode opgesteld voor verantwoord management. De in totaal zestien principes gaan onder andere over werknemerseducatie, bescherming van het milieu, mensenrechten en verspreiding van technologie. Het laatste principe handelt over compliance en rapportage. Bedrijven die met de code instemmen verklaren dat zij regelmatig audits en doorlichtingen (laten) verrichten naar de naleving (compliance) van de ondernemingsstandaarden, wettelijke verplichtingen en de principes zoals die in de code van de ICC staan omschreven. Op basis van deze doorlichtingen wordt periodiek informatie verstrekt aan de Raad van Commissarissen, aandeelhouders, werknemers, autoriteiten en de maatschappij.

Over het algemeen is een rapportagestructuur gewenst waarbij alle incidenten die gemeld worden ook worden geregistreerd. Aan de hand van de registraties kan dan een rapportage gemaakt worden die zowel aan het management als aan de functionarissen in het vangnet wordt verstrekt. Het is wenselijk dat de rapportage wordt meegenomen in de overlegplatforms binnen de organisatie (managementoverleg, overleg met de Ondernemingsraad, overleg met het middenkader etc.) en het beleid aan de hand van de rapportage wordt geëvalueerd. Om te voorkomen dat de aandacht voor integriteitzorg verslapt, is het noodzakelijk dat deze rapportage regelmatig plaatsvindt. In het gunstigste geval wordt de rapportage meegenomen in de beoordelingsgesprekken van het management.

XXV. Mogelijke gebruikers van geïntegreerde rapportage



7. Effectiviteitmeting

Onderzoek naar de effectiviteit van het vangnet onderstreept naar het personeel toe des te meer dat het management het vangnet serieus neemt. Vrij eenvoudig zijn enkele vragen over het functioneren van het vangnet mee te nemen in bijvoorbeeld een jaarlijks tevredenheidsonderzoek onder het personeel. Een diepgaande beoordeling van het vangnet zal gepaard gaan met een analyse van de bereikbaarheid, snelheid van de follow up, aantal geslaagde bemiddelingen, trendanalyse van de klachten en meldingen, de tevredenheid bij direct betrokkenen en juist ook de tevredenheid van de leden van het vangnet zelf. Op deze manier wordt het maximale gedaan om een optimaal vangnet te creëren.

Philips Nederland

"In de Verenigde Staten, waar de publieke belangstelling voor bedrijfsethiek groter is dan elders, werkt de Philips organisatie al langer met een telefonische meldlijn. Ik hoop dat er net als daar ook hier in Nederland regelmatig gebruik van wordt gemaakt. Niet omdat ik het leuk zou vinden te constateren dat we het hier in Nederland niet zo nauw nemen met de gedragsregels - er is overigens geen enkele aanleiding om dat te denken - maar omdat dat zou betekenen dat de Hotline een succes is. Deze meldlijn kan in mijn ogen zeker een steentje bijdragen aan de verantwoorde wijze van werken binnen de onderneming."

Mr. Dries Duynstee, country compliance officer van Philips in Nederland als toelichting op de per 1 januari 2001 in werking gestelde meldlijn

Ten slotte

Met dit boekje hebben wij getracht uw organisatie handvatten aan te reiken voor het ontwerpen en implementeren van een sluitend vangnet binnen uw organisatie. Het zijn slechts handvatten. Omdat iedere organisatie uniek is, is het aan iedere organisatie de uitdaging om een vangnet op maat te creëren. Een sluitend en goed gepositioneerd vangnet zal de organisatie en de medewerkers zeker helpen om ongewenst gedrag te verhelpen. Niet alleen repressief maar ook preventief! Wij wensen u met deze uitdaging veel succes.

39 Hofstede, M. (2000), *De Effectiviteit van Vertrouwenspersonen*. KPMG Ethics & Integrity Consulting, Amstelveen.

40 Kaptein, M., Klamer, H., & Linden, ter J. (1999), *De Integere Organisatie: Het nut van een bedrijfscode*. NCW, KPMG en Nationaal Platform Criminaliteitsbeheersing, Den Haag Media Groep, Rijswijk.

Relevante literatuur

- Amstel, R. & Volkers, H.J. (1993), *Seksuele Intimidatie: Voorkomen en beleid voeren: ervaringen bij 50 arbeidsorganisaties*. Den Haag: SDU.
- Bezemer, W. (1996), *Seksuele Intimidatie: Vijftig tips*. Alphen a/d Rijn: Samsom.
- FNV (2000), *Aanpak Ongewenste Omgangsvormen*. Amsterdam: Hoonte, Bosch & Keuning.
- *Handboek Fraudepreventie en Integriteit*. Alphen a/d Rijn: Samsom.
- *Het Groot Arbowerk*. Alphen a/d Rijn: Samsom (o.a. P.J. van der Zwet, (2000) 'Vertrouwenswerk: het organisatiebelang voorop', B8030-1 t/m B8030-16).
- Hofstede, M. (2000). *De Effectiviteit van Vertrouwenspersonen*. KPMG Ethics & Integrity Consulting, Amstelveen.
- Kaptein, M. (1998), *Ethics Management*. Dordrecht: Kluwer Academic Publishers.
- Kaptein, M., Klamer, H., & Linden, ter J. (1999), *De Integere Organisatie: Het nut van een bedrijfscode*. KPMG, NCW en Stichting Beroepsmoraal en Misdaadpreventie. Den Haag.
- Stichting van de Arbeid (2000), *Met Alle Respect!* Den Haag.

Zie voor meer literatuur op het gebied van vangnetten: www.ethiekmanagement.nl.

Websites

De website van het Nationaal Platform Criminaliteitsbeheersing (NPC) www.npc-web.nl geeft informatie over de aanpak van criminaliteit waarvan het bedrijfsleven slachtoffer wordt. In het NPC werken overheid en bedrijfsleven samen aan: voertuigcriminaliteit, integriteit/beroepsmoraal, thema's rondom financiële instellingen, informatiebeveiliging, regionale platforms, overvalcriminaliteit, publiek-privaat evenwicht, keurmerk veilig ondernemen, aangiftebereidheid en kwaliteitsmeter veilig uitgaan.
Onder de NPC-website vindt u tevens nadere informatie over de Stichting Beroepsmoraal en Misdaadpreventie. Hier treft u ook de tekst aan van dit boekje en de bijbehorende checklisten.

Op de website van de Vereniging VNO-NCW www.vno-ncw/criminaliteitsbeheersing.nl vindt u tips voor preventie en nieuws over criminaliteitsbeheersing in het bedrijfsleven.

De website www.ethiekmanagement.nl biedt personen die binnen organisaties werkzaam zijn op het gebied van ethiek en integriteit, een netwerk waarin zij informatie en ervaringen kunnen uitwisselen.
Tot de doelgroep behoren met name: (centrale) vertrouwenspersonen, compliance officers, integriteitfunctionarissen en -coördinatoren, ethiekmanagers, duurzaamheid officers, bedrijfsbeveiligers en riskmanagers.
De internetsite bevat: een mediarubriek, een activiteitenoverzicht (congressen, workshops), links naar relevante organisaties en netwerken, discussiegroepen (bijvoorbeeld over de invoering van een vangnet), instrumenten (checklisten), databestanden en publicaties (artikelen, boekverwijzingen, scripties).

Checklisten

1

Checklist 1: nut en noodzaak van integriteitzorg

Vul de onderstaande tabel in voor uw organisatie om te bepalen welke integriteitvraagstukken met name aandacht dienen te krijgen.

1. Welke (bijzondere) wetten gelden er? (kolom A)
2. Welke interne gedragscode(s), regels en procedures gelden er? (kolom B)
3. Wat is de (geschatte) frequentie waarmee integriteitinbreuken zich binnen de organisatie voordoen? (kolom C)
4. Wat zijn de (geschatte) kosten die gemoeid zijn met de betreffende integriteitinbreuken? (kolom D)
5. Wat zijn de geschatte toekomstige baten indien het huidige beleid zou worden verbeterd? (kolom E)
6. Kortom, op welke vraagstukken zou de organisatie zich in de toekomst volgens u met name moeten richten?

	Inbreuken/ vraagstukken	**A** Geldende wetten	**B** Interne gedrags-code(s)/ regels/ procedures	**C** Frequentie incidenten binnen de organisatie	**D** Indicatie huidige kosten voor de organisa-tie	**E** Verwachte toekomsti-ge baten bij gewijzigd beleid
1	Fraude					
2	Criminaliteit/diefstal					
3	Corruptie					
4	Misbruik werktijden/inzet					

	Inbreuken/ vraagstukken	**A** Geldende wetten	**B** Interne gedrags-code(s)/ regels/ procedures	**C** Frequentie incidenten binnen de organisatie	**D** Indicatie huidige kosten voor de organisa-tie	**E** Verwachte toekomsti-ge baten bij gewijzigd beleid
5	Privé-gebruik bedrijfsmiddelen					
6	(Seksuele) intimidatie/ machtsmisbruik					
7	Discriminatie					
8	Agressie en geweld					
9	Pesten					
10	Strijdige nevenactiviteiten					
11	Misbruik vertrouwelijke informatie (voorkennis, lekken)					
12	Overige vormen (bijvoor-beeld wetsontduiking, milieuschade, consumen-teninbreuken, verslaving)					
13						
14						

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.

2

Checklist 2: openheid binnen de organisatie

Vul de antwoorden op de onderstaande vragen in in de bijbehorende tabel. Indien mogelijk, splits de antwoorden uit naar het type integriteitvraagstuk.

1. Welke drempels ondervinden uw medewerkers voor het onderling aanspreken? (kolom A)
2. Welke drempels ondervinden uw medewerkers voor het melden van incidenten bij hun leidinggevende? (kolom B)
3. In hoeverre staat het hoger echelon (in de ogen van het personeel) open voor meldingen van incidenten vanuit de organisatie? (kolom C)
4. Wat is binnen uw organisatie de (impliciete) code voor het ventileren van kritiek? (zie Figuur IV)
5. Kunt u het percentage inschatten van de mate waarin incidenten collegiaal of via de lijn adequaat worden opgepakt? (kolom D)
6. Op welk niveau zou u uw organisatie willen plaatsen inzake de zelfcorrectie tussen medewerkers onderling en in de lijn? (zie figuur V)
7. Kortom, welke inbreuken worden onvoldoende binnen de lijn aan de orde gesteld?

	Inbreuken/ vraagstukken	**A** Collegiale drempels	**B** Drempels ten aanzien van leidinggevende	**C** Drempels ten aanzien van hoger echelon	**D** Percentage van incidenten dat binnen de lijn succesvol wordt gecorrigeerd
1	Fraude				
2	Criminaliteit/diefstal				
3	Corruptie				
4	Misbruik werktijden/inzet				

	Inbreuken/ vraagstukken	**A** Collegiale drempels	**B** Drempels ten aanzien van leidinggevende	**C** Drempels ten aanzien van hoger echelon	**D** Percentage van incidenten dat binnen de lijn succesvol wordt gecorrigeerd
5	Privé-gebruik bedrijfsmiddelen				
6	(Seksuele) intimidatie/ machtsmisbruik				
7	Discriminatie				
8	Agressie en geweld				
9	Pesten				
10	Strijdige nevenactiviteiten				
11	Misbruik vertrouwelijke infor-matie (voorkennis, lekken)				
12	Overige vormen (bijvoorbeeld wetsontduiking, milieuschade, consumenteninbreuken, verslaving)				
13					
14					

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.

3

Checklist 3: het huidige vangnet

Vul de antwoorden op de onderstaande vragen in in de bijbehorende tabel. Indien mogelijk, splits de antwoorden uit naar het type integriteitvraagstuk.

1. Waar kunnen medewerkers meldingen omtrent incidenten buiten de lijn - maar binnen de organisatie - neerleggen? (kolom A)
2. Welke taken hebben de loketten van het interne vangnet? (kolom B)
3. Voor wie is het loket bestemd? (kolom C)
4. Bij welke externe instanties kunnen medewerkers eventueel ook terecht met betrekking tot meldingen? (kolom D)
5. Welke taken hebben de loketten van het externe vangnet? (kolom E)
6. In hoeverre wordt er gebruikgemaakt van deze externe instanties? (kolom F)

	Inbreuken/ vraagstukken	**A** Loket	**B** Taken	**C** Doelgroep	**D** Externe instantie	**E** Taken externe instantie	**F** Gebruik externe instantie
1	Fraude						
2	Criminaliteit/diefstal						
3	Corruptie						
4	Misbruik werktijden/inzet						
5	Privé-gebruik bedrijfsmiddelen						
6	(Seksuele) intimidatie/ machtsmisbruik						
7	Discriminatie						
8	Agressie en geweld						
9	Pesten						
10	Strijdige nevenactiviteiten						
11	Vertrouwelijke informatie						
12	Overige vormen (bijvoorbeeld wetsontduiking, milieuschade, consumenten-inbreuken, verslaving)						
13							
14							

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.

4 Checklist 4: de effectiviteit van het intern vangnet

Vul de antwoorden op de onderstaande vragen in in de bijbehorende tabel.

1. Hoeveel meldingen komen er via het huidige interne vangnet per loket binnen? (kolom A)
2. Welke drempels ondervinden medewerkers bij het contact zoeken per loket van het vangnet? (kolom B) (Het is te overwegen om een kleine enquête uit te zetten onder (een selectie van) medewerkers of enkele interviews met medewerkers af te nemen). (kolom B)
3. Wat is het oordeel over het functioneren van het loket? (kolom C) Geef dit bijvoorbeeld aan met een cijfer van 1 tot 10. (Het is te overwegen om medewerkers die gebruik hebben gemaakt van het vangnet te vragen naar hun ervaringen en hoe zij oordelen over de kwaliteit van de hulp, het onderzoek enz. Houd daarbij rekening met de vertrouwelijkheid van de melders.)
4. Wat zijn de afwijkingen/discrepanties tussen het wenselijke en het huidige functioneren per loket? (kolom D)
5. Wat zijn de oorzaken voor de in kolom D beschreven discrepanties? Hoe hangen deze samen met de in hoofdstuk 4 genoemde factoren? (kolom E)
6. Geef redenen aan waarom uw organisatie het beter doet dan het beeld dat ontstaat uit de onderzoeken naar vangnetten. Met andere woorden: wees pas tevreden en zeker wanneer u voldoende overtuigend bewijs heeft over een effectief vangnet.

	Loket	**A** Aantal meldingen	**B** Drempels	**C** Oordeel functioneren loket	**D** Afwijking huidige en gewenste situatie	**E** Oorzaken afwijking
1	Lijn					
2	Staf					
3	Beveiliging					
4	Bedrijfsmaatschappelijk werk					
5	Ondernemingsraad					
6	Vertrouwenspersoon					
7	Compliance officer					
8	Klachtencommissie					
9	Overige loketten					

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.

5

Checklist 5: beslispunten ten aanzien van een eigen vangnet

Vul de antwoorden op de onderstaande vragen in.

1. Wat is uw keuze ten aanzien van de beslispunten, daarbij de uitgangspunten in ogenschouw nemend?

	Beslispunten	Keuze
1	Voorkomen onnodige meldingen of signaleren alle relevante meldingen?	
2	Intern meldpunt en/of extern meldpunt?	
3	Eén loket of een loket per vraagstuk?	
4	Centraal of decentraal?	
5	Voor medewerkers en/of externen?	
6	Fulltime of parttime?	
7	Eén voor allen of één op één?	
8	Onderzoek door leidinggevende en/of staf?	
9	Centrale en/of decentrale registratie?	
10	Centrale melding van incidenten of zelfreiniging van afdelingen?	
11	De functie van toezichthouder en vraagbaak scheiden of verenigen?	
12	Anoniem melden of identificeren?	
13	Klachtencommissie of niet?	

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.

6

Checklist 6: vormgeving van een eigen intern vangnet

1. Ga na wie de rollen uit tabel XXII en XXIII binnen uw organisatie krijgt toebedeeld.
2. Teken het voor uw organisatie gewenste vangnet. Ga daarbij als volgt te werk:
   A: Zet de inbreuken waarvoor u buiten de lijn een vangnet wil hebben op de horizontale as.
   B: Zet verticaal de loketten.
   C: Trek lijnen van het type inbreuk naar het daarvoor bestemde loket.
   D: Bepaal of er een centraal loket voor komt en/of een coördinator achter de loketten.
   E: Bepaal de onderlinge relaties tussen de loketten door voor de drie centrale processen na te gaan hoe die moeten worden doorlopen.
   F: Geef achter de loketten een korte omschrijving van de inrichting (voortvloeiend uit checklist 5). Bijvoorbeeld aantal, centraliteit en omvang functie.
3. Vergelijk het gewenste vangnet met het huidige vangnet en ga na welke aanpassingen dienen te geschieden.

	Rollen in vangnet	**Instantie**
1	Vraagbaak/informatiepunt	
2	Coach (steun/toeverlaat)	
3	Verwijzer	
4	Bemiddelaar/facilitator	
5	Goedkeurder	
6	Onderzoeker	
7	Ondersteuner bij verdediging	
8	Adviseur van maatregelen/sancties	
9	Registrator	
10	Signaleerder en adviseur van beleid ter preventie (gevraagd/ongevraagd)	
11	Aanjager	
12	Nazorgverlener	
13	Bewaker	
14	Normsteller/codeerder	
15	Beslisser van sancties/scheidsrechter	
16	Controleur	

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.

7

Checklist 7: een effectieve implementatie van het interne vangnet

1. Wat is het oordeel over de huidige inbedding van de onderstaande factoren? (kolom A)
2. Wat dient over 2 jaar de situatie te zijn per factor? (kolom B)
3. Welke activiteiten dienen te worden ontplooid om de kloof tussen de huidige en gewenste situatie binnen 2 jaar te overbruggen (kolom C)?

	Factoren	**A** Oordeel huidige situatie	**B** Gewenst functio-neren over 2 jaar	**C** Te ontplooien acti-viteiten om kloof tussen huidige en gewenste situatie te overbruggen
1	Commitment en visie van top			
2	Gedragscode			
3	Implementatie gedragscode			
4	Code voor vangnet (functionarissen, melders en verdachten)			
5	Selectie en opleiding			
6	Bewustwordingsactiviteiten			
7	Rapportage			
8	Effectiviteitmeting			

Deze checklist kunt u downloaden via webpagina www.npc-web.nl; klik aan Integriteit/Beroepsmoraal.