



INLEIDING SYSTEEMGERICHT TOEZICHT MILIEU EN VEILIGHEID VOOR GROTE BEDRIJVEN

Juli 2009

Inleiding systeemgericht toezicht milieu en veiligheid voor grote bedrijven

Juli 2009

Drs. K. Huizinga
VROM-Inspectie
Cascadeplein 10
Postbus 30020
9700 RM Groningen

Inhoudsopgave

1	INLEIDING	4
1.1	AANLEIDING	4
1.2	DOEL	5
1.3	LEESWIJZER	5
2	WAT IS SYSTEEMTOEZICHT?	6
2.1	HISTORIE	6
2.2	AFBAKENING, BEGRIPPEN EN WERKDEFINITIES	8
2.2.1	<i>Werkdefinities</i>	8
2.2.2	<i>Systeemtoezicht nader bekeken</i>	9
2.2.3	<i>Vermogen tot zelfcontrole</i>	10
2.2.4	<i>Dimensies van systeemtoezicht</i>	11
3	VERTROUWEN	13
3.1	INLEIDING	13
3.2	VERTROUWEN OPERATIONALISEREN	13
4	EFFECTIVITEIT VAN SYSTEEMGERICHT TOEZICHT	18
4.1	INFORMATIEPOSITIE TOEZICHTHOUDER	18
4.2	RISICO GESTUURD TOEZICHT	18
4.3	STIMULANS TOT LEREN	19
4.4	EFFICIËNTIE	19
4.5	CONCLUSIE	20
5	SYSTEEMTOEZICHT IN DE PRAKTIJK	21
5.1	PILOTS FRONTOFFICES CHEMIE EN AFVAL	21
5.2	SYSTEEMTOEZICHT IN ANDERE DOMEINEN	23
6	SYSTEEMGERICHT TOEZICHT; WANNEER IS HET ZINVOL?	24
6.1	UITGANGSPUNTEN	24
6.2	RANDVOORWAARDEN VOOR SYSTEEMGERICHT TOEZICHT	24
6.3	INTERVENTIES EN SYSTEEMGERICHT TOEZICHT	28
7	VERDERE ONTWIKKELING	30
	BIJLAGE 1 LIJST MET AFKORTINGEN	31
	BIJLAGE 2 ERVARINGEN IN DE VERENIGDE STATEN	32
	BIJLAGE 3 CRITERIA VOOR COMPLIANCE AND ETHICS PROGRAMS (US FEDERAL SENTENCING GUIDELINES 2004, CHAPTER 8)	35
	BIJLAGE 4 VRAGENLIJST COMPLIANCE COMPETENCE AUDIT	36
	BIJLAGE 5 TOELICHTING VRAGENLIJST COMPLIANCE COMPETENCE AUDIT	40
	BIJLAGE 6 EISEN NIVEAUS COMPLIANCE MANAGEMENT	46
	BIJLAGE 7 AFSPRAKENMODEL SYSTEEMGERICHT TOEZICHT	47

1 Inleiding

1.1 Aanleiding

De overheid wil het toezicht op de naleving van regels efficiënter en effectiever uitvoeren. De overweging hierbij is de algemene behoefte aan vermindering van de toezichtslast voor het bedrijfsleven. Maar ook van overheidszijde wordt in het algemeen de wenselijkheid van een verhoogde samenwerking en verbeterde kwaliteit van toezicht onderschreven. Diverse initiatieven tot verdere professionalisering zijn inmiddels ondernomen (methodiekontwikkeling, bundeling van uitvoeringscapaciteit).

Twee van de domeinen in het bedrijfsleven waar de overheid de toezichtslast wil verminderen zijn de chemiesector en de afvalsector. Zowel bij de grote en middelgrote bedrijven¹ als bij het midden- en kleinbedrijf² is onderzoek uitgevoerd naar de beleving van de administratieve last door het toezicht. Uit de eerste rapportage is gebleken dat de door grote en middelgrote bedrijven ervaren 'last' van het toezicht niet zo zeer een kwantitatief probleem is (de overheid inspecteert niet te vaak), maar vooral een kwalitatief probleem: de overheidsinspecties worden als onnodig belastend ervaren omdat de kwaliteit van voorbereiding, uitvoering en terugkoppeling beter kan. Voor de kleinere bedrijven geldt dat zij het overheidstoezicht niet als majeur probleem ervaren.

Een belangrijk uitgangspunt van het kabinetsbeleid voor overheidstoezicht is vertrouwen als basishouding. Het Programma Vernieuwing Toezicht beoogt bij te dragen aan een 'kleinere en betere Rijksdienst' door o.a. inspecties effectiever te doen zijn, toezicht meer te richten op de voornaamste risico's en een cultuuromslag te realiseren naar een basishouding van vertrouwen. De ambitie is hierbij dat bedrijven ervaren dat bij de inspecties optimaal gebruik wordt gemaakt van zorgsystemen en gegevens van bedrijven. Als die goed zijn, kan de inspectie zich grotendeels beperken tot systeemtoezicht. Mits juist toegepast in de situaties die zich hiervoor lenen, worden aan systeemtoezicht enkele belangrijke voordelen toegedicht:

- Systeemtoezicht kan toezicht effectiever maken:
 - Van systeemtoezicht gaat een betere leerstimulus uit doordat het gericht is op de interne bedrijfsprocessen en managementsystemen;
 - Door het toepassen van systeemtoezicht wordt een bedrijf erkend in zijn inspanningen om naleving te borgen;
 - Systeemtoezicht kan zorgen voor een voorspellende waarde doordat het zich richt op de oorzaken van ongevallen en schade aan gezondheid en milieu;
 - Door systeemtoezicht verkrijgt de toezichthouder een bredere blik op het bedrijf.
- Systeemtoezicht kan toezicht efficiënter maken. Dit komt vooral doordat bij systeemtoezicht gebruik wordt gemaakt van het zelfcontrolerend vermogen van bedrijven zelf.

De keerzijde is dat als systeemtoezicht niet juist wordt toegepast of wordt toegepast in situaties die niet geschikt zijn, er belangrijke nadelen kunnen optreden zoals teveel vrijheid voor bedrijven die de verantwoordelijkheid niet aankunnen.

¹ Meting toezichtslasten in het domein Chemie, Onderzoek naar de administratieve en ervaren lasten van toezicht binnen het domein Chemie, SIRA Consulting 2007

² Nulmeting kleine chemiebedrijven, KPMG 2008

1.2 Doel

Het doel van dit rapport is om eenduidigheid te brengen in de terminologie en het begrippenkader rond het thema systeemtoezicht en een stand van zaken te geven van wat nu bekend is over de afwegingen en instrumenten. Het gaat hierbij met name om de volgende vragen:

- Wat is systeemtoezicht?
- Hoe kunnen we de belangrijkste begrippen definiëren?
- In welke situaties heeft systeemtoezicht zin?
- Hoe kan systeemtoezicht worden uitgevoerd?
- Welke verdere ontwikkelingen en vervolgacties zijn nodig?

Dit rapport geeft de stand van zaken weer per medio 2009.

1.3 Leeswijzer

Achtereenvolgens komen in dit afwegingskader de volgende onderwerpen aan de orde.

- Wat is systeemtoezicht? (hoofdstuk 2);
- Vertrouwen (hoofdstuk 3);
- Effectiviteit (hoofdstuk 4);
- Systeemtoezicht in de praktijk (hoofdstuk 5);
- Systeemgericht toezicht; wanneer is het zinvol? (hoofdstuk 6);
- Verdere ontwikkelingen (hoofdstuk 7).

Dit rapport heeft betrekking op het toezicht op de grote bedrijven in het kader van de Wet milieubeheer en gerelateerde gebieden. Bij de opstelling van dit afwegingskader is gebruik gemaakt van het concept afwegingskader dat is opgesteld in opdracht van de VROM Inspectie door Gemini, Tebodin en Logica van 2008 en de concept notitie van MWH van december 2008. Next Step Management heeft de rapportage in opdracht van de VROM-Inspectie samengesteld.

2 Wat is systeemtoezicht?

2.1 Historie

Enige tijd geleden ontstond het idee dat alleen het beoordelen van de output een te beperkt handhavingsinstrument is om zicht te krijgen op de borging van de naleving van wet- en regelgeving door complexe onder toezicht staande organisaties (OTS), en dat het wellicht betere resultaten zou opleveren als de toezichthouder zich zou bemoeien met de achterliggende processen en strategieën van een OTS.

Eind jaren tachtig werden in een aantal industriële branches managementsystemen in gebruik genomen ten behoeve van kwaliteitszorg of milieuzorg. Voor deze systemen werden ISO normen ontwikkeld (resp. 9000 series en 14001).

In de jaren negentig werd de vergunning op hoofdlijnen ontwikkeld, waarbij de bovengenoemde systemen veelal als basis werden gebruikt. De ervaringen hiermee waren niet onverdeeld positief. Men vond onder andere dat er te weinig handvatten waren bij discussies over wat nu wel en niet toegestaan was.

Het vertrouwen in de waarde van certificering voor regelnaleving kreeg een belangrijke knauw door de TCR-affaire. Het bedrijf Tank Cleaning Rotterdam werd binnengevallen naar aanleiding van diverse ernstige milieuovertredingen en er volgden hoge veroordelingen tot zes jaar gevangenisstraf voor de daders. TCR had een week voor de inval certificaten ontvangen voor haar milieu- en kwaliteitszorgsysteem.

Vanaf de jaren tachtig is er een enorme ontwikkeling van allerlei keurmerken en certificaten geweest. De eisen die aan bedrijven worden gesteld om deze keurmerken te verkrijgen zijn lang niet altijd relevant in termen van compliance management. Soms zijn deze keurmerken meer opgezet vanuit commerciële overwegingen, bijvoorbeeld als toetredingsdrempel ter bescherming van de positie van de grote spelers in een sector. Het spreekt voor zich dat deze keurmerken niet (automatisch) geschikt zijn als basis voor systeemtoezicht.

Mythe # 1 Certificaten stellen niets voor, dus systeemtoezicht ook niet
Een certificaat heeft zoveel waarde als de eisen die aan de certificaathouder worden gesteld en de kwaliteit van de audit. Bij systeemtoezicht worden de systeemeisen (mede) door de overheid zelf bepaald en wordt de audit doorgaans ook door de overheid zelf uitgevoerd. De eisen die hierbij aan de bedrijven worden gesteld, zijn streng en gebaseerd op wat bedrijven en toezichthouders belangrijk vinden bij de borging van regelnaleving. De audits worden uitgevoerd door mensen met auditvaardigheden en kennis van de inhoud, zodat zij ook bij een audit de diepte in kunnen gaan.

In de Verenigde Staten heeft men al vele jaren ervaring met systeemtoezicht en zijn de voorwaarden voor een deel in wetgeving opgenomen (zie bijlage 2 en 3).

Na de vuurwerkramp in Enschede en de cafébrand in Volendam ontstond veel aandacht voor een verbetering van het toezicht in algemene zin. Direct na deze rampen heerste in kringen van toezichthouders sterk de neiging om bedrijven niet (zonder meer) te vertrouwen en een beleid van zero-tolerance te voeren.

In 2001 werd de eerste kaderstellende visie op toezicht gepresenteerd, die in 2005 een 'update' kreeg. Er kwam een grote beweging op gang om de handhaving te professionaliseren en meer planmatig aan te pakken. Het bedrijfsleven roerde zich met klachten over het toezicht. Het toezicht zou niet voldoende professioneel zijn en tot te veel last bij bedrijven leiden. Als gevolg van de motie Aptroot in 2006 werd een aantal implementatieacties geformuleerd die werden gebundeld in het programma Eenduidig Toezicht. De doelstelling van dit programma was om te komen tot een reductie van de toezichtslast voor bedrijven van 25%. Om dit te bereiken zouden de inspecties en andere toezichthouders beter moeten gaan samenwerken.

Begin 2008 presenteerde de minister van Binnenlandse Zaken het programma Vernieuwing Toezicht. Met dit programma wordt een effectief én efficiënt toezicht nagestreefd, waarin bedrijven minder last ondervinden van het toezicht en waarbij bedrijven met goede managementsystemen en correct naleefgedrag kunnen rekenen op meer vertrouwen van de overheid en een verminderde toezichtslast. Voor bedrijven die aan deze voorwaarden voldoen kan de toezichthouder besluiten het toezicht te concentreren op de controle van het managementsysteem en in mindere mate op de feitelijke naleving van de regels. Hierdoor ontstaan kansen op een betere borging van gewenste situaties aan de ene kant en bij een vastgestelde structureel goede aanpak door het bedrijf een vermindering van de toezichtslast. Bedrijven met een hoog risico op regelovertreding blijven onderworpen aan het intensieve klassieke toezicht. Klassiek toezicht richt zich op de output en betreft de controle of aan de wettelijke eisen (waaronder vergunningsvoorschriften) is voldaan, dus of maatregelen zijn genomen en of normen niet worden overschreden. Het is een beleidskeuze die onder meer zou moeten afhangen van de vraag waar het grootste effect verwacht wordt. De meest logische benadering lijkt te zijn systeemgericht toezicht bij bedrijven met een compliance management systeem en klassiek toezicht bij bedrijven waar dit niet zo is.

In recente beleidsstukken over toezicht wordt gesproken over de wenselijkheid van systeemtoezicht, met andere woorden een soort van toezicht gebaseerd op het zelfcontrolerend vermogen van een bepaalde beroepsgroep of sector.

De Kaderstellende Visie op Toezicht (2005) zegt hierover:

'Burgers en bedrijven zijn zelf verantwoordelijk voor het naleven van de regels' en 'toezicht sluit zoveel mogelijk aan op andere vormen van controle en verantwoording. Het maakt gebruik van deze andere 'checks and balances'.

De nota 'Vernieuwing Rijksdienst' (2007):

'... En tenslotte kan tevens het uitgaan van vertrouwen in plaats van wantrouwen een rol spelen, zeker in combinatie met het meer vertrouwen op het zelfregulerend vermogen van beroepsgroepen of branches. Als een beroepsgroep, een branche of een individueel bedrijf, een goed kwaliteitssysteem heeft en is gecertificeerd, is de behoefte om nog intensieve inspecties uit te voeren minder. Dat geldt ook als er binnen de beroepsgroep of branche zelf voorzieningen zijn getroffen op het vlak van kwaliteit en handhaving.'

In het programma 'Vernieuwing Toezicht' (2008) wordt het navolgende beeld geschetst van Toezicht anno 2010:

*‘De ambitie is dat bedrijven, instellingen en professionals het toezicht anno 2010 als volgt zullen ervaren (het perspectief van de ondertoezichtgestelde):
De manier van controleren is ook veranderd. De inspecties maken optimaal gebruik van onze kwaliteitssystemen en onze gegevens. Als die goed zijn, kan de inspectie zich grotendeels beperken tot systeemtoezicht. De inspectiediensten vanuit het rijk, de gemeente enz. werken onderling goed samen, zodat we door minder instanties benaderd worden en geen vragen meer dubbel hoeven te beantwoorden. De inspecteurs zijn deskundig en hebben oog voor onze bedrijfsprocessen. Ze zijn duidelijk over hun taak en over de inspectieresultaten. De regels zijn eenvoudiger geworden en het zijn er minder. Het kost geen onevenredige moeite om je eraan te houden. Inspecteurs maken duidelijk welke regels voor ons gelden, hoe die in elkaar zitten en hoe je ermee moet omgaan. Wie met opzet de regels overtreedt, wordt snel en streng aangepakt.’*

2.2 Afbakening, begrippen en werkdefinities

2.2.1 Werkdefinities

In dit rapport worden de volgende werkdefinities gehanteerd.

Compliance

Het naleven van wettelijke eisen inclusief vergunningsvoorschriften.

Compliance management systeem

Een intern beheersingssysteem dat een organisatie onder eigen verantwoordelijkheid opzet ter voorkoming van onrechtmatig handelen binnen die organisatie.

Metatoezicht

Synoniem voor Systeemtoezicht (zie onder Systeemtoezicht).

Systeemgericht toezicht

De integrale combinatie van systeemtoezicht en toezicht op output.

Systeemtoezicht

Toezicht op systemen, processen en methoden die gericht zijn op het borgen van de naleving van wettelijke eisen en niet op de feitelijke naleving zelf.

Toezicht

Alle handelingen uitgevoerd door een krachtens de wet hiertoe bevoegde instantie die gericht zijn op het inwinnen van informatie over de naleving van wettelijke eisen door een derde, het vormen van een oordeel of het publiek belang voldoende is bereikt en het eventueel interveniëren.

Toezicht op output

Toezicht op de naleving van wettelijke eisen.

2.2.2 Systeemtoezicht nader bekeken

Mythe # 2 Systeemtoezicht is alleen maar papieren controle
 Bij systeemtoezicht worden altijd controles op procedures, instructies, interne controlemaatregelen gecombineerd met toezicht op de output. Er wordt dus zowel naar het managementsysteem gekeken als naar de uitkomsten zoals bijvoorbeeld of er veilig wordt gewerkt op de werkvloer, of de emissies voldoen aan de norm etc.

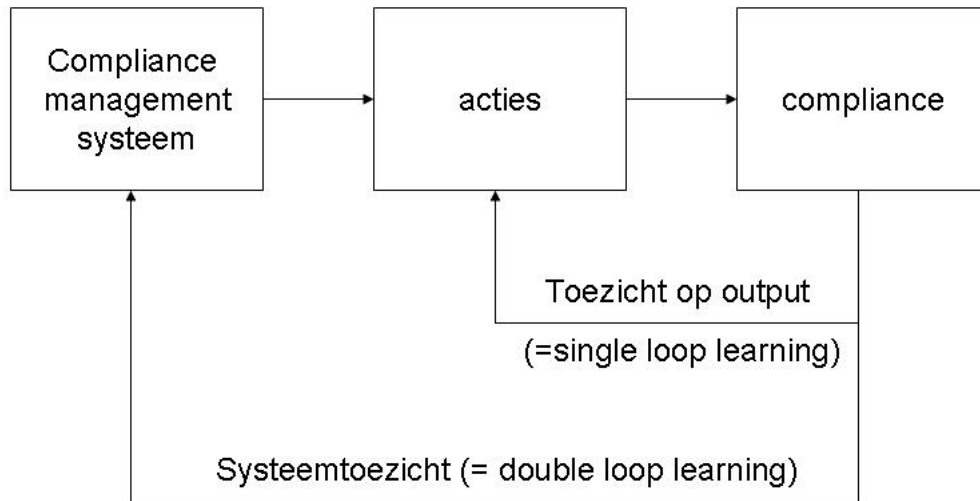
Voor een goed begrip van wat systeemtoezicht is, is het van belang onderscheid te maken tussen toezicht op output en systeemtoezicht. Het onderscheid tussen systeemtoezicht (ook wel metatoezicht genoemd) en toezicht op output kan worden toegelicht aan de hand van een model voor leren in organisatie³.

Bij toezicht op output controleert de toezichthouder of aan de vergunningsvoorschriften en wettelijke eisen wordt voldaan. Er wordt dus gekeken of de emissies de gestelde normen niet overschrijden, of bepaalde voorzieningen zijn gerealiseerd, etc. Dit toezicht is dus gericht op de beoordeling van de output en lokt alleen acties van het bedrijf uit om de overtreding ongedaan te maken. Het lerend effect hiervan is beperkt en heeft een 'single loop' karakter. Bijvoorbeeld een bedrijf dat geuremissienormen overtreedt kan besluiten een geurfilter te plaatsen. De vraag hoe het zover heeft kunnen komen dat de emissie optrad en de wijze waarop het interne toezicht werkt worden niet ter discussie gesteld.

Systeemtoezicht is een vorm van double loop learning omdat het gericht is op de onderliggende processen, strategieën en procedures die compliance als doel hebben. Systeemtoezicht grijpt daarmee in op de structurele oorzaken van naleving en kan daarom een structurele verbetering van de naleving bewerkstelligen. De gecombineerde inzet van systeemtoezicht en toezicht op output noemen we systeemgericht toezicht. Figuur 2-1 illustreert dit.

³ Argyrus, C. & Schön, D.A., 1978, Organizational Learning: A Theory of Action Perspective. Phillipines: Addison-Wesley Publishing Company Inc.

Figuur 2-1 Model voor systeemgericht toezicht



In deze notitie hanteren we de definitie van systeemtoezicht die in 2.2.1 is opgenomen.

Systeemtoezicht heeft zin als bij de OTS processen, strategieën en procedures in gebruik zijn of kunnen worden ontwikkeld die gericht zijn op de naleving van wettelijke eisen. Deze processen, strategieën en procedures vormen dan het systeem dat als subject van het systeemtoezicht fungeert. Wat kunnen we zeggen over deze processen, strategieën en procedures? Wanneer vormen deze een effectief compliance management systeem, met andere woorden, wanneer borgen deze de naleving afdoende?

Het is van belang op te merken dat toezicht nooit uitsluitend uit systeemtoezicht alleen kan bestaan. Ook al is een bedrijf nog zo ver met het borgen van naleving, er blijft altijd een noodzaak om steekproefsgewijze outputcontroles uit te voeren. Bij systeemgericht toezicht kunnen de outputcontroles worden gebruikt om de werking van het systeem te verifiëren. Zo kan de toezichthouder, om een goed beeld te krijgen van de mate van borging, vanuit geconstateerde tekortkomingen in het systeem gericht outputcontroles doen (top down) en vanuit outputcontroles kijken naar de werking van het systeem (bottom up).

2.2.3 Vermogen tot zelfcontrole

Veel grote bedrijven in Nederland hebben de afgelopen jaren geïnvesteerd in het ontwikkelen en implementeren van managementsystemen. Er zijn managementsystemen voor een groot aantal aspecten zoals kwaliteit, milieu, veiligheid en energie. Klanten, aandeelhouders, omwonenden, het moederconcern, de overheid: allemaal verwachten ze van het bedrijf dat het de risico's kent en onder controle heeft. De overheid dekt risico's af door voor bedrijven wetten en regels op te stellen en te controleren of deze worden nageleefd.

Managementsystemen van bedrijven zijn doorgaans niet primair gericht op het borgen en het naleven van wettelijke eisen, ook wel compliance management genoemd. Het systeem is er in de eerste plaats voor het management: om de bedrijfsvoering te optimaliseren. Er is bij grote bedrijven wel een groot potentieel om de naleving van wettelijke eisen te borgen in de eigen organisatie op basis van kennis van en ervaring met managementsystemen. Er zijn vaak managers voor kwaliteit, gezondheid,

veiligheid en milieu (KAM of QHSE) die waken over een veilige en milieuvriendelijke bedrijfsvoering. Echter, doordat de bestaande normen voor managementsystemen niet specifiek zijn gericht op het borgen van het naleven van wettelijke eisen, zijn er grote verschillen in nalevingsgedrag bij bedrijven die werken met gecertificeerde managementsystemen. Hoewel er in de ISO 14001 norm eisen zijn opgenomen voor regelnaleving, zijn er ook significante verschillen in nalevingsgedrag bij ISO 14001 certificaathouders.

Er bestaat (nog) geen formele norm voor het bepalen van de effectiviteit van compliance management. Wel zijn er criteria die kunnen worden gebruikt om tot een dergelijke norm te komen. Ook is er een concrete compliance competence auditmethode waarmee, onafhankelijk van het wettelijk domein, kan worden gemeten hoe effectief het compliance management systeem is (zie paragraaf 6.2). Dit is mogelijk omdat met deze audit niet de naleving van regels wordt gemeten, maar de mate van borging van naleving.

Mythe # 3 Systeemtoezicht gaat uit van blind vertrouwen
 Weliswaar is vertrouwen uitgangspunt bij systeemtoezicht, maar dit vertrouwen is gebaseerd op een grondige analyse van de werking van het compliance management en de cultuur van het bedrijf.
 Bedrijven die voldoen aan zowel de harde systeemeisen als de cultuuraspecten, verdienen vertrouwen.

De meerwaarde van systeemtoezicht ligt vooral in het benutten van het zelfcontrolerend vermogen van onder toezicht staande organisaties waardoor de naleving verbetert en de toezichthouder een beter zicht heeft op de risico's. Dit sluit goed aan bij de onderzoeken naar de toezichtslast in de sectoren chemie en afval. Hierbij werd geconcludeerd dat niet zo zeer de hoeveelheid toezicht voor bedrijven een probleem vormt, als wel de kwaliteit van het toezicht.

Nadat systeemtoezicht in een domein is opgezet zou het ook tot tijdwinst kunnen leiden als de toezichthoudende instantie kan besparen op o.a. outputcontroles die het bedrijf zelf al uitvoert. Het is ook mogelijk dat systeemtoezicht voor bedrijf en toezichthoudende instantie juist meer tijd vergt dan traditioneel toezicht. Deze extra inspanning is alleen zinvol als een betere naleving of risicobeheersing het gevolg is. We kunnen er van uit gaan dat systeemtoezicht in de aanlooperperiode meer tijd kost dan traditioneel toezicht.

2.2.4 Dimensies van systeemtoezicht

Uitgaande van de drie verschillende activiteiten waaruit toezicht bestaat (informatie verzamelen, oordelen, interveniëren) kunnen we in deze activiteiten onderscheid maken tussen toezicht op output en systeemtoezicht. Bij toezicht op output staat het onderdeel informatie verzamelen in het teken van informatie die relevant is t.o.v. de wettelijke norm. De toezichthouder verzamelt deze informatie op verschillende manieren en vormt dan een oordeel over de vraag of aan de wettelijke norm is voldaan. Bij overtreding kan deze besluiten te interveniëren door middel van een bestuursrechtelijke of strafrechtelijke sanctie.

Bij systeemtoezicht wordt geen informatie verzameld over de output, maar van het systeem dat de OTS gebruikt om ervoor te zorgen dat de wettelijke normen worden nageleefd en of eventuele afwijkingen goed worden afgehandeld. De hierbij verzamelde informatie wordt niet getoetst aan een wettelijke eis maar aan systeemeisen. In een aantal uitzonderingsgevallen zijn systeemeisen in de wettelijke eisen zijn opgenomen, zoals bv. in de luchtvaartindustrie en in het Brzo.

Bij systeemtoezicht wordt de interventie mede afhankelijk gemaakt van het compliance management niveau van de OTS en de wijze waarop de OTS op de overtreding reageert (ontdekken, rapporteren, herstel- en verbeteracties).

In onderstaand schema zijn de verschillende activiteiten weergegeven (niet uitputtend).

Onderdeel toezicht	Toezicht op output	Systeemtoezicht
Informatie verzamelen	meten, bemonsteren, fysiek inspecteren, administratie controleren	auditeren, beoordelen afhandeling afwijkingen, overleg OTS over accenten en aandachtspunten
Oordeel vormen	toets aan de wettelijke norm, onderscheid kernvoorschriften en aanvullende voorschriften, registreren oordeel in verslag	toetsen normen voor effectief compliance management, aan afsprakendocument of convenant, aan wettelijke systeemeisen, opstellen auditrapport
Interveniëren	bestuursrechtelijk of strafrechtelijk	Interventies op systeemniveau Differentiëren sancties bij overtreding afhankelijk van acties bedrijf om te voorkomen dat de overtreding zou plaatsvinden (CM) en herstelacties

3 Vertrouwen

3.1 Inleiding

Een belangrijk element bij systeemtoezicht is het begrip vertrouwen. Van Dale omschrijft vertrouwen als *geloof in iemands betrouwbaarheid*. Vertrouwen wordt, naast normen en waarden, burgerzin en sociale netwerken, gerekend tot het sociaal kapitaal in de maatschappij en is daarmee mede bepalend voor de manier waarop mensen met elkaar omgaan⁴. In een samenleving waar het vertrouwen hoog is, worden gezag en wetgeving doorgaans gerespecteerd, houdt men zich aan regels en afspraken en kan veelal worden volstaan met informele afspraken. In een samenleving waar het vertrouwen laag is wantrouwen burgers, bedrijven en overheid elkaar en worden veel regels en wetten gemaakt waarop moet worden toegezien en gecontroleerd. Als wetten en regels worden aangevuld met sociaal kapitaal zoals vertrouwen, kan substantieel worden bespaard op transactiekosten⁵ omdat dan juridische rompslomp en het intensief controleren achterwege kunnen blijven. Bij het ontbreken van vertrouwen zullen veel meer controlemechanismen noodzakelijk zijn en dat maakt het duurder.

Vertrouwen in onder toezicht staande organisaties (OTS) is niet vanzelfsprekend. Ontwikkelingen in o.a. de financiële sector in 2008 hebben duidelijk gemaakt dat er risico's verbonden zijn om OTS-en zonder meer vanuit vertrouwen ruimte te geven zonder dat hiervoor een duidelijke rechtvaardiging bestaat.

Vertrouwen als geloof in iemands betrouwbaarheid kan worden gerechtvaardigd door middel van een aantal rationele elementen. Naarmate meer sprake is van competenties (bekwaamheden), openheid over resultaten en afwijkingen, nakomen van afspraken en zelfreflectie neemt het vertrouwen tussen twee partijen toe⁶. In een relatie tussen twee partijen, bijvoorbeeld die tussen toezichthouder en OTS, werkt dit twee kanten op. Beide partijen kunnen door middel van hun gedrag bijdragen aan een groeiend vertrouwen.

Voor systeemtoezicht is het noodzakelijk dat de toezichthouder een gerechtvaardigd vertrouwen heeft in de effectiviteit van het systeem van de OTS. Andersom is het voor systeemtoezicht noodzakelijk dat de OTS voldoende vertrouwen heeft in de toezichthouder, immers van de OTS wordt gevraagd om (gevoelige) informatie te delen met de toezichthouder.

Een OTS kan ervoor zorgen dat aan dit basisniveau van vertrouwen wordt voldaan door zijn systeem op orde te brengen. Dit houdt in dat de OTS zijn systeem zo ontwerpt en implementeert dat het zorgt voor normconforme output.

In sommige sectoren zijn de eisen voor het systeem in wet- en regelgeving vastgelegd. In sectoren waar dit niet het geval is, kan de toezichthouder - al dan niet in samenspraak met de OTS of doelgroep - aangeven welke eisen gelden voor het systeem van de OTS om voor systeemtoezicht in aanmerking te komen.

3.2 Vertrouwen operationaliseren

Het ligt voor de hand dat deze eisen betrekking hebben op de vier elementen die leiden tot meer vertrouwen:

- competenties (bekwaamheden);
- openheid over resultaten afwijkingen;
- nakomen van afspraken;

⁴ Prast H.M., Mosch R.H.J. en Van Raaij W.F., Vertrouwen, cement van de samenleving en aanjager van de economie, De Nederlandsche Bank/Universiteit van Tilburg, 2005

⁵ Fukuyama F., Welvaart, Contact, 1995

⁶ Benninga, R., Nyenrode Alumni Magazine, 2007

- zelf-reflectie.

Op organisatieniveau kunnen deze vier elementen worden geadresseerd in een managementsysteem en worden vertaald naar systeemeisen (zie verder).

Bij systeemtoezicht wordt het toezicht gericht op het systeem van de OTS. Hierbij is dus niet meer de output leidend, maar wordt informatie over het systeem verzameld en geanalyseerd en wordt het systeem beoordeeld.

Om dit proces goed te kunnen uitvoeren is een basisniveau van vertrouwen tussen toezichthouder en OTS nodig, immers de OTS moet zijn kwetsbaarheden openbaar maken en de toezichthouder moet op een meer fundamenteel niveau gaan oordelen.

Een goede afstemming van de verhouding systeemtoezicht - outputcontrole (producttoezicht) op het niveau van de OTS leidt dus niet alleen tot een effectief toezicht op de situatie 'as it is', maar draagt ook bij aan een groeiend vertrouwen tussen toezichthouder en OTS. Vertrouwen is dus zowel randvoorwaarde als resultaat.

Zoals toegelicht is de politieke opdracht om toezicht te baseren op vertrouwen. Tot voor kort was het toezicht op de naleving van milieuregels in grote mate gebaseerd op wantrouwen. Bewijzen hiervoor zijn onder andere terug te vinden in de grote hoeveelheid milieuregels en de houding van een substantieel deel van de handhavers en toezichthouder ('vertrouwen is goed, maar controle is beter'). De werkwijze in het strafrecht is doorgaans gericht op het rondmaken van een zaak, ervan uitgaande dat de verdachte schuldig is.

Overmatige controle en regelgeving verminderen het vertrouwen tussen overheid en bedrijfsleven direct.

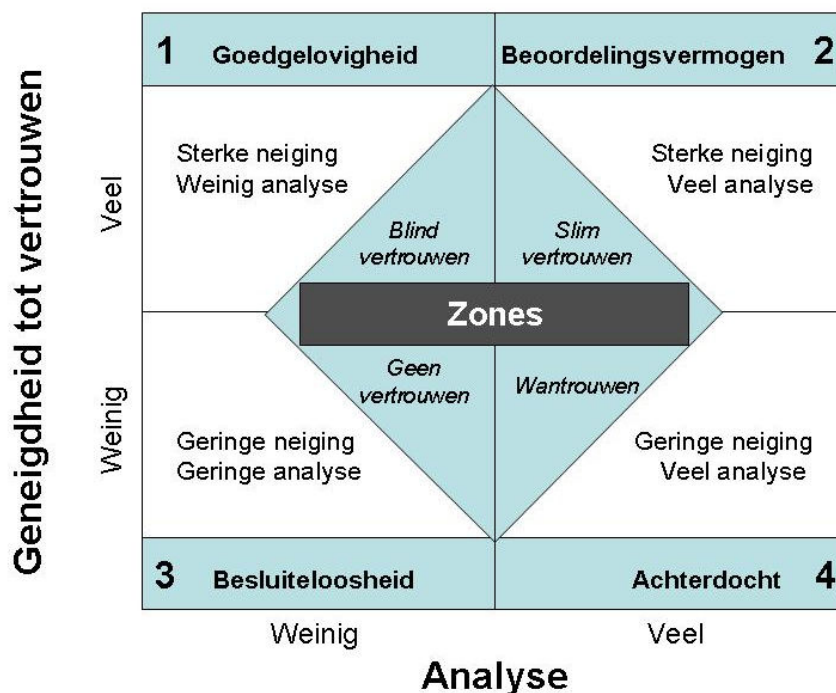
Het is niet voor niets dat toezicht moet worden gebaseerd op vertrouwen. Mensen die vanuit achterdocht werken denken vaak dat dit een effectieve manier is om risico's te beperken. Het tegendeel is waar. Achterdocht leidt tot hoge kosten door al die regels en controles en kan de aandacht afleiden van de echte risico's. Bovendien sluit de achterdochtige zich af van samenwerking, kennisuitwisseling en het perspectief van anderen⁷.

Aan de andere kant is uitgaan van vertrouwen zonder dat daar een goede basis voor bestaat, ook niet aan te raden. Net zo goed als we een houding van niet gerechtvaardigd wantrouwen willen vermijden, willen we ook een situatie van niet gerechtvaardigd vertrouwen voorkomen. Teveel vrijheid voor bedrijven die niet hun verantwoordelijkheid nemen, kan grote risico's opleveren.

Stephen Covey heeft een matrix ontwikkeld waarin geneigdheid tot vertrouwen en analyse tegen elkaar zijn uitgezet (zie figuur 3-1).

⁷ Stephen M.R. Covey, De Snelheid van vertrouwen, Business Contact, 2006

Figuur 3-1 Matrix Slim Vertrouwen (Covey, 2006)



Geneigdheid tot vertrouwen is vooral een gevoelszaak. Het gaat hier vooral om de bereidheid te geloven dat de andere partij betrouwbaar is en de wil vertrouwen te schenken.

Analytisch vermogen is vooral een rationele kwestie. Het is het vermogen om gevolgen en mogelijkheden te analyseren, evalueren, beredeneren en overwegen en met logische beslissingen en oplossingen te komen.

Bij systeemtoezicht is het van belang dat de partijen zich vinden in het 2^e kwadrant waarin op basis van een goede analyse én geneigdheid vertrouwen ontstaat.

Dit impliceert dat partijen die nu wel geneigd zijn om te vertrouwen, maar nog geen analyse toepassen, het vertrouwen gaan onderbouwen. In de sectoren chemie en afval is geëxperimenteerd met een auditmethode compliance competence waarin de vier elementen van vertrouwen van hoofdstuk 3 zijn omgezet in systeemeisen. De Inspectie Verkeer en Waterstraat heeft recent een afwegingskader voor systeemtoezicht vastgesteld waarin eenzelfde vertaalslag is gemaakt van vertrouwen naar systeemeisen⁸ (tabel 3-1).

Tabel 3-1 Van vertrouwen naar systeemeisen

Element van vertrouwen	Systeemeisen
Competenties	- actuele kennis wettelijke eisen - risico analyse methodiek ontwikkeld en toegepast - kennis en ervaring sleutelfiguren
Openheid over resultaat afwijkingen	- rapportage aan overheid en omgeving van afwijkingen, overtredingen en werking systeem
Nakomen van afspraken	- borging beheersing risicovolle aspecten - pro-actieve houding t.a.v. gestelde eisen - actieve gedragsbeïnvloeding op de werkvloer vanuit management - basisniveau managementsysteem

⁸ Afwegingskader Systeemtoezicht, IVW TCO, 27 november 2008

Zelfreflectie	- meten van de eigen naleving - identificeren en onderzoeken van afwijkingen - verbetermaatregelen - interne controle en functiescheiding (compliance functie) - analyse fraudegevoelige functies
---------------	---

De compliance competence audit is algemeen toepasbaar en is gericht op zowel harde systeemelementen (middelen, competenties e.d.) als cultuur (reactief – proactief). Met de compliance competence audit kan worden gemeten in hoeverre de naleving van wettelijke eisen door de OTS is geborgd in de organisatie van de OTS⁹. Dit meetinstrument is specifiek gericht op compliance management en voorziet in een lijst met 42 vragen en 56 bijbehorende verificatie items zodat het dienst kan doen als middel voor een externe verificatie audit (zie bijlage 4). Deze systeemeisen zijn ook in de vorm van een self assessment tool uitgebracht¹⁰. Partijen in kwadrant 1 van figuur 3-1 kunnen op basis van een goede onderbouwing door middel van deze instrumenten opschuiven naar kwadrant 2.

Voor diegenen die uitgaan van wantrouwen (kwadrant 3 en 4) ligt de zaak anders. Zij gaan niet mee in blind vertrouwen. Niet geheel onterecht voeren de wantrouwers aan dat certificaten niets voorstellen. Bedrijven met certificaten of keurmerken zijn niet per definitie goede nalevers.

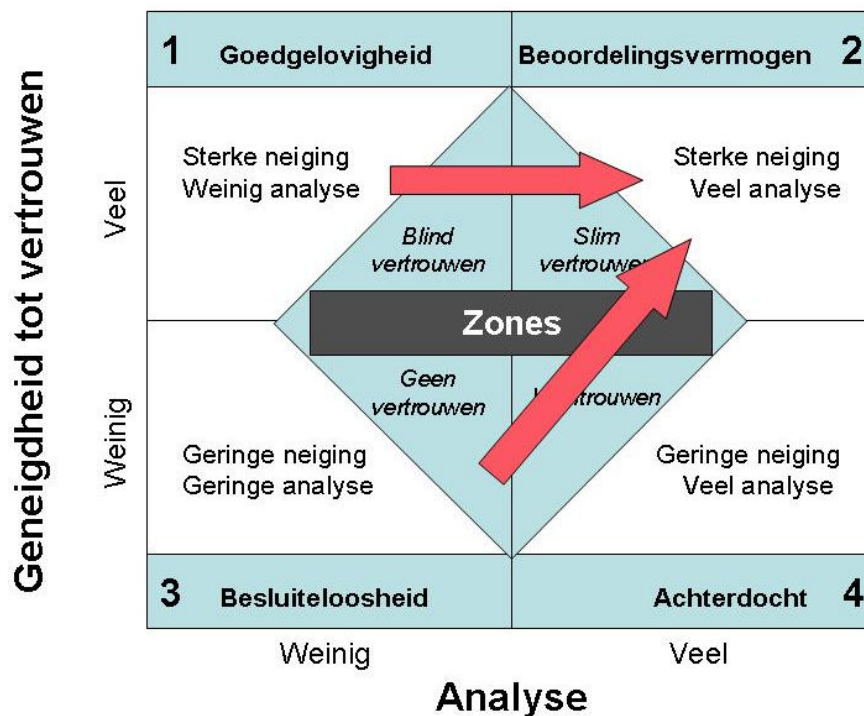
De neiging tot meer vertrouwen kan worden gevoed door het vertrouwen alleen aan een OTS te geven als aan het systeem van de OTS relevante eisen worden gesteld, die bij toepassing een goed oordeel mogelijk maken over de mate waarin de OTS de naleving van wettelijke eisen heeft geborgd.

Wat van de betrokken partijen mag worden gevraagd is de proactiviteit om aan te geven aan welke eisen een OTS moet voldoen, wil het in de ogen van de toezichthouder verantwoord handelen. Dit betekent niet dat we hiermee de garantie hebben dat nooit meer een overtreding zal worden begaan, maar wel dat we het eens zijn over de vraag wat een bedrijf redelijkerwijs kan doen om te borgen dat het goed gaat. In de VS heeft de formulering van de organizational guidelines en criteria voor compliance and ethics programs een aanzienlijke verbetering gegeven van de structurele borging van de regelnaleving (zie bijlage 2 en 3). Figuur 3-2 geeft deze beweging schematisch aan.

⁹ Bovenkerk, C. Verweij, M., de Bree, M.A. Systeemtoezicht: het operationaliseren van vertrouwen, paper LOM congres, juli 2008

¹⁰ <http://www.inspectieloket.nl/chemie/actueel/nieuws/testofuwbedrijfzelfcontrolerendis.aspx>

Figuur 3-2 Naar meer gerechtvaardigd vertrouwen



Een speciaal punt op het vlak van vertrouwen dat zich afspeelt in kwadrant 1 is het risico dat de OTS het voldoen aan systeemeisen misbruikt als *window dressing*. Dat wil zeggen de OTS voldoet aan de systeemeisen om hiermee in een soepeler toezichtsregime terecht te komen zodat er ruimte komt om de wettelijke eisen te overtreden en onder sancties uit te komen.

Om window dressing te voorkomen is het van groot belang dat de OTS bij systeemtoezicht op een strikte manier wordt getoetst tegen relevante eisen. Eerder zagen we dat keurmerken of certificaten niet automatisch iets zeggen over de mate waarin de OTS de naleving van wettelijke eisen heeft geborgd. De in de pilots ontwikkelde systematiek van compliance competence audit en op het CM niveau afgestemd toezicht kan wellicht een oplossing bieden voor het probleem van window dressing.

Mythe # 4 Met systeemtoezicht krijgen bedrijven te veel vrijheid
 Alleen bedrijven die hun zaakjes echt goed voor elkaar hebben,
 komen voor systeemtoezicht in aanmerking. Dit betekent niet dat
 er nooit iets mis zal gaan, maar wel dat deze bedrijven alles wat
 redelijkerwijs mogelijk is doen om ervoor te zorgen dat zij zich aan
 de wettelijke eisen houden en de risico's maximaal beheersen.
 Bedrijven die geen effectief compliance management systeem
 hebben komen niet voor systeemtoezicht in aanmerking.

4 Effectiviteit van systeemgericht toezicht

Het meten van het effect van toezicht is niet eenvoudig. Dit komt vooral doordat het erg lastig is om een directe relatie te leggen tussen de activiteiten van toezichthouders en het gedrag van de vertegenwoordigers van een OTS. Bij de vraag of systeemgericht toezicht effectief is, moet eerst de vraag worden beantwoord welke doel men met systeemgericht toezicht beoogt.

Als het doel is 'doen naleven', dan kan dit doel worden bereikt via verschillende subdoelen, waarvan het realiseren ervan bijdraagt aan het hogere doel *doen naleven*. We beschouwen vier subdoelen:

1. Goede informatiepositie toezichthouder
2. Realiseren van risico gestuurd toezicht
3. OTS-en stimuleren tot leren: betere naleving en betere beheersing van risico's op ongevallen, schade aan gezondheid en milieuschade
4. Efficiënt toezicht (lage lasten voor OTS en toezichthouder)

In dit hoofdstuk gaan wij na in hoeverre systeemgericht toezicht een middel kan zijn voor realisatie van bovengenoemde subdoelen. Wij gaan hierbij uit van de vorm van systeemgericht toezicht zoals deze in dit rapport is beschreven.

4.1 Informatiepositie toezichthouder

Toezicht begint met het verzamelen van informatie. Bij systeemgericht toezicht krijgt de toezichthouder in korte tijd gerichte informatie over de maatregelen die een OTS heeft genomen om ervoor te zorgen dat regels worden nageleefd en risico's worden beheerst.

Vanuit tekortkomingen in het systeem kan vervolgens gericht worden gezocht naar tekortkomingen in de output.

Andersom kan men bij geconstateerde tekortkomingen in de output via systeemtoezicht achterhalen wat de achterliggende oorzaak is van de tekortkoming.

VWA Voedselveiligheid gebruikt de informatie over het systeem van de OTS voor het doen van gerichte steekproeven op de output. Hierdoor kunnen veel gerichter outputcontroles worden gedaan. De IVW Luchtvaartinspectie geeft aan dat systeemtoezicht een voorspellende waarde heeft, met andere woorden men ziet eventuele problemen aankomen. Dit komt doordat systeemtoezicht informatie oplevert over de vraag waar risico's op ongelukken of fouten onacceptabel hoog worden nog voordat deze zich manifesteren in de vorm van daadwerkelijke ongelukken.

Bij toezicht op output wordt van de talloze - aan regels gebonden - aspecten en gedragingen van de werknemers van de OTS slechts een miniem deel waargenomen. Als uitsluitend outputcontrole wordt toegepast op complexe bedrijven, zoals in het milieudomein tot op heden gebruikelijk was, kan men zich afvragen of deze vorm van toezicht überhaupt statistisch relevant is.

Als het gaat om informatie verzamelen is systeemgericht toezicht (systeemtoezicht plus toezicht op output) eigenlijk altijd effectief omdat het informatie oplevert over de *oorzaken* van naleven of niet naleven. Echter, alleen bij bedrijven met managementsystemen is deze informatie op een eenvoudige (en dus goedkope) manier te verzamelen (zie verder bij efficiënt toezicht).

4.2 Risico gestuurd toezicht

Bij systeemtoezicht wordt beoordeeld in hoeverre de OTS de risico's op ongevallen, schade aan gezondheid en milieuschade effectief beheerst. Tevens wordt beoordeeld of dit gebeurt op een wijze die de goedkeuring van de toezichthouder kan hebben. De OTS kan hiertoe allerlei verschillende

methodieken inzetten die er toe leiden dat risico's worden geanalyseerd en gekwantificeerd en vervolgens beheersmaatregelen nemen zodat de restrisico's tot een aanvaardbaar niveau worden teruggebracht. Hoe beter het risicomanagement van de OTS, des te lager het restrisico. Op deze wijze kan de toezichthouder inzicht verkrijgen in de mate van risicomanagement per OTS en kan hij deze informatie gebruiken voor een risico gestuurde benadering van de sector.

Opgemerkt moet hierbij worden dat een volledig risicoloze maatschappij niet bestaat. Geen enkele vorm van toezicht zal risico's tot nul reduceren. Het gaat er vooral om risico's op een effectieve manier te managen.

Systeemtoezicht levert dus informatie op over de kwaliteit van het risicomanagement van een OTS en kan daarmee een belangrijke bijdrage leveren aan risico gestuurd toezicht.

4.3 Stimulans tot leren

Bij systeemgericht toezicht wordt de aandacht gevestigd op de kwaliteit van het compliance management systeem en hiermee op de processen, strategieën en procedures die naleving tot doel hebben. Argyris en Schon (zie paragraaf 2.2.2) hebben aangetoond dat een fundamenteel niveau van leren mogelijk is als de onderliggende processen en strategieën onderwerp van discussie en verbetering zijn. Bij systeemgericht toezicht wisselen de OTS en de toezichthouder informatie uit over dit diepere niveau op een wijze die voor de toezichthouder en de OTS kan worden begrepen. Op het moment dat de OTS niet (geheel) voldoet aan de systeemcriteria, wordt dit toegelicht en besproken. In verschillende sectoren waaronder bij de projecten in de domeinen chemie en afval is de ervaring dat OTS-en daadwerkelijk hun systeem verbeteren naar aanleiding van systeemtoezicht.

In de Europese burgerluchtvaart heeft systeemtoezicht in belangrijke mate bijgedragen aan het verlagen van de incident rate van 0,64 naar 0,16 fatale ongevallen per miljoen vluchten in de periode 1993 - 2007¹¹.

Systeemtoezicht is dus een vorm van double loop learning die er toe leidt dat de OTS zijn systeem verbetert. Hiertoe is het wel van belang dat de toezichthouder en het bedrijf beide begrijpen hoe een compliance management systeem werkt en bijdraagt aan een betere naleving en risicobeheersing en dat zij hierover met elkaar kunnen communiceren.

4.4 Efficiëntie

In algemene zin is al geconstateerd dat meer vertrouwen besparingen kan opleveren (zie paragraaf 3.1). De vraag bij efficiënt toezicht is: bereiken we ons doel op de meest efficiënte wijze? Hierbij dient zich de vraag aan hoe het doel er uit ziet (SMART) en hoe we kunnen bepalen of dit is bereikt. Pas dan is het mogelijk om de vraag goed te beantwoorden of systeemgericht toezicht een efficiënter alternatief is voor toezicht op output. Hierbij moet worden aangetekend dat men zich kan afvragen of er überhaupt op dit moment wel statistisch relevant toezicht op output is op complexe bedrijven (zie paragraaf 4.1). Uit het Total Quality Management was al bekend dat het efficiënter is om alle activiteiten in één keer goed te doen door mensen in systemen te laten werken. Bij systeemgericht toezicht willen we (a) het toezicht afstemmen op het niveau compliance management van de OTS en (b) de bedrijven met potentie tot compliance management (niveau 2 CM en hoger) stimuleren hun systeem verder te verbeteren.

¹¹ Veiligheidsstatistieken burgerluchtvaart, Inspectie Verkeer en Waterstaat 2008

Informatie verzamelen

Dit proces kan bij bedrijven met compliance management systemen heel efficiënt omdat de systemen van de OTS-en de informatie genereren. Het betreft hier zowel informatie over naleving, gezondheid, ongevallen en milieuschade als informatie over de werking van het systeem. Zo worden bij een groot industrieel bedrijf jaarlijks al snel tientallen interne inspectierondes gelopen en gerapporteerd.

Wellicht kan op termijn ook gebruik worden gemaakt van de werkwijze die bij ISO certificering wordt toegepast. Een mogelijke overweging is om aan de bestaande norm ISO 14001 een extra module of extra eisen toe te voegen met de relevante compliance management criteria zodat een norm ontstaat die voor toezicht op naleving van milieuregels kan worden gebruikt. Bij het beoordelen van het compliance management systeem dient dan wel geborgd te zijn dat de certificerende instelling een objectief en kwalitatief goed oordeel geeft. Ook dient de toezichthoudende instantie in een dergelijk geval te waarborgen dat het de kennis in huis houdt om systeemtoezicht en reality checks uit te kunnen voeren, mochten er problemen ontstaan in de uitvoering.

De OTS aanzetten tot verbeteren

Dit proces kan bij bedrijven met een basisniveau (vanaf niveau 2 CM) efficiënt omdat deze bedrijven al een voedingsbodem hebben voor leren op systeemniveau. Bedrijven die niet aan het basisniveau voldoen zijn minimaal nog enkele jaren bezig om een systeem op te zetten en een cultuuromslag te maken. Voor deze bedrijven heeft systeemtoezicht (nog) geen zin.

Bij beide bovenbeschreven processen is het wel van belang dat de toezichthouder niet doorschiet in details en het systeemgericht toezicht beperkt tot relevante punten.

Systeemtoezicht kan dus een efficiëntievoordeel opleveren als het in de juiste situatie en op de juiste wijze wordt toegepast.

4.5 Conclusie

Hoewel een hard bewijs lastig te geven is, zijn er duidelijke aanwijzingen dat systeemtoezicht in een aantal specifieke situaties een zinvolle bijdrage kan leveren aan het realiseren van de doelstellingen van goed toezicht. Vooral bij grote bedrijven liggen er kansen om door middel van systeemtoezicht de informatiepositie van de toezicht te verbeteren, het risico gestuurde toezicht te verfijnen, de OTS-en aan te zetten tot verbeteringen en toezicht efficiënter te maken.

5 Systeemtoezicht in de praktijk

5.1 Pilots frontoffices chemie en afval

In 2007 en 2008 is met de compliance competence audit vanuit de frontoffices geëxperimenteerd in de domeinen chemie en afval¹². Uit deze pilots blijkt dat voor de toezichthoudende instanties goede mogelijkheden bestaan om het toezicht af te stemmen op de interne controle en bewaking van de OTS. Zo kan het bijzonder verhelderend zijn als bedrijf en toezichthouder samen een risico analyse opstellen (één van de systeemeisen bij de compliance competence audit).

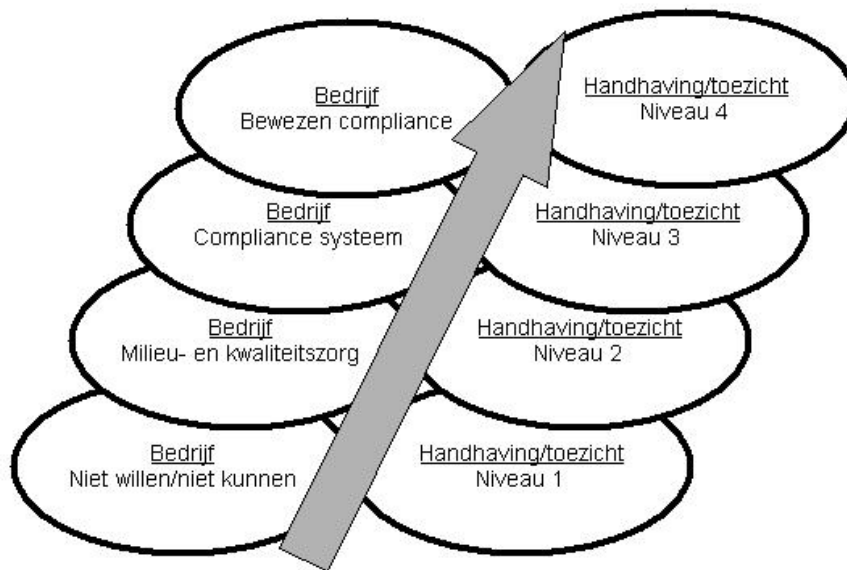
Bedrijven kunnen in vier niveaus van compliance management worden ingedeeld. Deze niveaus vormen een groeimodel dat aangeeft hoe bedrijven en toezichthouders samen naar een hoger niveau kunnen groeien door zich respectievelijk te concentreren op een betere borging van naleving en een aangepaste wijze van toezicht die uit gaat van groeiend vertrouwen.

1. Bedrijven die niet willen en/of niet kunnen naleven. Deze bedrijven zijn niet bereid tot regelnaleving en/of niet in staat tot regelnaleving vanwege het ontbreken van de benodigde competenties.
2. Bedrijven met een gecertificeerd of certificeerbaar management systeem zoals bijvoorbeeld conform ISO 9001 of 14001 certificaat of gelijkwaardig. Deze bedrijven hebben de basis van het kwaliteitsdenken (borging en continue verbetering) in bepaalde mate aantoonbaar in de vingers maar dit is niet specifiek gericht op het borgen van de naleving van wettelijke eisen.
3. Bedrijven met een effectief compliance management systeem (CMS). Deze bedrijven hebben een managementsysteem dat specifiek gericht is op het borgen van regelnaleving en het verbeteren van de nalevingsprestatie.
4. Bedrijven met bewezen compliance management. Deze bedrijven zitten in de 'eredivisie' van compliance management. Hebben een managementsysteem dat specifiek gericht is op het borgen van regelnaleving en verbeteren van de nalevingsprestatie dat zich meerdere jaren heeft bewezen door goede resultaten en continue verbetering.

Figuur 5-1 geeft deze vier niveaus van CM aan.

¹² Zie Eindrapport Pilot Compliance Management, VROM, juni 2008 en Toezichtslastvermindering bij een grote Afvalverwerkingslocatie, 2007

Figuur 5-1 Groeimodel: Niveaus van Compliance Management



Voor de niveaus 3 en 4 zijn in de pilots normen ontwikkeld op basis van de systeemeisen door middel van overleg tussen bedrijf en toezichthoudende instanties.

Bovenstaande figuur geeft aan dat bedrijven met verschillende niveaus van compliance management, een verschillende benadering vanuit de toezichthouders vragen.

Mythe # 5 Voor compliance management moet een heel nieuw systeem worden opgezet

Als een bedrijf een goed werkend managementsysteem heeft dat bv. voldoet aan gangbare normen als ISO 9001, 14001 of OHSAS 18001, dan is hiermee een groot deel van de functionaliteit van een effectief compliance management systeem aanwezig. Met een klein aantal specifieke uitbreidingen kan doorgaans dan al een goed werkend compliance management systeem worden gerealiseerd. Hierbij wordt dus in grote mate gebruik gemaakt van bestaande managementsystemen van bedrijven.

Compliance management moet een onderdeel van het managementsysteem zijn en wel dat deel dat specifiek is gericht op regelnaleving. Dit is dus een ander doel dan een kwaliteitssysteem of een milieuzorgsysteem heeft. Bij systeemtoezicht worden dus specifiek de compliance management onderdelen van het systeem beoordeeld.

In de pilot bij chemisch bedrijf ThermPhos International in Vlissingen zijn afspraken gemaakt tussen bedrijf en de provincie Zeeland over het toepassen van meer systeemtoezicht als het bedrijf niveau 3 en 4 CM behaalt. Ook is afgesproken dat afgezien wordt van sancties als het bedrijf minimaal niveau 3 CM haalt en de betreffende overtreding zelf opspoort, beëindigt en maatregelen neemt om herhaling van de overtreding te voorkomen. In het kader van deze pilot is onder andere een auditmethode compliance competence ontwikkeld (zie onder andere bijlage 4 en 5).

Ook in andere projecten (Twence/Provincie Overijssel, ATM/Provincie Noord-Brabant, VAR/Provincie Gelderland, AkzoNobel Delfzijl/Provincie Groningen) zijn vergelijkbare afspraken tussen bevoegd gezag en OTS gemaakt of in voorbereiding over de toepassing van systeemgericht toezicht afhankelijk van het CM niveau van het betreffende bedrijf. De Provincie Noord-Brabant is een pilot systeemtoezicht gestart met 15 grote bedrijven en heeft een beleidskader opgesteld dat is gebaseerd op de aanpak van de ThermPhos pilot¹³.

In de pilot bij AkzoNobel Delfzijl is naast toezicht ook vergunningverlening een onderdeel. Hier speelt de vraag hoe bij het opstellen van vergunningen rekening kan worden gehouden met het competentieniveau van de OTS en het uitvoeren van systeemtoezicht. Wordt bij systeemtoezicht een beroep gedaan op het zelfcontrolerend vermogen van de OTS, bij vergunningverlening kan een beroep worden gedaan op het zelfregulerend vermogen.

In bijlage 7 is een voorbeeld gegeven van de invulling van het systeemgerichte toezicht.

Doordat de betrokken partijen specifieke wensen en eisen hebben zijn de afspraken in de verschillende projecten niet geheel identiek. Kleine verschillen treden o.a. op ten aanzien van:

- de scope van de afspraken (alleen Wm of breder),
- de termijn waarop de OTS gereed is voor de verificatie audit van Cm niveau 3 en/of 4,
- de exacte formulering van de vragen en de toelichting (varianties op bijlage 4 en 5),
- door wie de verificatie audit wordt uitgevoerd (bevoegd gezag alleen of samen met certificerende instelling) en
- de vorm waarin de afspraken worden vastgelegd (schriftelijke bevestiging per brieven of toezichtconvenant);

5.2 Systeemtoezicht in andere domeinen

Op veel verschillende plaatsen werkt men aan de opzet en implementatie van systeemtoezicht. De Inspectieraad heeft hiervan in september 2008 een voorlopig overzicht opgesteld¹⁴. Systeemtoezicht wordt vooral toegepast in sectoren met grote complexe bedrijven actief zijn en waar substantiële risico's spelen.

Zo is systeemtoezicht op luchtvaartmaatschappijen al kort na de Tweede Wereldoorlog ontstaan en inmiddels gedeeltelijk wettelijk vastgelegd. In de hierop volgende jaren heeft de toepassing van systeemtoezicht zich uitgebreid naar aanpalende sectoren zoals luchthavens, verkeersleiders en onderhoudsbedrijven.

In de watersector houdt de Inspectie Verkeer en Waterstaat door middel van systeemtoezicht op het totale stelsel.

De Voedsel en Warenautoriteit heeft in 2009 systeemtoezicht op de agenda staan voor o.a. de formulebedrijven in de voedingsmiddelenindustrie.

In de ziekenhuissector heeft de brancheorganisatie eisen opgesteld voor een managementsysteem voor de borging van patiëntveiligheid en is hierover in gesprek met de Inspectie Gezondheidszorg.

¹³ Beleidskader voor de pilot systeemtoezicht 2009-2010, Provincie Noord-Brabant, 9 april 2009

¹⁴ Rijksacties rond systeemtoezicht, Inspectieraad, 1 september 2008

6 Systeemgericht toezicht; Wanneer is het zinvol?

Mythe # 6 Systeemtoezicht is dé oplossing voor alle problemen
 Net als een hamer vooral effectief is als je een spijker in een stuk hout wilt slaan, zo is systeemtoezicht alleen in bepaalde gevallen zinvol. Systeemtoezicht is één van de vele instrumenten die een toezichthoudende instantie kan inzetten om het toezicht effectief te doen zijn. Systeemtoezicht heeft alleen zin als het gericht wordt toegepast op bedrijven die een compliance management systeem hebben of dit binnen afzienbare tijd kunnen opzetten.

6.1 Uitgangspunten

Om de voordelen van systeemtoezicht te kunnen benutten is het zaak om te bepalen in welke situaties systeemgericht toezicht nuttig kan worden toegepast (randvoorwaarden). In de volgende paragrafen wordt bij deze randvoorwaarden stilgestaan.

6.2 Randvoorwaarden voor systeemgericht toezicht

Vertrouwen op basis van systeemeisen

De belangrijkste randvoorwaarde is dat er een basisniveau van vertrouwen is en dat de OTS voldoet aan een minimumniveau. Met de compliance competence audit (bijlage 3 en 4) kan worden vastgesteld in hoeverre vertrouwen gerechtvaardigd is. Ten aanzien van de vier niveaus compliance management van figuur 5-1 kunnen we het volgende stellen:

Niveau 1 CM:

Bedrijven in deze categorie hebben geen (volledig en werkend) managementsysteem en komen niet in aanmerking voor systeemgericht toezicht.

Niveau 2 CM:

Bedrijven in deze categorie hebben een basis managementsysteem. Deze bedrijven hebben het vermogen om naleving te borgen omdat zij gewend zijn te werken met een managementsysteem. Maar omdat dit systeem van deze bedrijven (nog) niet specifiek is gericht op regelnaleving, moeten bedrijven in deze categorie nog verbeteringen doorvoeren om op niveau 3 of 4 CM te komen. Dit betekent dat de toezichthouder met deze bedrijven wel afspraken kan maken dat zij in aanmerking komen voor systeemgericht toezicht op het moment dat zij het management systeem zodanig verbeteren dat dit voldoet aan niveau 3 of 4 CM.

Niveau 3 CM:

Bedrijven in deze categorie beschikken over een goed werkend compliance management systeem dat voldoet aan de minimum eisen (bijlage 6). Deze bedrijven komen in aanmerking voor systeemgericht toezicht.

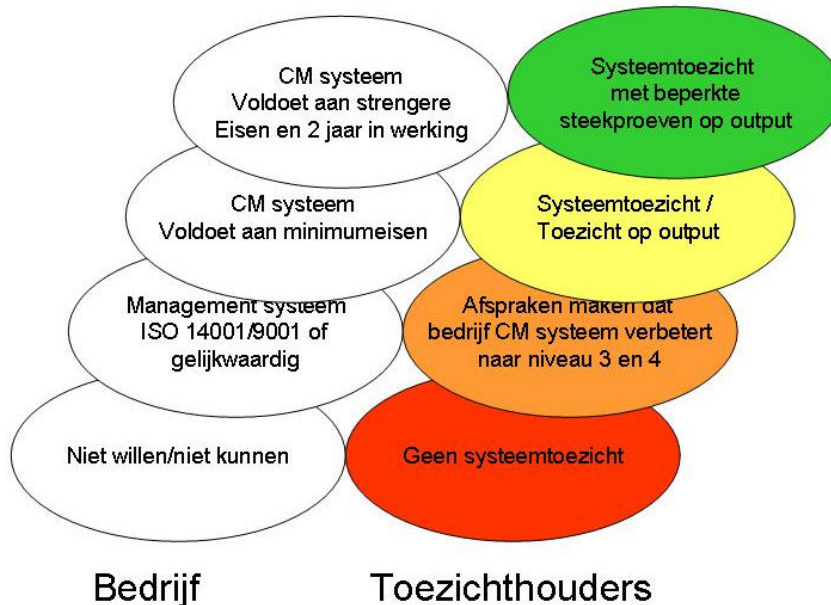
Niveau 4 CM:

Bedrijven in deze categorie hebben een bewezen compliance management systeem dat voldoet aan strengere eisen dan die gelden voor niveau 3 CM (bijlage 6). Deze bedrijven zijn qua harde

stysysteemelementen en cultuur het meest vergevorderd en komen in aanmerking voor een vorm van systeemgericht toezicht die vooral bestaat uit systeemtoezicht en minimale steekproefsgewijze outputcontroles.

In figuur 6-1 is weergegeven welke niveaus compliance management en toezicht bij elkaar horen.

Figuur 6-1 Niveaus compliance management en toezicht



Het onder toezicht staande bedrijf moet, om aanmerking te komen voor afspraken over systeemtoezicht, dus minimaal beschikken over een managementsysteem dat gecertificeerd of certificeerbaar is conform ISO 14001 of 9001 of op andere wijze kunnen aantonen dat men kwaliteitszorg toepast. Van bedrijven die niet met een dergelijk managementsysteem werken is onduidelijk of deze gewend zijn te werken met borgingsmaatregelen en verbetercycli (continue verbetering).

Dit basisniveau van vertrouwen (niveau 2 CM) is de primaire randvoorwaarde waaraan moet worden voldaan voor het toepassen van systeemgericht toezicht (SGT).

Naast dit basisniveau van vertrouwen zijn er nog enkele randvoorwaarden waaraan moet worden voldaan voordat geconcludeerd kan worden of SGT zinvol is. Het gaat hierbij om:

- competenties toezichthouders
- bijdrage aan de effectiviteit en efficiëntie van toezicht
- acceptatie van betrokkenen

Deze randvoorwaarden worden hieronder toegelicht.

Benodigde competenties

De toezichthouder dient, naast de inhoudelijke kennis en ervaring van het vakgebied, over extra competenties beschikken om systeemtoezicht uit te kunnen voeren. Het gaat hierbij met name om auditvaardigheden en bedrijfskundige en organisatorische kennis. Een alternatief voor het zelf opbouwen van deze competenties is deze van buitenaf te betrekken door het inschakelen van een derde (bijvoorbeeld een certificerende instelling). Het spreekt vanzelf dat dit alleen mogelijk is als deze instellingen voor de betreffende sector bestaan en voldoende kwaliteit kunnen leveren.

Systeemgericht toezicht vraagt ook om een andere houding van de toezichthouder. Als de toezichthouder enerzijds te snel terugvalt in oude reflexen bij een afwijking of overtreding, is het snel gedaan met de zorgvuldig opgebouwde vertrouwensrelatie. Anderzijds zal de toezichthouder indien nodig ook moeten kunnen ingrijpen als de OTS niet adequaat reageert op problemen. Voor de toezichthoudende instantie betekent systeemtoezicht dat men de kwaliteiten die men bij de OTS-en wenst te zien in termen van kwaliteitszorg en proactieve cultuur, dient te spiegelen in de eigen organisatie. Een toezichthoudende instantie die in deze opzichten tekort schiet, zal minder geloofwaardig zijn voor de OTS-en.

Bijdrage aan de effectiviteit en efficiëntie van toezicht

Allereerst speelt hier de vraag of systeemtoezicht kan bijdragen aan het realiseren van de doelen van toezicht. Hier is dus de vraag of SGT bijdraagt aan de doelen die zijn gesteld voor het toezicht op de domeinen chemie en afval (zie hoofdstuk 4).

Verder worden algemene normen gesteld aan overheidstoezicht. Deze normen houden kortweg in dat het toezicht gebeurt vanuit een onafhankelijke functie, er geen elementen ontbreken, dat de elementen op elkaar zijn afgestemd en dat het gebaseerd is op beleid¹⁵.

Daarnaast is de vraag of systeemtoezicht bijdraagt aan vertrouwen. Daarvoor is verbeterambitie nodig bij de het bedrijf en het vermogen tot continue verbetering (vertrouwd zijn met continue verbetering op de eigen processen). Zoals eerder opgemerkt is het hierbij van belang dat de toezichthoudende instanties gelijke tred kunnen houden met deze ontwikkeling door systeemtoezicht professioneel uit te voeren.

Mythe # 7 Een compliance management systeem betekent gegarandeerd 100% naleving van wettelijke eisen

In een complexe wereld bestaat geen 100% garantie dat er nooit iets mis zal gaan of dat niet incidenteel een regel wordt overtreden. Bij compliance management gaat het er om wat gedaan wordt om te voorkomen dat het mis gaat én, als het eens een keer mis gaat, wat er van geleerd wordt.

Een incidentele overtreding betekent dus niet perse dat het compliance management systeem niet goed functioneert.

Naast de effectiviteit van systeemtoezicht is de efficiëntie van belang. Enerzijds betekent dit dat het bedrijf een lagere toezichtslast ervaart, ofwel in kosten dan wel in perceptie. Kostenbesparingen zijn denkbaar, zowel voor toezichthouders als bedrijf, omdat systeemtoezicht zich richt op de oorzaken van bepaalde tekortkomingen, terwijl toezicht op output zich op symptomen richt. Anderzijds betekent dit dat voor de toezichthouders de lasten en baten van systeemtoezicht op termijn (na het doorlopen van de leercurve om systeemtoezicht in te voeren en onder de knie te krijgen) moeten opwegen tegen de kosten voor toezicht op output.

Acceptatie van betrokkenen

Om te beginnen gaat het er om dat de direct betrokkenen, toezichthouders, bedrijven en sector, er belang bij hebben dat systeemtoezicht wordt ingezet. Als één van de partijen met onoverkomelijke kosten, risico's, kans op (reputatie)schade of andere bezwaren wordt geconfronteerd, kan er op substantiële weerstand worden gerekend.

¹⁵ Wieles J., Toezicht en de Algemene Rekenkamer, presentatie congres Compliance en overheidstoezicht, Bynkershoekinstituut, 2007

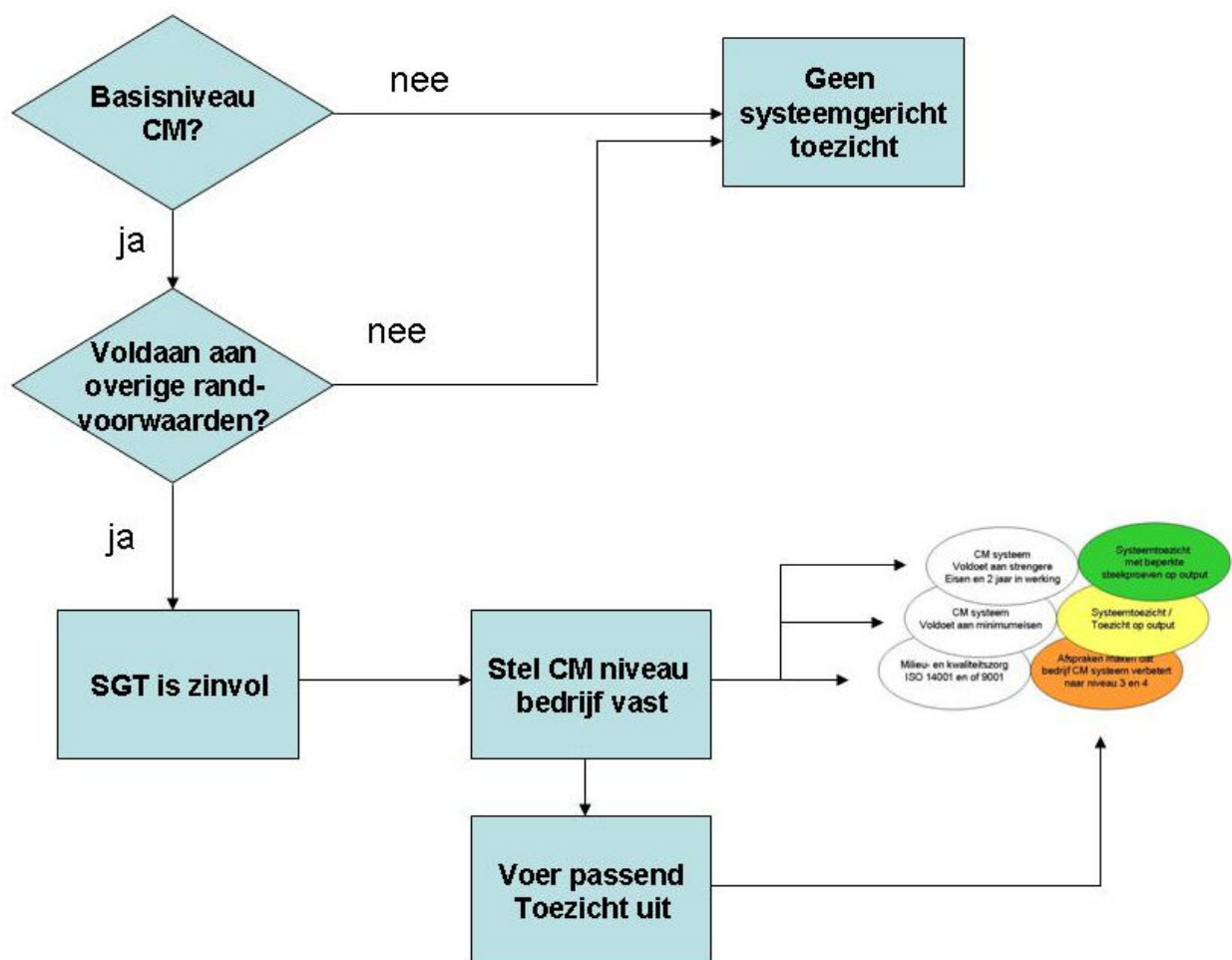
Verder is de eventuele weerstand van indirect betrokken zoals toezichtspartners (OM/justitie, andere inspecties en toezichthouders), samenleving en politiek van belang. In dit verband speelt met name de vraag of deze partijen het erover eens zijn dat systeemtoezicht een effectief instrument is in een bepaalde situatie en dat het vertrouwen gerechtvaardigd is.

Het laatste punt betreft het Nederlandse en Europese institutionele kader (beleid en wetgeving). Soms zijn er beleidsmatige of wettelijke belemmeringen die systeemtoezicht in de weg staan. Het omgekeerde komt echter vaker voor; namelijk dat systeemtoezicht in wettelijke kaders wordt voorgeschreven en hierin ook wordt bepaald hoe het moet worden uitgevoerd.

In de wetgeving die van toepassing is op de domeinen chemie en afval wordt slechts in beperkte mate het hebben van een managementsysteem voorgeschreven; het belangrijkste voorbeeld is de verplichting in het Brzo'99 tot het hebben van een veiligheidsbeheerssysteem. Hiervoor is een voornorm ontwikkeld, de NTA 8620, die gebaseerd is op de OHSAS 18001 en de ISO 14001.

In onderstaand beslisschema (Figuur 6-2) is weergegeven welke vragen beantwoord moeten worden om te komen tot de beslissing STG in te zetten.

Figuur 6-2 Beslisschema Systeemgericht Toezicht



6.3 Interventies en systeemgericht toezicht

In deze paragraaf wordt kort stilgestaan bij de rol van interventies bij systeemtoezicht. Beoogd wordt niet om hier een volledig en doorwrocht exposé te geven van de juridische en beleidsmatige aspecten.

Interventies kunnen gericht zijn op het herstel van een incidentele normoverschrijding, op correctie van structurele afwijkingen van normen, of op verbeteringen van het systeem. In de hogere niveaus van de groeimodel (figuur 6-1) passen interventies die erop zijn gericht aan te zetten tot een verdere verbetering van het systeem, of die erop zijn gericht om de OTS te belonen voor de goede werking van het systeem.

- Als er systeemonderdelen falen, dringt de toezichthouder aan op structurele verbeteringen. De implementatie van verbeteringen wordt gevolgd.
- Bij goed werkende systemen kan de OTS met positieve interventies worden beloond, bijvoorbeeld door middel van witte lijsten, of meer formeel, door middel van het verlenen of continueren van een vergunning. Een dergelijke beloning kan een extra stimulans voor verbetering geven.

Naarmate een OTS effectief de regelnaleving borgt en zijn eigen afwijkingen en overtredingen opspoorde, deze beëindigt en maatregelen neemt om herhaling te voorkomen, ligt het voor de hand om af te zien van interventies in de bestraffende sfeer (zowel bestuurs- als strafrechtelijk). Hier zijn twee overwegingen voor:

1. Bij systeemtoezicht wordt van het bedrijf verlangd dat het ervoor zorgt dat het de eigen naleving borgt. Onderdeel van compliance management is een lerende component: het bedrijf identificeert de eigen afwijkingen en overtredingen, onderzoekt deze en neemt verbetermaatregelen. Om de werking van dit mechanisme goed te kunnen beoordelen vraagt de systeemtoezichthouder om informatie.

Sancties zijn in een dergelijke situatie niet effectief. Hier geldt de transparantieparadox: het toepassen van een sanctie op grond van informatie die het bedrijf zelf heeft verzameld, verwerkt en aangeleverd is wel mogelijk, maar gaat doorgaans ten koste van de openheid van de OTS ten opzichte van de toezichthouder die men juist bij systeemgericht toezicht nastreeft¹⁶.

Deze paradox heeft een harde en een zachte kant.

De zachte kant gaat over het wederzijdse vertrouwen. Zonder vertrouwen van het bedrijf in de overheid in haar toezichthoudende rol is de kans erg klein dat de toezichthouder in staat zal zijn om de benodigde informatie te verzamelen om het systeem goed te kunnen beoordelen en dus om systeemtoezicht te kunnen uitvoeren. Dit betekent dat de overheid als toezichthouder en handhaver ervoor moet zorgen dat het bedrijf vertrouwen heeft in de toezichthoudende overheid.

Dit vertrouwen kan op basis van dezelfde elementen worden gebaseerd als die op grond waarvan de toezichthouder vertrouwen kan hebben in een OTS: competenties, openheid, nakomen van afspraken en zelfreflectie (zie hoofdstuk 3). Het opbouwen van vertrouwen is belangrijk en een uitdaging in een wereld die jarenlang is gebaseerd geweest op wederzijds wantrouwen.

De harde kant heeft te maken met de concrete duidelijkheid over wat er met de door het bedrijf geleverde informatie gaat gebeuren op het moment dat het bedrijf voor de keuze staat deze informatie te overhandigen. Nu adviseren bedrijfsjuristen het management vaak om terughoudend te zijn met het verstekken van gevoelige compliance informatie omdat onduidelijk is tot welke gevolgen dit leidt. (Voor meer informatie hierover zie bijlage 2).

2. Ten tweede zijn er verschillende mogelijkheden voor het afzien van sancties.

Bestuursrechtelijke sancties zijn er op gericht om de overtreding te beëindigen en om herhaling te voorkomen. Deze sancties zijn nodig als een OTS overtredingen begaat en deze niet adequaat

¹⁶ Gabriël-Breukers, Hulp bij de Handhaving, WLP Nijmegen, 2008

afhandelt (zelf constateren, beëindigen en maatregelen nemen om herhaling te voorkomen). Als het systeem van de OTS wel effectief voorziet in deze acties, is dit type sancties niet meer nodig¹⁷.

Strafrechtelijke sancties kunnen achterwege worden gelaten op grond van het opportuniteitsbeginsel dat is vastgelegd in artikel 167 en 242 Sv. Hierin is bepaald dat van vervolging kan worden afgezien op gronden aan het algemeen belang ontleend (artikel 167) zolang het onderzoek op de terechtzitting niet is gestart (artikel 242)¹⁸. Beperking van de strafrechtelijke sancties is mogelijk bij het opleggen van een voorwaardelijke transactie met als bijzonder voorwaarde dat het bedrijf een compliance management systeem opzet¹⁹.

Het Landelijk Overleg Milieuhandhaving heeft in haar landelijke sanctiestrategie criteria geformuleerd voor het afzien van bestuurs- en strafrechtelijke optreden. Op milieugebied biedt hiertoe de LOM sanctiestrategie²⁰ mogelijkheden. Deze stelt dat optreden (bestuurs- dan wel strafrechtelijk) achterwege kan blijven indien de overtreding:

- * niet doelbewust is begaan en
- * een kennelijk incident betreft en
- * gering van omvang is en
- * van een overigens goed nalevende overtreder
- * die onverwijld afdoende maatregelen heeft getroffen.

¹⁷ Eindrapport Pilot Compliance Management ThermPhos, Frontoffice Chemie, 2008

¹⁸ Deze mogelijkheid wordt genoemd door Gabriël-Beukers S.K., Hulp Bij Handhaving, 2008

¹⁹ Van deze mogelijkheid heeft het OM gebruik gemaakt in de casus van een grondreinigingsbedrijf in Amsterdam in 2001 op basis van de Aanwijzing Hoge Transacties van 1999. Een deel van de geldboete kon achterwege blijven onder de voorwaarde dat het bedrijf een compliance management systeem zou opzetten om herhaling te voorkomen.

²⁰ Landelijke Strategie Milieuhandhaving, Sanctiestrategie als bedoeld in criterium 2.3 van de Professionalisering in de Milieuhandhaving, eindversie dd 25 maart 2004 met mandaat vastgesteld door het Bestuurlijk Landelijk Overleg Milieuhandhaving

7 Verdere ontwikkeling

Hoofdstuk 6 geeft aan wanneer systeemgericht toezicht zin heeft en hoe systeemgericht toezicht kan worden uitgevoerd. Op een aantal punten dienen acties te worden ondernomen om de toepassingsmogelijkheden van systeemgericht toezicht uit te breiden. In dit hoofdstuk wordt een beknopt overzicht gegeven van deze punten.

- verankeren van systeemgericht toezicht in het landelijke beleid en eventueel wetgeving;
- actualiseren en specificeren toelichting van de compliance competence audit;
- opstellen van een leidraad voor het beoordelen van het risicomanagement als onderdeel van het compliance management systeem;
- opstellen van een basismodel voor het afspraken document waarin is vastgelegd hoe het vernieuwde toezicht voor elk niveau compliance management er precies uitziet;
- uitwerken integraal systeemgericht toezicht vanuit verschillende toezichthouders;
- onderzoeken van de juridische aspecten van systeemgericht toezicht;
- afstemmen met het Openbaar Ministerie over de rol van strafrecht bij systeemgericht toezicht;
- monitoren van afspraken van de pilotbedrijven (o.a. ervaringen transparantieparadox);
- uitwerken gevolgen vergunningverlening (pilot AkzoNobel);
- uitwerken competentiebehoefte toezichthouders (strategische kenniskaart, leerlijn);
- bepalen eisen toezichthoudende instanties;
- afstemmen met de ontwikkelingen inzake Brzo;
- onderzoeken of en zo ja, onder welke voorwaarden gebruik kan worden gemaakt van certificerende instellingen en certificatie zoals bv. ISO 14001.

Om aan de uitwerking van deze punten gestalte te geven is een werkgroep systeemgericht toezicht geformeerd waarin vertegenwoordigers o.a. van provincies, IPO, VROM Inspectie, Arbeidsinspectie, en bedrijfsleven deelnemen.

Bijlage 1 Lijst met afkortingen

CM	Compliance management
IVW	Inspectie Verkeer en Waterstaat
OTS	Onder toezicht staande organisatie
SGT	Systeemgericht toezicht
SMART	Specifiek, Meetbaar, Aantoonbaar, Realistisch en Tijdgebonden
ST	Systeemtoezicht
VWA	Voedsel en Warenautoriteit

Bijlage 2 Ervaringen in de Verenigde Staten

Toeziht

In de Verenigde Staten zijn er diverse regelingen en programma's waaraan bedrijven kunnen deelnemen en waaraan vrijwillige inspanningen van bedrijven op het terrein van compliance management leiden tot aangepast en verminderd preventief toezicht.

Het performance track program bijvoorbeeld (<http://www.epa.gov/performance-track>) nodigt bedrijven uit om borgingsmaatregelen in hun managementsystemen te nemen ter bescherming van het milieu en geeft bedrijven in ruil daarvoor meer ruimte door controles vooraf aan te kondigen en deze te richten op de werking van de maatregelen. In een evaluatie bijeenkomst in 2005²¹ zijn door deelnemers (verenigd in de Performance Track Participants Association) de volgende voordelen genoemd:

- 'Het programma geeft ons de kans om milieu effecten te kwantificeren en levert een structuur voor het meten van milieu resultaten' (Coca Cola, two plants);
- 'Het geeft intern zichtbaarheid aan de veiligheids- en gezondheidsprogramma's. Ook heeft het geholpen om milieuprogramma te integreren in de business processen. Het heeft de dialoog op gang gebracht en tot begrip geleid tussen toezichthouders en bedrijf. De erkenning is prachtig' (Rockwell Collins);
- 'Performance Track is een geweldig programma dat de dialoog op gang brengt tussen overheid en bedrijf' (Johnson & Johnson).

Verbetermogelijkheden liggen in:

- snellere afhandeling van vergunningaanvragen van leden;
- afstemming met rijks-/ lokale luchtemissie programma's;
- controlebezoeken moeten een partnership worden tussen EPA en de plant met afzien van optreden als het bedrijf goed heeft gereageerd op een evt. overtreding.

De USEPA werkt met twee delen in de sanctie: een deel dat staat voor de verwijtbaarheid (gravity) en een deel dat staat voor het door de overtreder genoten economische voordeel. EPA hecht er veel waarde aan als bedrijven zelf overtredingen opsporen en oplossen. In dat geval is er een laag of geen gravity part. Het beleid van de USEPA zoals uitgewerkt in 'Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations', USEPA, 2000, geeft aan dat als ondernemingen overtredingen begaan en voldoen aan voorwaarden ten aanzien van het preventieve en correctieve maatregelen, worden tegemoet gekomen in de interventie die de USEPA pleegt:

- 100% of 75% reductie van de gravity based penalty (deel van de straf die als verwijtbaar wordt aangemerkt. Het economisch voordeel dat een bedrijf eventueel geniet, wordt wel afgenomen door middel van een boete;
- geen aanbeveling voor strafrechtelijke vervolging;
- geen verzoek om interne audit rapporten, waarbij USEPA wel de vrijheid behoudt om een eigen onderzoek te starten als overtredingen worden vermoed.

Strafrechtelijke richtlijnen voor organisaties

De Federal Sentencing Guidelines²² zijn voor wat betreft de Organizational Sentencing Guidelines (strafrechtelijke richtlijnen voor o.a. bedrijven, vakbonden, stichtingen en overheidsorganen) in 1991 van kracht geworden. Deze richtlijnen zijn ontworpen om zowel de bestraffing te regelen alsook om organisaties te bewegen om strafbaar handelen op te sporen en te voorkomen.

²¹ http://www.epa.gov/performance-track/benefits/regadmin/OPAR_PTrack_meeting_summary.pdf

²² US Federal Sentencing Guidelines, Chapter 8 Organizational Guidelines, 2004

In hoofdstuk 8 van de Federal Sentencing Guidelines (FSG) wordt geregeld op welke wijze de (strafrechtelijke) strafmaat voor een overtredende onderneming wordt vastgesteld:

Er is een basisboete als uitgangspunt. Als er financieel voordeel voor de overtredende onderneming is geweest, kan dit financiële voordeel de basis vormen.

Vervolgens is er een deel van de boete gekoppeld aan de mate van schuld of verwijtbaarheid (culpability score). Wanneer de overtredende onderneming een 'effective compliance and ethics program' heeft, worden punten afgetrokken waardoor de culpability score tot nul kan afnemen. Ook als de onderneming zelf de overtreding meldt worden punten van de culpability afgetrokken.

In dit hoofdstuk van de FSG is ook bepaald wat men verstaat onder een effective compliance and ethics program. Dit is uitgewerkt in een aantal algemeen geformuleerde compliance management criteria. Deze criteria zijn:

1. compliance standaarden en procedures die redelijkerwijs geschikt zijn om onrechtmatig handelen te voorkomen;
2. overall toezicht op compliance door gezaghebbend personeel (directielid);
3. kritische functies worden bekleed door mensen met schoon blazoën;
4. communicatie, training en opleiding;
5. monitoring, auditing en rapportage systemen;
6. interne controle en discipline;
7. continue verbetering.

Hierbij wordt gesteld dat een enkele overtreding niet automatisch betekent dat het programma niet effectief is. (De volledige tekst van hoofdstuk 8 van de FSG is opgenomen in bijlage 1).

Een bedrijf komt alleen voor strafvermindering in aanmerking als een overtreding direct wordt gerapporteerd aan het bevoegd gezag en er geen directe betrokkenheid is van de directie.

De invoering van de guidelines in 1991 hebben een enorme impuls gegeven aan de opzet van compliance and ethics programs door bedrijven. Doordat de criteria zijn gesteld in termen die bedrijven begrijpen, leverde implementatie niet al teveel discussie op²³. Overigens zijn milieu overtredingen vooralsnog uitgezonderd van het systeem van strafvermindering omdat men het in 1991 lastig vond om de economische aspecten goed in te schatten. Het staat wel op de planning om milieuovertredingen in de toekomst te gaan opnemen. Voorlopig heeft de USEPA haar eigen beleid hiervoor vastgesteld.

De guidelines en de criteria voor C&E programs worden preventief gebruikt door bedrijven om hun systeem op te baseren. Het is voor bedrijven erg nuttig om te weten welke criteria de overheid stelt aan hun gedrag op het niveau van de rechtspersoon. De afzonderlijke Agencies zoals de EPA (milieu inspectie) gebruiken afgeleide eisen om op basis hiervan hun toezicht te differentiëren.

Als er een overtreding wordt gepleegd, toetst de inspector-general van de Federal Agency in hoeverre aan de criteria for C&E programs is voldaan. Dit oordeel bepaalt dus mede de strafmaat²⁴.

Er is (nog) geen standaard meetinstrument die aangeeft hoe een audit op een C&E program kan worden uitgevoerd. Momenteel is het de overheid zelf die vaststelt of voldaan wordt aan de eisen en doen bedrijven er goed aan bewijzen te leveren dat men voldoet aan de criteria.

Opvallend is dat in de Verenigde Staten, ondanks het feit dat de bovengenoemde organizational guidelines al geruime tijd van kracht zijn en tussentijds nog enkele malen aangepast, soms nog wel een zgn. litigation dilemma wordt ervaren. Dit dilemma is vergelijkbaar met de transparantie paradox (Gabriel-Breukers, 2008) en duidt op de spanning die er is tussen enerzijds de druk om meer openheid van zaken te geven over de eigen nalevingsprestatie (door het bedrijf zelf geconstateerde overtredingen en welke maatregelen het bedrijf om herhaling te voorkomen) en anderzijds de dreiging

²³ Mondelinge communicatie Amy Schreiber, US Federal Sentencing Commission

²⁴ Mondelinge communicatie Mary Lee Brown, University of Pennsylvania

dat deze informatie tegen het bedrijf wordt gebruikt. Gevolgen van dit dilemma staan volgens de American Chemistry Council (ACC)²⁵ haaks op de wens van openheid en continue verbetering:

- Mensen gaan minder vastleggen uit angst dat dit later tegen het bedrijf kan worden gebruikt en gebruiken mondelinge informatie overdracht. Dit gaat met name in grote organisaties ten koste snelle gedetailleerde informatie overdracht.
- Mensen gaan zichzelf censureren om te voorkomen dat de vastgelegde informatie tegen hen kan worden gebruikt.
- Communicatie wordt beperkt. Hoe meer een document wordt verspreid, des te groter de kans dat het in verkeerde handen komt.
- Onderzoek naar afwijkingen wordt ontmoedigd uit angst dat de uitkomsten tegen het bedrijf worden gebruikt.

Er zijn voorbeelden van het gebruik van materiaal dat in een ethiek training werd gebruikt om aan te tonen dat een bedrijf zich schuldig maakte aan discriminatie. De informatie van het verbeterproces werd hier direct tegen het bedrijf gebruikt²⁶.

Kennelijk is de werking van de guidelines niet altijd zodanig effectief dat het bedrijven altijd aanzet tot volledige openheid. De kwetsbaarheid geldt met name ook ten aanzien van aanklachten van derden. Mogelijke oplossingen die in de VS worden overwogen zijn o.a. het geven van immuniteit aan documenten die door een compliance management systeem worden gegenereerd, d.w.z. deze mogen niet worden gebruikt tegen het bedrijf²⁷. We moeten dit dilemma overigens wel zien in het licht van de cultuur in de VS om snel naar de rechter te stappen.

In het algemeen gesproken worden de organizational guidelines en de bijbehorende methodiek van strafvermindering ervaren als effectief omdat het bedrijven aanzet tot goede programma en het de openheid in het algemeen bevordert²⁸.

²⁵ Task-force of attorney-client privilege, James W. Conrad Jr., American Chemistry Council, 2005

²⁶ Stender vs. Lucky Stores Inc. 803 F. Supp. 259 (N.D. Cal. 1992)

²⁷ Goldsmith M., King C.W., Policing Corporate Crime, The Dilemma of Internal Compliance Programs, Vanderbilt Law Review, 1997

²⁸ Mondelinge communicatie Mary Lee Brown, University of Pennsylvania

Bijlage 3 Criteria voor compliance and ethics programs (US Federal Sentencing Guidelines 2004, Chapter 8)

1. The organization shall establish standards and procedures to prevent and detect criminal conduct.
- 2a. The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.
- 2b. High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.
- 2c. Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.
3. The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.
4. (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.

(B) The individuals referred to in subdivision (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.
- (5) The organization shall take reasonable steps—

(A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;

(B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.
6. The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.
7. After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.

(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

Bijlage 4 Vragenlijst Compliance Competence Audit

Systeem wettelijke kaders

Eis	Verificatie item	Geschikt	Geïmplemen- teerd	Gedocumen- teerd
1.1 Onderhoudt het bedrijf een systeem waarin alle relevante wettelijke eisen zijn opgenomen?	vastlegging regels in database of register			
1.2 Is de verantwoordelijkheid voor het onderhoud van het systeem vastgelegd?	vastlegging verantwoordelijkheid			
1.3 Heeft het bedrijf op basis van een risicoanalyse het detailniveau van de borging van de wettelijke eisen vastgesteld?	beschrijving methodiek risicoanalyse			
1.4 Bevat het systeem een expliciete koppeling tussen de risicovolle wettelijke eisen en de onderdelen van het compliance management systeem waarin de naleving van deze eisen is geborgd?	cross reference met wettelijke regels en interne afspraken, procedures en instructies			
1.5 Houdt het bedrijf het systeem actueel en volledig?	actieve screening wijzigingen			
	aanpassing database of register bij nieuwe regels			
1.6 Onderzoekt het bedrijf structureel de duidelijkheid en de naleefbaarheid van de wettelijke eisen?				

Visie en gedrag

2.1 Heeft het bedrijf een op schrift gestelde, gedragen visie op regelnaleving?	verspreiding visie			
	Inhoud visie			
2.2 Steunt de directie het compliance management systeem?	agenda directieoverleg			
2.3 Heeft het bedrijf een gedragscode waarin concreet is vastgelegd wat het bedrijf van de werknemers verwacht t.a.v. regelnaleving?	Inhoud gedragscode			
	review gedragscode elke 3 jaar			
2.4 Zijn de visie en de gedragscode bekend bij de medewerkers?	verspreiding gedragscode			
2.5 Is in de gedragscode expliciet aangeduid wat van de medewerkers wordt verwacht inzake openheid, opleiding, pro-activiteit en zelf kritische houding ten aanzien van regelnaleving?	inhoud gedragscode			

Kwaliteitsdenken, opleiding, zelfkritische houding en continue verbetering

Eis	Verificatie item	Geschikt	Geïmplementeerd	Gedocumenteerd
3.1 Heeft het bedrijf een gecertificeerd managementsysteem? (bv. ISO 9000/14001) ²⁹ ?	werkend management systeem			
3.2 Wordt het onderhavige managementsysteem systematisch toegepast voor het borgen van regelnaleving?	procedures gericht op regelnaleving			
3.3 Stelt het bedrijf objectieve gekwantificeerde doelstellingen vast ten aanzien van regelnaleving?	maximum aantal afwijkingen			
	doelstellingen meetbaar en realistisch			
3.4 Stelt het bedrijf jaarplannen op waarin voorgenomen acties zijn gedefinieerd ten aanzien van regelnaleving?	is duidelijk wie de actie uitvoert			
	is duidelijk wanneer de actie gereed is			
3.5 Heeft het bedrijf vastgesteld hoe de nalevingsprestatie wordt bepaald?	procedure meting nalevingsprestatie			
	meting objectief en reproduceerbaar			
3.6 Wordt de nalevingsprestatie planmatig gemeten?	rapportage van de meting			
3.7 Registreert het bedrijf systematisch afwijkingen ten aanzien van regelnaleving?	continue planmatige registratie			
3.8 Onderzoekt het bedrijf systematisch de oorzaak van deze afwijkingen?	registratie onderzoek			
3.9 Onderneemt het bedrijf systematisch actie naar aanleiding van het onderzoek naar de oorzaak van afwijkingen ter verbetering van de nalevingsprestatie?	vastlegging acties (wie, wanneer)			
	monitoring uitvoering acties			
3.10 Is er een werkwijze hoe nieuwe werkinstructies t.a.v. regelnaleving aan medewerkers worden gecommuniceerd?	opleidingsplan			
	inhoud			

²⁹ In overleg met de overheid en eventueel de branche organisatie kan een afwijkende eis worden bepaald.

Compliance officer en pro-activiteit

Eis	Verificatie item	Geschied	Geïmplemen- teerd	Gedocumen- teerd
4.1 Heeft het bedrijf een functionaris (hierna te noemen compliance officer) of afdeling (hierna te noemen compliance afdeling) die toeziet op de regelnaleving door het bedrijf?	functie- of afdelingsomschrijving			
4.2 Zijn de taken, bevoegdheden en verantwoordelijkheden van de compliance officer of compliance afdeling schriftelijk vastgelegd?	eenduidige vastlegging taken, bevoegdheden en verantwoordelijkheden			
4.3 Is er een vervangingsregeling voor het geval dat de compliance officer afwezig is?	aangewezen persoon bij compliance afdeling: bezetting gegarandeerd			
4.4 Onderhoudt de compliance officer of compliance afdeling contacten met de overheid met betrekking tot het definiëren van de betekenis van wettelijke eisen voor het bedrijf?	periodiek minstens twee maal per jaar			
	verslagen gesprekken met de overheid			
	inhoud besprekingen			
4.5 Rapporteert de compliance officer of compliance afdeling rechtstreeks aan het hoogste management en onafhankelijk van degenen die binnen het bedrijf verantwoordelijk zijn voor de regelnaleving?	deelname compliance officer in hoogste management overleg			
4.6 Is de compliance officer of compliance afdeling bevoegd te spreken namens het bedrijf?	bevoegdheid schriftelijk vastgelegd (wat, wie)			
4.7 Heeft de compliance officer adequate ervaring, opleiding en training opgedaan?	training compliance officer personeelsdossier			

Openheid en jaarverslagen

Eis	Geschied	Geïmplemen- en-teerd	Gedocumen- teerd
5.1 Communiqueert het bedrijf op open wijze met overheid, omwonenden en andere belanghebbenden over de eigen regelnaleving?			
5.2 Communiqueert het bedrijf op open wijze met belanghebbenden over de werking en de resultaten van het compliancesysteem?			
5.3 Stelt het bedrijf een jaarverslag op waarin wordt gerapporteerd over de eigen nalevingsprestatie?			
5.4 Wordt dit jaarverslag beschikbaar gesteld aan belanghebbenden?			
5.5 Vermeldt dit jaarverslag de prestatie van het bedrijf ten aanzien van het naleven van alle relevante wettelijke eisen?			
5.6 Is dit jaarverslag transparant en eenduidig?			

Pre-screening medewerkers en disciplinaire maatregelen

Eis	Verificatie item	Geschied	Geïmplementeerd	Gedocumenteerd
6.1 Heeft het bedrijf aan de werknemers en bestuurders duidelijk gemaakt welke maatregelen het bedrijf neemt met betrekking tot personen die willens en wetens overtredingen begaan?	intern vastgelegde afspraken			
6.2 Heeft het bedrijf aan de werknemers en bestuurders duidelijk gemaakt dat het bedrijf geen maatregelen neemt tot degene die onopzettelijke overtredingen meldt?	intern vastgelegde afspraken			
6.3 Heeft het bedrijf een overzicht van fraudegevoelige functies?	lijst met functies			
	criteria voor fraudegevoelige functies			
6.4 Heeft het bedrijf maatregelen genomen om ervoor te zorgen dat - fraudegevoelige functies worden bekleed door personen die integer handelen?	screeningsprocedure			
	schriftelijk vastgelegde maatregelen bij niet integer handelen			
6.5 Heeft het bedrijf een systeem om steekproefsgewijs te controleren of de kritische fraudegevoelige taken integer worden uitgevoerd?	minstens twee maal per jaar steekproef			
	resultaten steekproef vastgelegd in rapportage			
6.6 Neemt het bedrijf meteen maatregelen bij het constateren van overtredingen?	vastgelegde maatregelen			
6.7 Heeft het bedrijf aan de werknemers duidelijk gemaakt dat het melden van overtredingen verplicht is?	intern vastgelegde afspraken			
6.8 Heeft het bedrijf een systeem om het melden van overtredingen te bemoedigen?	snelle terugkoppeling melding vanuit management			
	eenvoudige meldingsprocedure			
	mogelijke gevolgen van de melding zijn de melder bekend			

Bijlage 5 Toelichting vragenlijst Compliance Competence Audit

1. Inleiding

De afgelopen jaren heeft de overheid inspanningen verricht om het toezicht op de naleving van wettelijke eisen te moderniseren. Het nieuwe programma Vernieuwing Toezicht (tot voor kort Eenduidig Toezicht geheten) gaat verder waar eerdere modernisering van het toezicht ophielden (zie www.inspectieloket.nl).

Toezicht moet meer zijn gebaseerd op vertrouwen. Uitgangspunten van het nieuwe programma zijn onder andere dat inspecties vooral zijn gericht op risicovolle bedrijven, dat goede bedrijven minder worden gecontroleerd en dat eigen managementsystemen van bedrijven benut worden bij het toezicht. Veel grote bedrijven in Nederland hebben de afgelopen jaren volop geïnvesteerd in het ontwikkelen en implementeren van managementsystemen. Er zijn zorgsystemen voor een groot aantal onderwerpen zoals kwaliteit, milieu, veiligheid en energie. Klanten, aandeelhouders, omwonenden, het moederconcern, de overheid: allemaal verwachten ze van het bedrijf dat het de risico's kent en onder controle heeft.

De overheid dekt risico's af door voor bedrijven wetten en regels op te stellen en te controleren of deze worden nageleefd. Managementsystemen van bedrijven er in de eerste plaats voor het management: om de bedrijfsvoering te optimaliseren. Ze zijn niet primair gericht op het borgen van de naleving van wettelijke eisen. Dit laatste wordt ook wel compliance management genoemd.

Er is bij grote bedrijven wel een groot potentieel om de naleving van wettelijke eisen te borgen in de eigen organisatie op basis van kennis van en ervaring met managementsystemen. Er zijn vaak specifieke managers voor kwaliteit, gezondheid, veiligheid en milieu (QHSE). Echter, doordat de bestaande normen voor managementsystemen niet specifiek zijn gericht op het borgen van de naleving, zijn er grote verschillen in nalevingsgedrag bij bedrijven die werken met gecertificeerde managementsystemen. Dit is zelfs het geval bij de vernieuwde milieuzorgnorm ISO 14001.

Wat tot op heden ontbrak is een specifieke norm voor het bepalen van de effectiviteit van compliance management. De checklist compliance competence waarop deze toelichting betrekking heeft is gebaseerd op het onderzoek 'Waste and Innovation'³⁰, en die is aangepast aan de hand van de bevindingen van een pilot van ThermPhos International, de Provincie Zeeland, de VROM Inspectie (vanuit het frontoffice Chemie) en Syncera.

Het doel van de checklist is om te meten in hoeverre een bedrijf de naleving van wettelijke eisen in de eigen organisatie heeft geborgd.

2. Vertrouwen als basis

Modern overheidstoezicht gaat uit van vertrouwen als basishouding. Vertrouwen kan worden omgezet in vier elementen die aangrijpingspunten voor actie geven³¹. De formule is hieronder weergegeven.

³⁰ Waste and Innovation, M.A. de Bree, Berghauser Pont Publishing, 2006

³¹ Bron: Robert Benninga

**Vertrouwen = geloofwaardigheid x kwaliteit van de relatie x betrouwbaarheid
zelfingenomenheid**

geloofwaardigheid:	is het waar te maken?
kwaliteit van de relatie:	open, prettig, kwetsbaar
betrouwbaarheid:	afpraak is afspraak
zelfingenomenheid:	gebrek aan zelfreflectie en -kritiek

Een effectief compliance management systeem is opgebouwd uit 6 verschillende onderdelen, te weten

- Systeem wettelijke kaders
- Visie en gedrag
- Kwaliteitsdenken, opleiding, zelfkritische houding en continue verbetering
- Compliance officer en pro-activiteit
- Openheid en jaarverslagen
- Pre-screening medewerkers en disciplinaire maatregelen

Deze onderdelen vormen samen een compliance management systeem en zorgen ervoor dat de beoordelende overheid meer vertrouwen krijgt in het bedrijf. Door het compliance management systeem wordt het bedrijf competentier in termen van regelnaleving (geloofwaardigheid), het bedrijf communiceert open over de nalevingsprestatie en de afwijkingen (kwaliteit van de relatie), door het kwaliteitsdenken toe te passen op regelnaleving kan het bedrijf haar afspraken beter nakomen (betrouwbaarheid) en door de cyclus van continue verbetering toe te passen op compliance onderzoekt het bedrijf structureel de eigen prestatie (zelfreflectie en –kritiek).

Elk van de onderdelen van de checklist bevat een aantal vragen waarop moet worden getoetst. Bij de meeste vragen zijn één of meer verificatie items opgenomen die dienen als hulpmiddel om de vraag goed te kunnen beantwoorden. Een verificatie item is een concrete aanwijzing die helpt bij het beantwoorden van een vraag van de checklist.

Een verificatie item is alleen dan akkoord, als deze zowel geschikt, geïmplementeerd als gedocumenteerd is. De auditor kan voor elk van deze drie aspecten op de checklist aangeven of hieraan is voldaan, zodat de auditee duidelijk kan zien op welke aspecten eventueel niet goed wordt gescoord. Deze aspecten zijn ontleend aan de nieuwe inspectiemethodiek van het Brzo.

De checklist dient te worden gebruikt als basis voor een externe verificatie audit. Deze audit bestaat uit 6-8 interviews met sleutelfiguren van de auditee en bestudering van relevante documenten, registers, bestanden en overzichten. Na het onderzoek worden de bevindingen opgenomen in een schriftelijke conceptrapportage met de ingevulde checklist en een toelichting per onderdeel van de checklist en de score op de checklist.

2.1 Eisen auditor en auditerende instelling

Aan de kennis en vaardigheden van de auditor die de verificatie audit uitvoert van het compliance management systeem worden de volgende eisen gesteld:

- werk en denkniveau dat minimaal gelijk is aan het hoger beroepsonderwijs

-de leider van het auditteam is gekwalificeerd als lead-auditor en als auditor compliance competence

- Kennis van:

- auditprincipes, -procedures en -technieken
- wet- en regelgeving in relatie tot het domein waarop het compliance management systeem betrekking heeft
- organisatie- en bedrijfsprocessen, inclusief culturele en maatschappelijke gebruiken
- managementsystemen in het algemeen en normen, methoden en technieken met betrekking tot managementsystemen
- technische aspecten die relevant zijn voor de betreffende sector
- systeemtoezicht en alle relevante aspecten hiervan

Voor de leider van het auditteam geldt als extra eis dat deze is gekwalificeerd als lead-auditor

De verificatie audit kan worden uitgevoerd door het gezag dat bevoegd is voor de wettelijke eisen waarop het compliance management systeem betrekking heeft of door een certificerende instelling. Indien de audit wordt uitgevoerd door een certificerende instelling wordt aangesloten bij de eisen die zijn opgenomen in paragraaf 3.1 van het certificatiesysteem Milieumanagementsystemen volgens ISO 14001 N071129, 20 december 2007, met de volgende aanvullingen:

- eis 3.1.3 geldt niet voor de ISO 14001, maar voor de checklist compliance competence versie 11 december 2007
- eis 3.1.4. geldt niet. Het openbaar maken van informatie is voorbehouden aan bedrijf en bevoegd gezag;

3. Toelichting per vraag en verificatie item

3.1 Systeem wettelijke eisen

Het systeem wettelijke eisen is het geheel aan maatregelen en activiteiten die een bedrijf onderneemt om ervoor te zorgen dat het bedrijf te allen tijde weet aan welke wettelijke eisen het moet voldoen en deze vertaalt naar interne borgingsmaatregelen. Aangezien de wettelijke eisen aan verandering onderhevig zijn, dient deze borging geen statische toestand te zijn, maar dynamisch te worden ingevuld zodat ook de naleving van wijzigingen in wettelijke eisen worden geborgd.

Hiertoe is het van belang dat het bedrijf expliciet heeft geregeld

- welke relevante wettelijke domeinen er zijn,
- welke functionaris of functionarissen wijzigingen of ontwikkelingen in dit domein volgen en
- wie de wettelijke eisen wijzigingen zonodig doorvertaalt naar maatregelen om te borgen dat ze worden nageleefd.
- wat de verantwoordelijkheden van deze functionarissen zijn.

Een overzicht van wettelijke eisen kan bestaan uit een register met alle relevante wettelijke eisen dat regelmatig wordt geactualiseerd op basis van een hiertoe strekkende procedure. De toewijzing van de verantwoordelijkheid om wijzigingen en ontwikkelingen in bepaalde wettelijke domeinen bij te houden kan bestaan uit een beknopt overzicht met daarin het wettelijke domein (bijvoorbeeld 'milieuwetgeving', of 'Kernenergiewet' met daarachter de naam van degene die verantwoordelijk is om dit domein inhoudelijke te volgen.

Uitgangspunt bij overheidstoezicht én compliance management is het streven naar volledige naleving van wettelijke eisen en voorschriften die op een bedrijf van toepassing zijn.

Bij bedrijven kan het aantal normen groot en de aard en complexiteit uiteenlopend zijn. Sommige mogen nooit, tegen geen enkele prijs worden overtreden (bijvoorbeeld voorschriften die rechtstreeks gericht zijn op het voorkomen van persoonlijk letsel) en vergen maximale borging. Andere mogen ook

niet overtreden worden, maar hebben minder ernstige risico's. In die gevallen moet een optimum worden gezocht (verhouding tussen inspanning en risico).

Daarom dient het bedrijf op basis van een risico analyse vast te stellen welke risico's bestaan, hoe groot de mogelijke effecten hiervan zijn en welke wettelijke eisen bedoeld zijn om deze risico's te beheersen. Het bedrijf dient ervoor te zorgen dat naleving de wettelijke eisen die zijn gerelateerd aan de risico met de meest ernstige effecten het meest gedetailleerd is geborgd. Bij de bepaling van de ernst van de gevolgen moet in elk geval (mede) worden gebaseerd op aspecten die voor de wetgever relevant mogen worden geacht. Op het gebied van industriële activiteiten zijn dat bijvoorbeeld:

- veiligheid
- milieubelasting
- consistentie met overheidsbeleid
- aantasting van reputatie van de sector
- aantasting van de geloofwaardigheid van het openbaar bestuur

Dit betekent bijvoorbeeld dat het naleven van een eis ten aanzien van de uitstoot van kwik expliciet en het meest uitgebreid met procedures en instructies wordt geborgd vanwege het feit dat overtreding hiervan leidt tot ernstige en onomkeerbare milieuschade.

Aanbevolen wordt dat het bedrijf de risico analyse methode en de toepassing hiervan afstemt met het betreffende bevoegde gezag om op voorhand overeenstemming te bereiken over prioriteitstelling en aanpak.

Het systeem wettelijke eisen dient overigens een expliciete koppeling (cross reference) te bevatten tussen de wettelijke eisen en de delen van het managementsysteem waarin de borging is geregeld. Deze koppeling kan bijvoorbeeld bestaan uit het noemen van het vergunningsvoorschrift (bv. voorschrift 3.4) uit de Wet milieubeheervergunning (met eenduidige aanduiding (kenmerk) van de vergunning) waarin staat dat het bedrijf elk jaar een massabalans van afvalstoffen moet verstrekken aan het bevoegd gezag en de procedure (bv. Procedure P03.12) waarin is geregeld wie de massabalans opstelt, hoe hij dit doet en met welke hulpmiddelen, wie de massabalans formeel accordeert en wanneer de massabalans wordt ingediend.

Compliance management vereist een proactieve houding ten aanzien van wettelijke eisen en bevoegd gezag. Mocht het zo zijn dat wettelijke eisen onduidelijk of niet naleefbaar zijn, dan is het van belang dat dit wordt gesignaleerd en besproken met het bevoegd gezag voordat zich problemen voordoen met interpretatie of overtreding van die eisen. Bedrijven met een werkend compliance management systeem wachten dus niet af met onduidelijke of niet naleefbare wettelijke eisen, zetten de overheid voortijdig aan tot verbetering van deze eisen.

3.2 Visie en gedrag

Een belangrijk onderdeel van compliance management is de vraag of het bedrijf een gedragen visie heeft op regelnaleving (compliance) en of deze effectief wordt omgezet in gedrag dat is gericht op compliance.

Een gedragscode kan een goed hulpmiddel zijn. In algemene zin geldt dat hoe concreter de gedragscode is uitgewerkt, des te beter deze ondersteunend werkt op het borgen van compliance. Een voorbeeld hiervan is de gedragscode die in financiële instellingen is ontwikkeld om geschenken aan te nemen.

De gedragscode dient aan te geven dat van de medewerkers een open, proactieve en zelfkritische houding wordt verwacht t.a.v. compliance. Ook dient de gedragscode aan te geven dat van de medewerkers wordt verwacht dat zij zich actief op de hoogte houden van relevante wettelijke eisen. Een ander belangrijk aspect is de betrokkenheid van het management. Indien het management zelf zichtbaar leeft naar de gedragscode en actief is in de bewaking van de naleving ervan, zal dit ook een positief effect hebben op de rest van de organisatie. Dit kan bijvoorbeeld blijken uit het feit dat het

management actief deelneemt aan interne controles en audits of uit het feit dat in MT vergaderingen uitgebreid aandacht wordt besteed aan compliance.

3.3 Kwaliteitsdenken, opleiding, zelfkritische houding en continue verbetering

Kenmerk van het compliance management systeem is dat het kwaliteitsdenken specifiek wordt ingezet voor de borging van naleving van wettelijke eisen.

Een gecertificeerd managementsysteem conform gangbare ISO normen als ISO 9002 of ISO 14001 vormt een goede basis voor een compliance management systeem. De middelen die bij een dergelijk systeem worden ingezet voor het borgen van kwaliteits- of milieudoelen, kunnen in aangepaste vorm kunnen dienen voor het borgen van compliance.

Naast de genoemde ISO normen zijn er nog meer normen die een goede indicatie geven voor de mate waarin de betreffende organisatie het kwaliteitsdenken heeft ingevoerd. Daarom kan in overleg met betrokken overheden en brancheorganisaties ook een ander managementsysteem basis zijn voor een goede score op vraag 3.1.

Het bedrijf dient te hebben geborgd dat medewerkers die een rol spelen bij het naleven van wettelijke eisen door het bedrijf, worden geïnformeerd over wat er van hen op dit gebied wordt verwacht. Dit kan door middel van het toelichten van een procedure of instructie en het evenwel trainen van medewerkers.

Eén van de kenmerken van een bedrijf met een effectief compliance management systeem is een kritische houding ten opzichte van de eigen nalevingsprestatie. Daartoe dient het bedrijf de Deming cirkel van continue verbetering (plan-do-check-act) specifiek toe te passen op het thema compliance. Dit houdt in dat het bedrijf meetbare doelstellingen formuleert ten aanzien van compliance, de nalevingsprestatie planmatig meet tegen deze doelstellingen, eventuele afwijkingen onderzoekt en corrigerende en preventieve maatregelen neemt. De toepassing van dit mechanisme van continue verbetering dient verifieerbaar te zijn in de vorm van rapportages en registraties. Het meten van de nalevingsprestatie kan eventueel worden uitgevoerd door een extern gespecialiseerd bureau, maar kan ook in eigen beheer worden uitgevoerd. Aannemelijk moet zijn dat de meting van de nalevingsprestatie onafhankelijk gebeurt van de verantwoordelijke leidinggevende. Resultaten kunnen worden registreert en gevolgd door middel van een geautomatiseerd systeem.

3.4 Compliance officer en pro-activiteit

Bij een bedrijf met een effectief compliance management ziet een functionaris of een afdeling toe op de naleving binnen de eigen organisatie. Deze functionaris toetst gedragingen en voorzieningen toetsen aan de wettelijke norm, overtreders aanspreken en afwijkingen rapporteren aan het verantwoordelijk management?

Voor de effectiviteit van deze zogenoemde compliance officer of compliance afdeling zijn twee aspecten van belang. Op de eerste plaats dient de compliance officer of compliance afdeling een formele positie te hebben die ervoor zorgt dat hij onafhankelijk van de (lijn)organisatie kan rapporteren aan het (top)management over de nalevingsprestatie. In de praktijk kan deze functie op verschillende manieren worden ingevuld. Op zichzelf is het geen bezwaar als de compliance officer of afdeling ook een adviserende taak heeft voor de (lijn)organisatie, als dit maar niet ten koste gaat van zijn onafhankelijke positie ten opzichte van het toezien op en rapporteren over de nalevingprestatie.

Op de tweede plaats dient de compliance officer te beschikken over de benodigde kennis en ervaring en in de organisatie voldoende aanzien te hebben om zijn rol goed te kunnen spelen.

Bedrijven met een effectief compliance management systeem hebben een proactieve houding ten opzichte van compliance. Dit uit zich onder meer in het actief onderhouden van contacten met het bevoegd gezag over bijvoorbeeld de interpretatie van wettelijke eisen, de naleving van regels, etc.

3.5 Openheid en jaarverslagen

Een open, coöperatieve relatie tussen het bedrijf en het bevoegde gezag heeft een positieve invloed op de naleving. Een bedrijf dat open met de toezichthoudende instantie communiceert over zijn nalevingsprestatie maakt zich kwetsbaar ten opzichte van het bevoegde gezag en wekt – onder voorwaarden- vertrouwen. Enerzijds is dit bevorderlijk voor de relatie en de naleving. Anderzijds loopt het bedrijf het risico dat het bevoegd gezag naar aanleiding van de openheid sancties oplegt voor door het bedrijf zelf gemelde overtredingen.

Van een bedrijf mag worden verwacht dat men open communiceert over de eigen nalevingsprestatie. Van een overheid mag worden verwacht dat proportioneel wordt gereageerd en dat bijvoorbeeld rekening houdt met het zelf melden van overtredingen, onderzoekt welke (repressieve, curatieve en preventieve) maatregelen het bedrijf heeft genomen en haar reactie daarop aanpast. Het ligt voor de hand dat een overheid gepast reageert op een overtreding. In het geval van een pilot in Zeeland zijn hierover afspraken gemaakt tussen bedrijf en bevoegd gezag.

Als de openheid van beide kanten komt, mag van het bedrijf worden verwacht dat het bevoegd gezag volledig wordt geïnformeerd over de nalevingsprestatie.

3.6 Pre-screening medewerkers en disciplinaire maatregelen

Het bedrijf heeft op schrift gesteld welke disciplinaire maatregelen kunnen worden genomen tegen werknemers die willens en wetens wettelijke eisen overtreden.

Tevens heeft het bedrijf duidelijk gemaakt aan werknemers dat het melden van overtredingen van wettelijke eisen verplicht is en dat de melder niet wordt bestraft. Het melden wordt gestimuleerd door bijvoorbeeld een eenvoudige en toegankelijke meldingprocedure, door een snelle en duidelijke terugkoppeling naar de melder en door duidelijk te maken dat de melder niet wordt bestraft voor zijn melding.

Sommige functies bij bedrijven zijn fraudegevoeliger dan andere. Zo zal bij een afvalbedrijf de functie van acceptant kritisch zijn omdat deze doorgaans controleert of de voor acceptatie aangeboden afvalstoffen voldoen aan de eisen. Het bedrijf heeft daarom aantoonbaar bepaald welke fraudegevoelige functies bestaan, hoe ervoor wordt gezorgd dat deze functies worden vervuld door werknemers die integer handelen en geregeld dat op dit integer handelen periodiek wordt gecontroleerd. Deze controle kan er bijvoorbeeld uit bestaan dat in interne audits extra aandacht wordt besteed aan de vervulling van deze functies.

Bijlage 6 Eisen Niveaus Compliance Management

Compliance Management	Criteria
Niveau 1	Bedrijf heeft geen gecertificeerd systeem op basis van ISO14000 of ISO 9001 of op een ander wijze het kwaliteitsdenken aantoonbaar ingevoerd.
Niveau 2	Bedrijf heeft een gecertificeerd systeem op basis van ISO14000 of ISO 9001 of op een ander wijze het kwaliteitsdenken aantoonbaar ingevoerd.
Niveau 3	100% voldoen aan de volgende onderdelen van de vragenlijst*: 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9. - op minimaal 50% van de volgende onderdelen van de vragenlijst voldoen: 1.6, 3.10, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 6.1, 6.2, 6.6, 6.7, 6.8. Om in niveau 3 te blijven moet wel worden voldaan aan de volgende voorwaarden: - Major bevindingen die tijdens jaarlijkse toetsing worden geconstateerd worden zo spoedig mogelijk en uiterlijk binnen drie maanden verholpen. Onder major bevindingen wordt verstaan: een negatieve score op één van de volgende onderdelen van de vragenlijst*: 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 6.1, 6.2, 6.6, 6.7, 6.8 voor zover deze er toe leiden dat niet aan de eisen van de bovengenoemde twee punten wordt voldaan en/of een overtreding op een aspect in de hoogste risicocategorie**. - Minimaal 1x per jaar toetsing van het systeem.
Niveau 4	- Als bij de derde jaarlijkse toetsing blijkt dat aan 100% van de volgende onderdelen van de vragenlijst* wordt voldaan: 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 6.1, 6.2, 6.6, 6.7, 6.8. Om in niveau 4 te blijven moet wel worden voldaan aan de volgende voorwaarden - Major bevindingen die tijdens jaarlijkse toetsing worden geconstateerd worden zo spoedig mogelijk en uiterlijk binnen drie maanden verholpen. Onder major bevindingen wordt verstaan: een negatieve score op één van de volgende onderdelen van de vragenlijst*: 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 6.1, 6.2, 6.6, 6.7, 6.8 en/of een overtreding op een aspect in de hoogste risicocategorie**. - Minimaal 1x per jaar toetsing van het systeem.

* met vragenlijst wordt bedoeld de vragenlijst compliance competence audit (bijlage 4) met de bijbehorende toelichting (bijlage 4).

** dit is maatwerk per bedrijf.

Bijlage 7 Afsprakenmodel systeemgericht toezicht

CM niveau	Toezicht	Repressieve handhaving	
	Wijze van toezicht	Overtredingen die het bedrijf zelf heeft geconstateerd en waarvoor afdoende actie is genomen voor herstel en voorkomen van herhaling	Overtredingen die de Provincie constateert en die het bedrijf niet heeft geconstateerd of die het bedrijf heeft geconstateerd, maar waarvoor geen of onvoldoende actie is genomen voor herstel en voorkomen van herhaling
Niveau 1	Toezicht op output	Bestaande handhavingsstrategie	
Niveau 2	Toezicht op output plus eventueel bottom up systeemgericht toezicht	Bestaande handhavingsstrategie	
Niveau 3	Systeemgericht toezicht. Geleidelijke verschuiving, afhankelijk van ervaring met en vertrouwen in het systeem. Indicatief eindbeeld is ca 50% systeemtoezicht en 50 % toezicht op output	Bestuursrechtelijk optreden niet nodig onder voorwaarde van een adequate aanpak door het bedrijf. De provincie bevestigt de overtreding met vermelding adequate afhandeling bedrijf in een brief.	Sneller bestuursrechtelijk optreden; met een stap minder dan in de huidige handhavingsstrategie. Terugval naar lager CM niveau bij major bevindingen. Afwijkingen van deze afspraak zijn mogelijk, mits onderbouwd.
Niveau 4	Systeemgericht toezicht: indicatief: 80% systeemtoezicht en 20% toezicht op output	Bestuursrechtelijk optreden niet nodig onder voorwaarde van een adequate aanpak door het bedrijf. De provincie bevestigt de overtreding met vermelding adequate afhandeling bedrijf. in een brief .	Sneller bestuursrechtelijk optreden; met een stap minder dan in de huidige handhavingsstrategie. Terugval naar lager CM niveau bij major bevindingen. Afwijkingen van deze afspraak zijn mogelijk, mits onderbouwd.

