Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
Ministerie van Financiën

Vertrouwen geven en in control zijn; En nu doen!

Congresverslag 19 januari 2012

Vertrouwen geven en in control zijn; En nu doen!

Verslag congres op 19 januari 2012

Auteurs:
Martin de Bree (Next Step Management BV / Erasmus Instituut Toezicht & Compliance)
Herman de Bruine (Haagse Hogeschool)
Robert Vos (Directie Begrotingszaken)
René Witte (Directie Begrotingszaken)

Eindredactie:
Robert Vos (Directie Begrotingszaken)

Voorwoord

Voor u ligt de publicatie 'Vertrouwen geven en in control zijn; En nu doen!'. Deze publicatie bevat het verslag van het congres met de gelijkluidende titel dat op 19 januari 2012 op de Rijksacademie voor Financiën, Economie en Bedrijfsvoering (RAFEB) is gehouden.

Deze publicatie is een vervolg op de eerdere publicaties 'Vertrouwen geven en in control zijn; Gaat dat samen?' (april 2009) en 'Vertrouwen geven en in control zijn; Hoe doe je dat? (december 2010).

Allereerst wil ik de dagvoorzitter Wilma de Munck hartelijk danken voor de inspirerende leiding van het congres alsmede de deelnemers voor hun actieve bijdrage. Daarnaast een speciaal woord van dank aan de beide sprekers tijdens het congres die beiden bereid waren hun presentatie te vertalen naar een geschreven tekst voor deze publicatie. In hoofdstuk 2 gaat Martin de Bree in op "Systeemtoezicht: mythes en fabels" en neemt Herman de Bruine ons in hoofdstuk 3 mee in de wereld van "Hoog Betrouwbare Organisaties" (High Reliability Organizations). Beide hoofdstukken worden door Robert Vos afgesloten met een paragraaf waarin specifiek op de relatie tussen deze twee onderwerpen en vertrouwen wordt ingegaan. Daarna geven René Witte en Robert Vos in hoofdstuk 4 een overzicht van de ervaringen met de negen kritische succesfactoren en de vertrouwenscan, zoals die in de forumdiscussie naar voren zijn gekomen. Hierbij danken wij Bert Pruijn (nVWA/interne auditdienst), Hillie Beentjes (Koninklijke Marechaussee/directie Planning & Control), Ad van Ginneken (RWS/dienst Zeeland) en Peter de Barse (Belastingdienst/regio Rijnmond) voor het inbrengen van hun ervaringen als lid van het forum en Marlies Ypma (OCW/interne auditdienst) voor haar schriftelijke inbreng.

In het eerste congres stonden de negen kritische succesfactoren als referentiekader centraal, in het tweede congres de vertrouwenscan als concrete tool (hulpmiddel) en nu in het derde congres de ervaringen met zowel het referentiekader als de tool. Zoals de forumleden op een vraag uit de zaal aan het einde van het congres gezamenlijk zeiden: meer uitgaan van vertrouwen is een kwestie van gewoon doen, maar je moet het wel willen.

Moge deze publicatie (en de twee eerder verschenen publicaties) daartoe een stimulans zijn[1]

Robert Vos

Eindredacteur

1 De twee eerder verschenen publicaties zijn niet meer hardcopy te verkrijgen. Het PDF-bestand van deze boekjes zijn echter wel beschikbaar en op te vragen bij Robert Vos, Ministerie van Financiën (r.o.vos@minfin.nl).

Inhoud

1. Inleiding

Met de brief van 22 december 2004 zond de minister van Financiën het rapport van het 'Interdepartementaal Beleidsonderzoek: Regeldruk en Controletoren' toe aan de Tweede Kamer[2]. Aanleiding voor dit beleidsonderzoek was het idee dat de lasten van beheers- en controlemaatregelen niet opwegen tegen de baten ervan. Als oorzaken hiervan werden aangegeven:

- Complexiteit van regels
- Stapeling van regels
- Te weinig bewuste inschatting van risico's bij beheersingsmaatregelen en controle
- Stapeling van control(e)s

In dit rapport werden o.a. de volgende voorstellen gedaan:

- Doorlichting van regels, gericht op reductie
- Uitgaan van de verantwoordelijkheid van het management voor de interne beheersing die nodig is voor een efficiënte, effectieve en rechtmatige doelrealisatie
- Meer uitgaan van risicoanalyse. Beheersmaatregelen en controle-inspanningen daarop richten (meer ruimte voor differentiatie op basis van bewuste keuzes)
- Eenmaal controleren en daar (binnen randvoorwaarden) op vertrouwen (single audit)

In het kader van de doelstelling van vermindering van de regeldruk en controletoren is directie Begrotingszaken in 2009 gestart met het project 'Vertrouwen geven, maar toch in control zijn'. Daarbij staat de vraag centraal: onder welke voorwaarden kan je meer uitgaan van vertrouwen (en dus komen tot lagere controle kosten en een plezierigere werksfeer), en toch in control zijn (omdat er sprake is van gerechtvaardigd vertrouwen). Dit project sluit nauw aan bij de doelstelling van de activiteiten in IOFEZ verband in het kader van 'Minder gedoe'.

In het kader van dit project is allereerst op basis van bestudering van de wetenschappelijke literatuur een referentiekader ontwikkeld voor 'vertrouwen geven, maar toch in control zijn': de negen kritische succesfactoren. In de publicatie 'Vertrouwen geven en in control zijn; Gaat dat samen?' (april 2009) worden de negen kritische succesfactoren uitvoerig toegelicht. Op het congres van 25 juni 2009 waarin deze eerste publicatie gepresenteerd werd, bleek een grote behoefte te bestaan aan het verder uitwerken van dit referentiekader in een concrete tool. Dit is de aanleiding geweest voor de tweede publicatie 'Vertrouwen geven en in control zijn; Hoe doe je dat? (december 2010) en het gelijknamige congres op 19 december 2010, waarin de vertrouwenscan als tool gepresenteerd werd. Het afgelopen jaar kwamen veel vragen binnen over ervaringen met het toepassen van de vertrouwenscan. Dit is aanleiding geweest voor het organiseren van een derde congres met als titel 'Vertrouwen geven en in control zijn; En nu doen! Tijdens dit congres zijn uitvoerig de ervaringen belicht van vier organisaties[3] die gebruik gemaakt hebben van het referentiekader van de negen kritische succesfactoren en de vertrouwenscan. Tevens werd op dit congres aandacht besteed aan systeemtoezicht en hoog betrouwbaar organiseren in relatie tot vertrouwen. In deze derde publicatie treft u een impressie aan van dit congres op basis van de verschillende bijdragen, met enige aanvullingen om tot een compleet beeld te komen.

2 Tweede Kamer, vergaderjaar 2004-2005, 29 950, nr. 1

3 De Interne Auditdienst van OCW was door omstandigheden verhinderd. De ervaringen van OCW zijn in hoofdstuk 4 wel opgenomen op basis van een schriftelijke inbreng.

2. Systeemtoezicht en vertrouwen

a. Systeemtoezicht, mythen en fabels (M.A. de Bree)

Inleiding

Veel bedrijven die onder toezicht staan gebruiken managementsystemen waarmee zij hun processen beheersen. Systeemtoezicht is een vorm van toezicht waarbij de toezichthouder inspeelt op deze managementsystemen met als doel bedrijven te stimuleren hun managementsysteem in te zetten voor het beheersen van maatschappelijke risico's en regelnaleving.
De ervaringen die ik hier presenteer zijn gebaseerd op het systeemtoezicht dat provincies momenteel toepassen op milieuregels die gelden voor chemische bedrijven. De Provincie Noord-Brabant heeft een belangrijke rol gespeeld bij het ontwikkelen van deze vorm van systeemtoezicht[4] en heeft hiermee in 2010 de Trofee Vernieuwing Toezicht gewonnen.

Aan de hand van zeven mythen en fabels leid ik u door systeemtoezicht heen.

Mythe 1: Certificaten stellen niets voor

Een certificaat heeft net zoveel waarde als de eisen die aan de kandidaat certificaathouder worden gesteld en de kwaliteit van de certificeringsaudit. Bij systeemtoezicht worden de systeemeisen door de overheid zelf bepaald en wordt de audit 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 de regelnaleving. Deze eisen hebben betrekking op allerlei verschillende onderdelen van het (compliance) managementsysteem waarbij het zowel gaat om de aanwezigheid en de doelmatigheid van systeemonderdelen (zoals procedures en instructies), als om de implementatie hiervan (werkt het bedrijf volgens deze procedures en levert dit in de praktijk de vereiste resultaten op?).
Als een bedrijf aan de systeemeisen voldoet, krijgt het van de overheid geen certificaat, maar wordt het in een categorie geplaatst die recht geeft op aangepast toezicht (hierover later meer). De audits worden uitgevoerd door overheidstoezichthouders die zijn getraind in auditen en kennis hebben van de inhoud, zodat zij ook bij een audit de diepte in kunnen gaan.

Mythe 2: Systeemtoezicht is alleen maar papieren controle

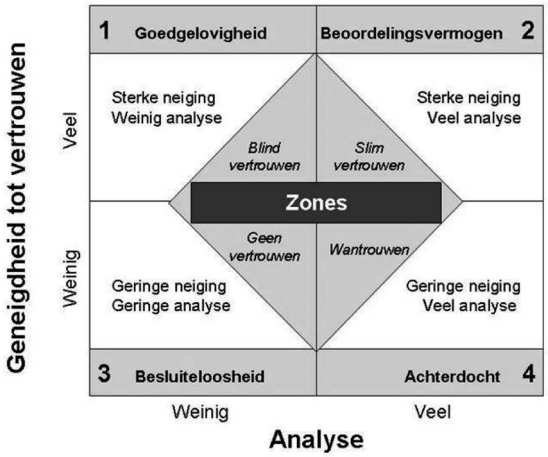
Bij systeemtoezicht worden altijd controles op procedures, instructies, interne controlemaatregelen gecombineerd met toezicht op de output. Er wordt dus zowel naar het managementsysteem gekeken als naar de fysieke resultaten zoals of er veilig wordt gewerkt, of de emissies voldoen aan de norm etc. In de toezichtwereld is er brede consensus dat toezicht nooit alleen maar kan bestaan uit het controleren van de 'papieren werkelijkheid'. Er zullen altijd steekproeven noodzakelijk zijn om te verifiëren of het systeem de vereiste resultaten oplevert. Bij systeemtoezicht worden deze zogenoemde 'outputcontroles' tevens gebruikt om te verifiëren of de eigen controles die het bedrijf in het kader van haar compliance managementsysteem (CMS) uitvoert, een juist beeld geven van de werkelijkheid.

4 *Zie www.brabant.nl/systeemtoezicht*

Mythe 3: Systeemtoezicht gaat uit van blind vertrouwen

Vertrouwen speelt bij systeemtoezicht een belangrijke rol. Covey maakt onderscheid in vertrouwen gebaseerd op weinig analyse ('blind vertrouwen') en vertrouwen gebaseerd op veel analyse ('slim vertrouwen'). Bij systeemtoezicht passen we geen blind vertrouwen toe, maar gerechtvaardigd vertrouwen. Met andere woorden, voordat vertrouwen door de toezichthouder kan worden gegeven, moet er eerst informatie zijn waaruit de conclusie kan worden getrokken dat dit vertrouwen gerechtvaardigd is.

Figuur 1 Vertrouwensmatrix (Covey, 2009)



Pas als we weten dat het onder toezicht staande bedrijf laat zien dat hij het vertrouwen waard is, kan er ruimte worden gegeven. Dat is gemakkelijker gezegd dan gedaan, want hoe bepaal je nu als toezichthouder precies of een bedrijf het vertrouwen verdient?

Benninga (2007) stelt dat vertrouwen is gebaseerd op vier factoren, te weten betrouwbaarheid, kwaliteit van de relatie, geloofwaardigheid en zelfreflectie (zie onderstaande formule).

$$\text{Vertrouwen} = \frac{\text{betrouwbaarheid} \times \text{kwaliteit van de relatie} \times \text{geloofwaardigheid}}{\text{zelfingenomenheid}}$$

Betrouwbaarheid = afspraak is afspraak
Kwaliteit van de relatie = open, prettig, kwetsbaar
Geloofwaardigheid = kennis, competenties
Zelfingenomenheid = gebrek aan zelfreflectie

Bron: Benninga, 2007

De vier elementen die Benninga (2007) noemt zijn bij systeemtoezicht vertaald in eisen aan compliance management systemen van bedrijven. Hierdoor ontstaat een beoordelingsgrondslag voor de compliance management systemen die generiek is, met andere woorden die in elk willekeurig domein kan worden toegepast. In onderstaande tabel zijn deze systeemeisen opgesomd.

Tabel 1 Van elementen van vertrouwen naar systeemeisen (IVW, 2008)

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

De in tabel 1 genoemde systeemeisen zijn verder uitgewerkt in een auditsystematiek waarbij op basis van een checklist het compliance management systeem wordt beoordeeld. Weliswaar is vertrouwen uitgangspunt bij systeemtoezicht, maar dit vertrouwen is gebaseerd op een doordachte en grondige analyse van de opzet en werking van het compliance management systeem. Hoe beter dit compliance management systeem werkt, des te meer vertrouwen.

Het is goed op te merken dat vertrouwen een tweezijdig fenomeen is, met andere woorden, het is een kenmerk van een relatie tussen twee partijen, in dit geval tussen toezichthouder en bedrijf. Dat betekent dat niet alleen het vertrouwen van de toezichthouder in het bedrijf een belangrijk aspect is, maar ook het omgekeerde. Als het bedrijf niet voldoende vertrouwen heeft in de toezichthouder, zal het bedrijf terughoudend zijn met het verstrekken van gevoelige informatie, die weer nodig is voor de toezichthouder om goed te kunnen beoordelen of het bedrijf voldoende kritisch is t.a.v. de eigen processen en prestatie en voldoende lering trekt uit gemaakte fouten.
Vertrouwen speelt bij systeemtoezicht op twee manieren een rol:

1. Als randvoorwaarde om te komen tot een zinvolle uitwisseling van informatie zodat een goed beeld kan worden gevormd van de mate van beheersing door het onder toezicht staande bedrijf;
2. Als product doordat bij systeemtoezicht *van twee kanten* invulling wordt gegeven aan de vier factoren die een vertrouwensrelatie kenmerken.

Mythe 4: Met systeemtoezicht krijgen bedrijven veel teveel vrijheid

Bij systeemtoezicht wordt het bedrijf ingedeeld in één van vier niveaus.

1. Op het eerste niveau bevinden zich bedrijven die geen managementsysteem van betekenis hebben. Dit hoeft niet te betekenen dat deze bedrijven slechte nalevers zijn, maar wel dat de naleving niet geborgd is in een managementsysteem.
2. Op het tweede niveau bevinden zich bedrijven die wel beschikken over een – al dan niet gecertificeerd – managementsysteem, maar dit systeem voldoet nog niet aan de eisen die de overheid stelt aan een compliance management systeem. Omdat deze bedrijven wel de potentie hebben om binnen afzienbare tijd een dergelijk compliance

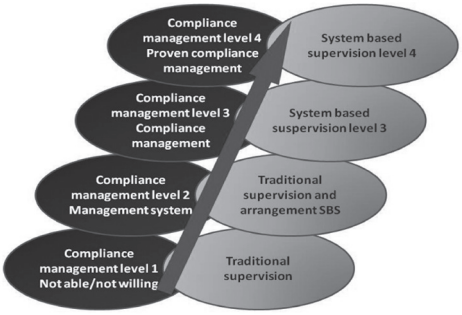
management systeem op te zetten, maakt de overheid afspraken met deze bedrijven om naar het derde niveau te groeien.

3. Op het derde niveau bevinden zich bedrijven die een goed werkend compliance management systeem hebben. Pas op dit niveau wordt het toezicht aangepast, namelijk door minder outputcontroles te doen en terughoudend te zijn met sancties. Wel wordt het compliance management systeem jaarlijks beoordeeld.
4. Als deze bedrijven aan een aantal aanvullende eisen voldoen en het compliance management systeem gedurende twee jaar op orde houden, komen zij in aanmerking voor het vierde niveau. Op dit niveau worden de outputcontroles verder teruggebracht tot een niveau van steekproeven. Ook hier wordt het compliance management systeem jaarlijks beoordeeld.

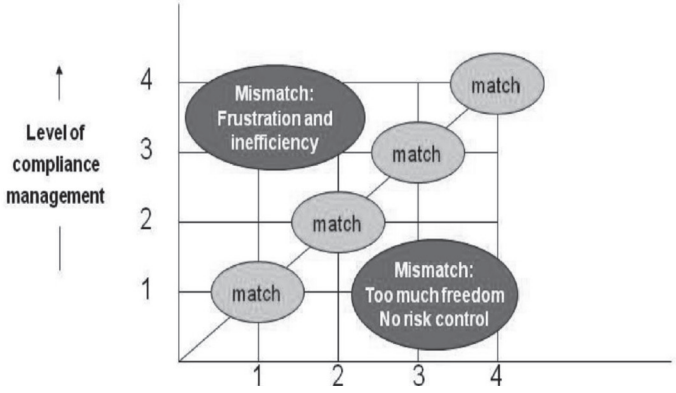
Deze werkwijze geeft de overheid de mogelijkheid om bedrijven te stimuleren structureel de naleving van regels in hun organisatie te borgen. De ervaring is dat dit o.a. leidt tot verbetering van het risicomanagement en het borgen van regelnaleving door de bedrijven.

Alleen bedrijven die hun zaakjes aantoonbaar goed voor elkaar hebben, komen dus voor aangepast toezicht in aanmerking. In figuur 2 zijn de vier niveaus van compliance management weergegeven.

Figuur 2 Niveaus compliance management met hieraan aangepast toezicht.



Figuur 3 Niveaus compliance management: match en mismatch systeemtoezicht.



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

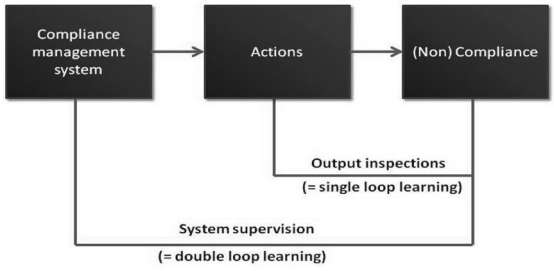
Als een bedrijf een goed werkend managementsysteem heeft dat bv. voldoet aan gangbare normen als ISO 9001, 14001 of OHSAS 18001, dan is al een groot deel van de functionaliteit van een effectief compliance management systeem aanwezig. Met een klein aantal specifieke uitbreidingen kan doorgaans (dan) al een goed werkend compliance management systeem worden gerealiseerd. Hierbij wordt dus in grote mate gebruik gemaakt van bestaande managementsystemen van bedrijven.
Het is wel zo dat de overheid met andere ogen naar managementsystemen kijkt dan de certificerende instellingen. Het gaat er bij de overheid met name om kritisch vast te stellen in hoeverre het bedrijf ervoor zorgt dat de maatschappelijke risico's worden beheerst en de regelnaleving wordt geborgd. Dit kan betekenen dat een gecertificeerd bedrijf, ondanks het certificaat, haar managementsysteem moet verbeteren om te voldoen aan de eisen die de overheid stelt.

Mythe 6: Systeemtoezicht is dé oplossing voor alle problemen

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 werkend compliance management systeem hebben. Systeemtoezicht kan in principe op twee manieren bijdragen aan effectief en efficiënt toezicht.

a. Door middel van systeemtoezicht kan het toezicht worden afgestemd op het niveau van intrinsieke beheersing door het onder toezicht staande bedrijf. Hierdoor wordt het toezicht in feite aangepast aan het niveau van restrisico nadat dit is vastgesteld door middel van het beoordelen van het compliance management systeem. Op deze manier worden er geen onnodige controles uitgevoerd en kan de toezichtcapaciteit worden geconcentreerd op die bedrijven die meer toezicht nodig hebben.
b. Misschien wel het grootste voordeel van systeemtoezicht, mits toegepast onder de juiste condities, is dat met systeemtoezicht een leerprikkel kan worden gegeven aan het onder toezicht staande bedrijf om de interne beheersing te verbeteren. Doordat systeemtoezicht ingrijpt op systeemniveau kan een meer fundamentele vorm van leren worden bewerkstelligd dan wanneer alleen incidentele overtredingen zouden worden aangepakt. Hierdoor verbetert het compliance management systeem met een betere risicobeheersing en regelnaleving door het bedrijf als resultaat. Dit 'double loop learning' wordt geïllustreerd in figuur 3.

Figuur 3 Single en double loop learning bij (systeem)toezicht



Al eerder is opgemerkt dat vertrouwen een tweezijdig fenomeen is. Het leereffect van systeemtoezicht treedt alleen op als de overheidstoezichthouder in zijn wereldbeeld ook de mogelijkheid kent van bedrijven die bereid zijn om hun maatschappelijke verantwoordelijkheid te nemen. Als de overheidstoezichthouder uitgaat van de veronderstelling dat bedrijven in dit opzicht per definitie niet te vertrouwen zijn, zal de toezichthouder bedrijven die acteren op het derde en vierde niveau van het model in figuur 2, niet als zodanig (h)erkennen en wordt zijn wereldbeeld de beperkende factor die het leren in de weg staat. Het is niet alleen van belang dat de individuele toezichthouder deze mogelijkheid open houdt, maar dat ook de toezichthoudende organisatie waarvan hij deel uitmaakt, dit in haar beleid onderkent.

Mythe 7: Systeemtoezicht garandeert dat er nooit meer iets mis zal gaan

In een complexe wereld bestaat geen 100% garantie dat er nooit iets mis zal gaan of dat niet incidenteel een regel wordt overtreden. Met het toepassen van systeemtoezicht beoogt de overheid bedrijven aan te sporen om de maatschappelijke risico's zo goed mogelijk te beheersen en de naleving van wettelijke eisen te borgen. Een incidentele overtreding betekent dus niet perse dat het compliance managementsysteem niet goed functioneert, maar wel dat er goed moet worden gekeken naar de structurele oorzaken zodat hiervan kan worden geleerd om de risico's op herhaling te verkleinen.

b. Relatie systeemtoezicht en vertrouwen (R.O. Vos)

Bij systeemtoezicht vertrouw je zoals hierboven door de Bree is betoogd op de betrouwbaarheid van het aanwezige management control systeem. Dit betekent geen blind vertrouwen (vertrouwen zonder controle), integendeel: systeemtoezicht kan niet zonder 'reality checks' om de werking van het management controlsysteem te kunnen beoordelen. Het tweede punt dat de Bree aangeeft is dat systeemtoezicht een bepaald volwassenheidsniveau van de organisatie veronderstelt : minimaal niveau 3 (in figuur 2 van de Bree).

Er is een duidelijke relatie tussen dit volwassenheidsniveau en het voldoen aan de negen kritische succesfactoren (KSF) zoals die als referentiekader geformuleerd zijn voor 'vertrouwen geven en in control zijn'. Hieronder worden de belangrijkste eisen voor systeemtoezicht, zoals die naar voren komen in de presentatie van de Bree, gepresenteerd aan de hand van de indeling van de negen kritische succesfactoren:

- Duidelijkheid omtrent verwachtingen (KSF 1)

Systeemtoezicht draait om de verwachting dat de andere partij de regels - vertaald naar procedures, instructies en interne controle maatregelen - ook daadwerkelijk naleeft. Vandaar dat in het presentatie van de Bree de werking van het compliance management systeem (CMS) centraal staat.

- Deskundigheid (KSF 2)

Bij deskundigheid gaat het om de kwaliteit van het compliance managementsysteem. De Bree geeft aan dat organisaties vanaf niveau 3 (figuur 2) zich kwalificeren voor systeemtoezicht. Het is belangrijk ook bij deze organisaties jaarlijks de kwaliteit van het compliance managementsysteem te beoordelen om daadwerkelijk vast te stellen dat de kwaliteit op het vereiste niveau blijft

- Gemeenschappelijk belang (KSF 3)

Essentie van systeemtoezicht is dat het managementsysteem control systeem van de organisatie en dan in het bijzonder het compliance gedeelte, tevens gebruikt wordt voor het beheersen van maatschappelijke risico's en regelnaleving. Dit zal alleen goed werken indien ook de organisatie voldoende belang heeft bij het beheersen van maatschappelijke risico's en het borgen van de regelnaleving. Dan is het een efficiënte en prettige manier van met elkaar omgaan. Hoe minder de organisatie het beheersen van maatschappelijke risico's en regelnaleving als zijn belang ziet, hoe groter de kans is dat de betrouwbaarheid van het compliance management systeem in dat opzicht maar matig is.[5]

- Goed gevoel (KSF 4)

Vertrouwen is een tweezijdig fenomeen. Het staat voor de kwaliteit van de relatie: open, prettig, kwetsbaar (Benninga, 2007). Voor de toezichthouder dragen positieve ervaringen en openheid in de communicatie in belangrijke mate bij aan een goed gevoel ten aanzien van de organisatie, maar ook de organisatie zal een goed gevoel bij de toezichthouder moeten hebben (zie hieronder).

- Open informatie-uitwisseling (KSF 5)

De toezichthouder heeft informatie nodig om de conclusie te kunnen trekken dat het vertrouwen gerechtvaardigd is. Als de organisatie niet voldoende vertrouwen heeft in de toezichthouder, zal het terughoudend zijn met het verstrekken van goede informatie. Een zinvolle uitwisseling van informatie is voor de toezichthouder van groot belang, in het bijzonder openheid over resultaatafwijkingen: rapportage van afwijkingen, overtredingen en werking systeem (IVW, 2008). Om deze informatie te kunnen ontvangen, zal de toezichthouder moeten investeren in de relatie door zelf ook aanspreekbaar en betrouwbaar te zijn.

- Inzicht in risico's en risicoacceptatie (KSF 6)

Randvoorwaarde voor systeemtoezicht is een goed beeld van de mate van risicobeheersing door de organisatie. Het gaat dan in het bijzonder om inzicht die nodig is om goed te kunnen beoordelen of de organisatie voldoende kritisch is ten aanzien van de eigen processen en prestaties en leert van fouten. Er bestaat geen 100% garantie dat er nooit iets mis zal gaan of dat niet incidenteel een regel wordt overtreden. Vertrouwen geven betekent per definitie een bepaalde mate van risico-acceptatie. Daarbij geldt dat het niveau van risico dat men accepteert (bijvoorbeeld 3% fouten) hoger moet liggen dan het ingeschatte niveau van risico (bijvoorbeeld 2%). Ligt dit andersom dan zal men in het algemeen door extra maatregelen en/of controles het niveau van het (rest)risico zodanig omlaag proberen te brengen dat het wel beneden het niveau van risico-acceptatie komt te liggen. Accepteert men geen enkel risico (zero tolerance) dan is er geen ruimte om te werken met vertrouwen.

5 Dit komt ook duidelijk naar voren in het artikel 'Voor wie of wat is systeemtoezicht zinvol?' van Honingh en Helderman (2010): de sectoren luchtvaart en sector delfstoffenwinning komen met afstand als beste uit de bus. De onderzoekers schrijven dit met name toe aan het feit dat die sectoren- naast dat ook de veiligheid van eigen medewerkers in het geding is- minder mogelijkheden hebben om risico's op andere partijen af te wentelen, fouten te verbloemen of te discussiëren over (subjectieve) normen. Bij de andere onderzochte sectoren (vleesverwerkende industrie/vleesketen, financiële dienstverlening, voor- en vroeg- schoolse educatie en de kwaliteitsbeoordeling in de zorgsector/certificatie in de geestelijke gezondheidszorg) zijn de condities in de ogen van de onderzoekers minder gunstig.

- Mogen controleren (KSF 7)

Bij systeemtoezicht worden altijd controles op procedures, instructies, interne controlemaatregelen gecombineerd met toezicht op de output. Systeemtoezicht kan nooit alleen bestaan uit het controleren van de 'papieren werkelijkheid'. Er zullen altijd steekproeven ('reality checks') noodzakelijk zijn om te verifiëren of het systeem de vereiste resultaten oplevert. Bij systeemtoezicht worden deze zogenoemde 'outputcontroles' tevens gebruikt om te verifiëren of de eigen controles die de organisatie in het kader van haar compliance managementsysteem uitvoert, een juist beeld geven van de werkelijkheid. Door middel van systeemtoezicht kan de omvang van de controle worden afgestemd op het niveau van intrinsieke beheersing door het onder toezicht staande bedrijf. Hierdoor wordt het aantal controles in feite aangepast aan het niveau van restrisico nadat dit is vastgesteld door middel van het beoordelen van het compliance managementsysteem. Op deze manier worden er geen onnodige controles uitgevoerd en kan de toezichtcapaciteit worden geconcentreerd op die organisaties die meer toezicht nodig hebben.

- Bespreken incidenten en leren (KSF 8)

Een incidentele overtreding betekent niet per se dat het compliance managementsysteem niet goed functioneert, maar wel dat er goed moet worden gekeken of hier geen structurele oorzaken aan ten grondslag liggen. Het is belangrijk van incidenten te leren om de kans op herhaling te verkleinen. Dit betekent dus niet na een incident direct vervallen in een 'Pavlov-reactie' van meer controle, maar eerst het incident bespreken en analyseren. Er zal wel voldoende lering getrokken moeten worden uit de incidenten die zich hebben voorgedaan. Want als er te veel incidenten (blijven) plaatsvinden, zal vroeger of later het vertrouwen alsnog verdwijnen.

- Consequenties (sancties) bij te veel of bewuste inbreuken (KSF 9)

Als er veel of bewuste inbreuken plaatsvinden zal dit niet zonder gevolgen kunnen blijven. Systeemtoezicht kan dan niet aan de orde zijn. Er zal dan een terugval naar traditioneel toezicht dienen plaats te vinden. Dat is dan niveau 1 in figuur 2 (niet kunnen/niet willen). Vertrouwen/systeemtoezicht is letterlijk en figuurlijk iets dat men moet verdienen: het is niet gratis of vrijblijvend.

Overall-conclusie:
De eisen die de Bree in zijn presentatie stelt aan systeemtoezicht, zijn goed te vertalen naar de negen kritische succesfactoren voor vertrouwen.

3. Omgaan met risico's

a. Hoog betrouwbare organisaties ('High Reliability Organizations') (H. de Bruine)

- Waar komt hoog betrouwbaar organiseren vandaan

Eind jaren '70 van de vorige eeuw dreigt een incident bij een kerncentrale in Harrisburg (Three Mile Island) te ontaarden in een nucleaire ramp. Wat is er aan de hand? Juist kernenergie is een sector waarin veel systemen operationeel zijn om te voorkomen dat er ongelukken gebeuren. Gekoppeld aan regulering en toezicht zouden ongelukken niet moeten (kunnen) plaatsvinden. Dan gaat er toch iets fout, waar ligt dan de oorzaak?

Eerste reactie is dan vaak: dat ligt aan een menselijke fout (iemand heeft onterecht een klep open laten staan). Deze reactie was voor de Amerikaan Charles Perrow (1999) reden om meer van dit soort ongelukken te onderzoeken. Zijn conclusie was dat technologie tegenwoordig zo ingewikkeld is, dat niemand meer precies weet hoe het zit. Allerlei veiligheidssystemen, onverwachte en ongeplande afhankelijkheden maken het (bijna) onmogelijk te voorspellen, wat er precies in een kerncentrale gebeurt.

Doordat kleine foutjes worden gecorrigeerd door ingebouwde systemen en daarmee de veerkracht van een systeem wordt ondergraven, bestaat de mogelijkheid dat door samenloop van omstandigheden het risico op een omvangrijke ramp eigenlijk alleen maar groter wordt. Perrow's stelling was dat bij sommige vormen van technologie zoals kernenergie en kernwapens ongelukken daarom 'normaal' zijn en het verstandiger is om niet meer van deze technologie gebruik te maken. Deze vormen van technologie zijn immers niet te vertrouwen.

Een onderzoeksgroep in Californie heeft zich toen de vraag gesteld hoe het komt dat er niet veel meer rampen met kerncentrales (en gelijksoortige organisaties met ingewikkelde technologie) optreden. Dit onderzoek vond plaats in organisaties waarvan Perrow aangaf dat de kans op ongelukken groot was, zoals kerncentrales, vliegdekschepen en luchtverkeersleiding. Hun onderzoek werd gedaan op het moment dat het (nog) goed ging in de betreffende organisaties.

De eerste uitkomsten van dit onderzoek gaven het volgende beeld van succesvolle organisaties. Deze organisaties noemden ze hoog betrouwbare organisaties (High Reliability Organizations).

- Kenmerken van hoog betrouwbare organisaties (HRO's)

HRO's worden gekenmerkt door een hoge mate van vakmanschap, discipline, vertrouwd leiderschap en heldere standaarden waar medewerkers echt wat aan hebben in de praktijk. Als er iets moeilijks of ingewikkelds is, zijn ze goed in staat om besluiten te nemen met gebruik van relevante deskundigheid op het juiste niveau in de organisatie en procedures aan te passen naar bevind van zaken. Tenslotte realiseren hun medewerkers zich wat hun bijdrage aan het geheel is.

Onderin het vliegdekschip realiseert een monteur zich dat als hij buizen niet goed op elkaar aansluit, de kerosine levering aan vliegtuigen in gevaar komt. Vliegtuigen kunnen niet meer vliegen en het vliegdekschip heeft geen nut meer.

Dit soort organisaties houdt kort gezegd van routine, structuur en orde, of zoals in het gevangeniswezen wordt genoemd: Rust, Reinheid en Regelmaat.

Toch is dit niet genoeg. Er zijn altijd dingen die niet te voorzien of te voorspellen zijn. Er zijn altijd situaties waar niet aan gedacht is en die daarom niet in de regelgeving verwerkt zijn. Het gaat er dan om snel te signaleren dat zaken anders lopen dan gedacht of verwacht en hier adequaat op te reageren.

Als een monteur een sleutel verliest op het vliegdek, dan wordt het hele start- en landingsproces stilgelegd[6]*. Want als zo'n sleutel wordt opgezogen in een straalmotor kan dit behoorlijke schade of erger veroorzaken.*

Het ongeluk dat het einde van de Concorde betekende, werd veroorzaakt doordat een metalen beugel op de startbaan een lekke band veroorzaakte[7].

Op een vliegdekschip wordt daarom de monteur die meldt dat hij een sleutel heeft laten vallen en niet heeft teruggevonden, naar voren geroepen om in het openbaar gecomplimenteerd te worden.

Werner von Braun stuurde een fles champagne naar een ingenieur die, toen een lancering van een Redstone-raket mislukte, aangaf dat hij dit wellicht had veroorzaakt door kortsluiting te veroorzaken bij een prelan-ceringstest. Onderzoek gaf aan dat dit inderdaad de oorzaak van het ongeluk was; de bekentenis betekende dat een duur herontwerp niet nodig was.

Daarnaast zijn medewerkers in staat om te handelen als er iets onverwachts gebeurt, iets te improviseren met wat voor handen is. De instelling van de medewerker is daarbij de cruciale factor.

Het niet opvangen van zwakke signalen en gebrek aan veerkracht is de verklaring voor de tal van ongelukken. Denk hierbij ook aan Cools (2005): 'Niet slechte formele corporate go-vernance, maar zonnekoninggedrag van CEO's, hebzucht en geloof in luchtkastelen waren de werkelijke oorzaken van de grote fraudeschandalen'.

- Denken vanuit de werkelijkheid als een ijsberg: opmerkzaam zijn voor wat zich onder de waterlijn bevindt

Achtergrond van deze wijze van kijken van HRO's naar organisaties is de 'ijsberg' van het systeemdenken[8]. Onder wat we waarnemen aan gebeurtenissen zitten patronen en ontwikkelingen die deze aankondigen. Deze patronen worden veroorzaakt door systemen en interactiepatronen die hun grond weer vinden in de mentale modellen die bepalen hoe mensen denken. We kunnen prachtige systemen maken die waarschuwingssignalen afgeven, maar de vraag is of we deze wel serieus nemen of nog erger wegredeneren.

De instelling die HRO's hebben om zwakke signalen op te vangen en veerkrachtig te reage-ren, wordt door Weick en Sutcliffe (2011) opmerkzaamheid genoemd.

- Hoe ziet opmerkzaamheid er uit: het vliegdekschip

Het begrip opmerkzaamheid en het gedrag dat daarbij hoort wordt hieronder geïllustreerd aan de hand van een vliegdekschip. Eerst een beeld van het werk op een vliegdekschip.

6 Alle voorbeelden (tenzij anders aangegeven) van HRO's zijn ontleend aan Karl E. Weick en Kathleen M. Sutcliffe (2011) Management van het Onver-wachte, BBNC, Rotterdam

7 Het ongeluk met de Concorde (25 juli 2000) kende twee oorzaken: een ontwerpfout en een metalen beugel op de startbaan (Volkskrant 14 december 2004)

8 Zie bijvoorbeeld Bill Bryan, Michael Goodman, Jaap Schaveling (2006) Systeemdenken, ontdekken van organisatiepatronen, Academic Service, Den Haag

Stelt u zich een drukke dag voor op Schiphol dat nog één landingsbaan, vliegtuigtrap en uitgang beschikbaar heeft. Zorg dat vliegtuigen tegelijkertijd opstijgen en landen, in de helft van de tijd die er nu voor staat, beweeg de landingsbaan heen en weer en op en neer, en verplicht een ieder die opstijgt dezelfde dag weer te landen. Laat de vliegtuigen op het randje van hun kunnen vliegen. Zet dan de radar uit om detectie te voorkomen, beperk het radioverkeer zoveel mogelijk, tank de vliegtuigen op het dek met "ronkende" motoren, een vijand in de lucht en her en der bommen en raketten op het dek. Drenk alles in zeewater en olie, en beman het geheel met twintigjarigen, waarvan de helft nog niet eerder een vliegtuig van dichtbij heeft gezien. Tussen haakjes: er mogen geen doden vallen.

(ontleend aan Weick & Sutcliffe)

Dit beeld is wellicht wat overtrokken, maar u kunt zich voorstellen dat landen en opstijgen van vliegtuigen een proces is waar niets fout mag gaan "Failure is not an option".[9] Om dit goed te laten verlopen begint het ermee dat het vliegtuig geen gas terugneemt, maar juist vol gas de landing uitvoert. Dit is noodzakelijk om dat als er iets fout gaat, het vliegtuig een doorstart kan maken en niet in zee terecht komt. In HRO termen: toegewijd aan veerkracht, mocht er iets fout gaan dan hebben we de mogelijkheid te corrigeren. Elke landingspoging wordt scherp bewaakt door zogenaamde Landing Signal Officers (LSO's). Deze bewaken of de landing goed wordt ingezet, mocht het vliegtuig teveel afwijken van wat nodig is voor een veilige landing dan stuurt de LSO de piloot door en moet deze de landing opnieuw inzetten. Daarbij wordt er ook opgelet of de piloot in de communicatie wel alert genoeg reageert. In HRO termen: gerichtheid op verstoringen. Er wordt daarbij niet gedacht: 'De piloot heeft het al zo vaak gedaan, dat zal ook nu wel goed gaan, de vorige keer ging het toch ook goed'. Elke landing en elke piloot wordt kritisch gevolgd ('hij kan een slechte dag hebben'). In termen van HRO: terughoudendheid tot simplificeren. Ook wordt elke landing met de piloot nabesproken. HRO's besteden veel tijd aan het onderzoeken/evalueren van gebeurtenissen en zijn behoedzaam met hun ervaringen: is de context inmiddels niet veranderd, zijn onze aannames nog steeds juist? Kenmerkend is ook hun gevoeligheid voor de uitvoering. Is de piloot wel voldoende bij de les of eigenlijk met zijn gedachte bij iets anders. Let iedereen wel op of worden ze afgeleid. Het laatste kenmerk is hun respect voor deskundigheid. Het besluit om een piloot 'af te vlaggen' en daarmee zijn landing af te breken en het opnieuw te laten uitvoeren wordt genomen door de Landing Signal Officers (LSO's). De LSO's staan lager in de hiërarchie dan de coördinator, maar de coördinator vlagt af omdat de LSO, die in een betere positie staat om het te beoordelen, het zegt.

- Maar er gaat ook weleens wat fout …

Ook op een vliegdekschip gaat weleens wat fout. Mislukt een lancering. Een fenomeen dat daarbij kan optreden is dat de piloot zo druk

9 De hierna volgende beschrijving en stills zijn ontleend aan de Discovery Channel documentaire Carrier, Fortress at Sea uit 1995.

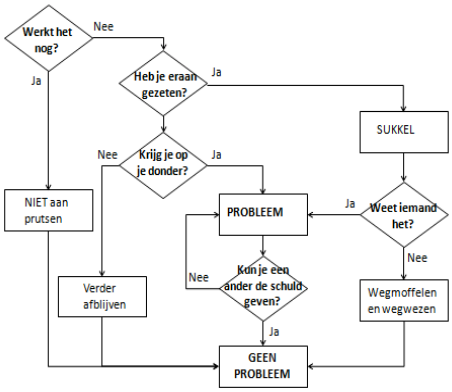
bezig is het vliegtuig in de lucht te houden dat hij er niet aan denkt om zijn schietstoel te gebruiken. Het kan dan gebeuren dat hij de schietstoel pas gebruikt, omdat anderen vanaf het vliegdek het hem hebben staan toeschreeuwen dat hij moet springen. De piloot wil niet dood, maar 'I was so busy flying the aircraft, that I wasn't interested in ejecting at the time', een vorm van tunnelvisie. Dit fenomeen kan, gelukkig met minder heftige gevolgen, ook in andere organisaties plaatsvinden. De mens is feilbaar. De vraag is hoe gaan we hiermee om? Onfeilbaarheid vragen is onmenselijk. We hebben allemaal onze blinde vlekken, we kunnen afgeleid zijn, we hebben elkaar daarom nodig om elkaar scherp te houden. Er is een cultuur nodig waarin mensen aanspreekbaar zijn, als ze wat fout doen en dat er wat van geleerd wordt.

In het Nederlandse collectieve geheugen hebben Sven Kramer en Gerard Kemkers zich een plaats veroverd sinds het incident dat Kramer een gouden medaille kostte op de Olympische Winterspelen van 2010. Toch stond op 7 en 8 januari 2012 Kemkers weer als coach langs de baan toen Kramer Europees allround kampioen werd in Boedapest.

In hoeveel organisaties zou Kemkers er nog steeds staan? Waarschijnlijk niet zo gek veel. Het is de kwaliteit van de organisatie en hoe met fouten wordt omgegaan die met deze afloop wordt getoond. Het toont ook de kracht van (opgebouwd) vertrouwen. In zo'n organisatie willen mensen wel werken. Niet alle organisaties gaan zo met fouten om.

- Mentale instelling in de omgang met fouten

Hiernaast ziet u een systeem om ervoor te zorgen dat er alleen maar ernstige branden plaatsvinden in organisaties. Als dit schema wordt getoond wordt er vaak (besmuikt) gelachen. Veel mensen herkennen deze dynamiek. Het demonstreert ook waarom het beter is te spreken over hoog betrouwbaar organiseren dan van hoog betrouwbare organisaties. Organiseren is iets wat zich afspeelt tussen mensen, wat moeilijk in de organisatiestructuur is te verankeren. Het kan ontstaan door kleine incidenten, het gevoel niet rechtvaardig behandeld te zijn. Vertrouwen komt te voet en gaat te paard. Met elke organisatie die zegt helemaal geen problemen of afwijkingen van de regels te hebben, zou u als toezichthouder een probleem moeten hebben. Dan is er ten principale iets fout. Dan is er een behoorlijke kans dat deze mentale instelling regeert. Dit houdt overigens verband met hoe mensen kijken naar organisaties, met hun mentale modellen. De Deense hoogleraar Erik



Hollnagel (2010) heeft over hoe mensen kijken naar waarom dingen fout gaan in organisaties de volgende tweedeling gemaakt.

Dingen gaan goed omdat:	
Theorie W	Theorie Z
Systemen goed ontworpen en tip top onderhouden zijn	Mensen leren ontwerptekorten en tegenstrijdigheden op de vangen
Procedures compleet en correct zijn	Mensen passen hun werk aan aan de vragen die eraan worden gesteld
Mensen handelen zoals verwacht en ze geleerd is	Mensen interpreteren en passen procedures toe toegesneden op de situatie
Ontwerpers voorzien en anticiperen op alle omstandigheden	Mensen ontdekken en corrigeren als zaken fout lopen
Mensen zijn faalfactoren	Mensen zijn succesfactoren

De eerste wijze (theorie W) van kijken is dat we als organisatie beschikken over perfecte goed onderhouden systemen, daar zitten immers hele goede deskundige ontwerpers achter. Procedures zijn op orde en werkbaar. Als mensen nu maar eens doen wat van ze verwacht wordt, dan komt alles goed. Mensen zijn de faalfactor. Achterliggende gedachte is dat alle omstandigheden te voorzien zijn.

De Deense atoomfysicus Niels Bohr heeft ooit gezegd 'zaken zijn moeilijk te voorspellen, met name de toekomst'.

De tweede wijze (theorie Z) van kijken gaat daarvan uit. Dit geeft een organisatie waarin bespreekbaar is dat er (met goede redenen) afgeweken wordt van regels en procedures, omdat niet alles te voorzien is. Het menselijk systeem corrigeert of hanteert tegenstrijdigheden (zoals verschillende eisen van inspecties), ontwerpfouten/–omissies. De organisatie heeft behoefte aan mensen die weten waar 'het' om gaat en praten over de zaken zoals ze werkelijk zijn. Het verschil tussen procedures (en hoe we gedacht hadden dat het moest gaan) en hoe het werkelijk gaat is dan bespreekbaar. Als dat niet mogelijk is en wordt gezegd dat uiteraard alle regels precies worden nageleefd, is dat een reden om als toezichthouder met zo'n organisatie in gesprek te gaan.

- Systemen en regels een noodzakelijke maar onvoldoende voorwaarde

Betekent dit dat systemen en regels overbodig zijn? Natuurlijk niet! Systemen en regels zijn echter feilbaar en de mens is de voorziening om deze feilbaarheid hanteerbaar te maken. Systemen en regels zijn een noodzakelijk maar onvoldoende voorwaarde zoals we in de wiskunde plegen te zeggen. Wat betekent dat voor de omgang met systemen, regels en procedures?

In de Gezondheidszorg is een onderzoek gedaan door Resar (2006). Resar heeft de Pareto regel 20% van de oorzaken staan voor 80% van de fouten toegepast op regelgeving. Hij stelt dat 20% van de regels 80% van de fouten voorkomt en dat twee keer toepassing van deze systematiek leidt tot een betrouwbaarheid van 95%. Dat is in heel veel praktische situaties al heel mooi. Het streven om echter die laatste 5% ook met regelgeving weg te werken kost echter (onevenredig) veel energie en is kansloos in het licht van het citaat van Bohr. Een verstandige afweging is dus geboden. Daarbij moet ook

Pareto verdeling

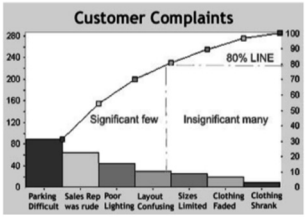
20% oorzaken

⇩

80 % fouten.

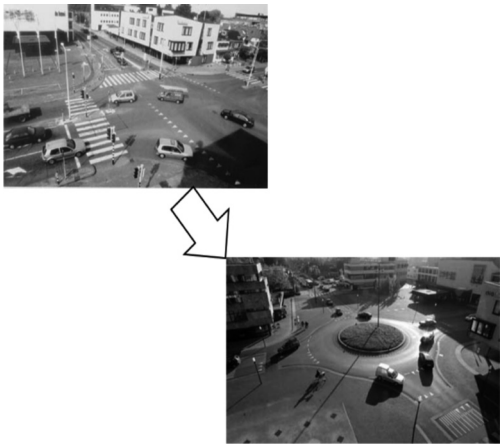
2 maal toegepast

95% reductie

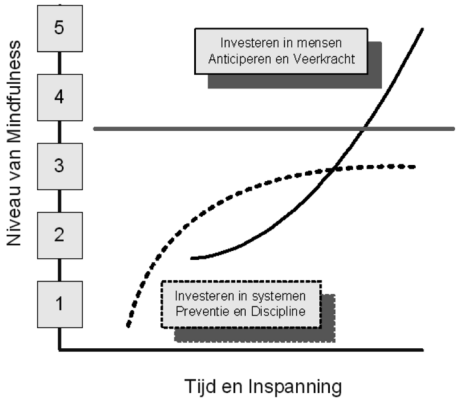


nog worden bedacht dat zeer gedetailleerde regelgeving kan leiden tot een vals gevoel van veiligheid (aan alles is gedacht). Dit kan fnuikend zijn voor de veerkracht c.q. het gebruik van gezond verstand.

Er zijn natuurlijk ook andere prachtige voorbeelden dat we vaak met minder (maar wel betere) regels afkunnen. Een klassiek voorbeeld daarvan zijn de twee plaatjes van een verkeerssituatie in Drachten[10]. In de bovenste situatie met stoplichten, zebrapaden, en voorrangswegen zijn meer regels van toepassing dan in de onderste situatie met een rotonde. Het voorkomt bijvoorbeeld dat je midden in de nacht op een verder verlaten weg staat te wachten tot je stoplicht op groen springt.



Systemen kennen hun beperkingen zo tonen ook de ervaringen van Shell. In reactie hierop heeft Shell het Hearts en Minds[11] programma opgezet. Het model hierachter wordt nu ook in andere organisaties gebruikt. In bepaalde opzichten lijkt het op wat de Bree in hoofdstuk 2 aangeeft in de opeenvolgende ontwikkelingsfasen van compliance management. Met dit programma wordt bevorderd dat de organisatie zich ontwikkelt in de omgang met veiligheid en incidenten van pathologisch tot generatief.



Grofweg verloopt deze ontwikkeling in een aantal fasen:
In fase 1 (pathologisch): 'natuurlijk hebben we incidenten, het is een gevaarlijke business'. 'We voldoen aan de regelgeving en we ontslaan de malloot die het incident veroorzaakte'.
In fase 2 (reactief) staat veiligheid hoog op de agenda m.n. na een incident. Het management neemt veiligheid serieus, maar 'waarom doen werknemers niet wat hen wordt verteld'. Hierna volgt fase 3 (calculatief): we hebben systemen en procedures (inclusief veel audits) en bewakingssystemen. Toch voldoet dit systeem niet volledig, verder investeren in steeds betere systemen levert steeds minder op.
Daarvoor is het nodig in fase 4 (proactief) te komen. Hierin zijn er middelen

10 Ontleend aan de KPMG onderwijstoolkit: Vertrouwen, Integriteit & Leiderschap.
11 Zie hiervoor bijvoorbeeld Apollo 13 consult (2011) Mindful organiseren, Apollo 13 consult, Nijmegen.

om zaken te regelen voordat zich een incident voordoet. Het management staat open voor zwakke signalen, maar is nog steeds gefocused op de cijfers. Procedures worden gedragen door de werkvloer. Uiteindelijk is het streven fase 5 (generatief). Op alle niveaus in de organisatie is een chronisch ongemak met onzekere situaties. Er is een permanente oplettendheid. Veiligheid wordt gezien als een bron van inkomsten. Nieuwe ideeën zijn welkom.

In fase 4 en 5 zijn systemen geen nodeloze ballast, maar hebben organisaties ingezien wanneer regelgeving doorschiet en hoe ze echt kunnen leren van fouten. De organisatie vertoont de veerkracht die nodig is om onverwachte/ onvoorziene gebeurtenissen te gebruiken als ze positieve gevolgen hebben voor het bedrijf en negatieve consequenties zoveel mogelijk te beperken en of zelfs te voorkomen. HRO denken is als het ware de finishing touch.
Hoog betrouwbaar organiseren is vooral een pleidooi voor behoedzaam vertrouwen. Zelfs als er systemen zijn, is het nodig te kijken naar onderliggende mentale modellen die bepalen hoe betrouwbaar een organisatie werkelijk is. Wees daarom altijd bedacht op de signalen wanneer mensen uw vertrouwen niet verdienen.

b. Relatie risicobeheersing en vertrouwen (R.O. Vos)

Vertrouwen is de verwachting dat mensen of dingen ons niet in de steek laten, ook al is dat mogelijk. Vertrouwen is de bereidheid dat risico te lopen. Deze definitie van Nooteboom (2002) koppelt vertrouwen nadrukkelijk aan de wijze waarop men met risico's omgaat. Heeft men zicht op het risico dat de verwachting dat mensen of dingen ons niet in de steek laten, niet wordt waargemaakt? En in welke mate is men bereid dit risico te accepteren?[12] Hoog betrouwbare organisaties (HRO's) zijn op dit punt zeer interessant omdat zij op een speciale manier met deze vragen omgaan. Aan de ene kant zijn er zeer duidelijke afspraken, procedures etc., maar tegelijk wordt aan de andere kant de eigen verantwoordelijkheid van de medewerkers binnen het geheel benadrukt, inclusief de mogelijkheid ter bereiking van de doelstelling van de regels af te kunnen wijken. Binnen hoog betrouwbare organisaties wordt dus zowel sterk gestuurd op 'hard controls' als op 'soft controls', waarbij 'fouten melden' belangrijker is dan 'geen fouten maken'. Daarnaast zijn de 'principles' (doelstelling bereiken) belangrijker dan de 'rules' (zich aan de regels houden). Er wordt zowel geïnvesteerd in het 'kunnen' (deskundigheid en het vergroten van de deskundigheid door te leren van fouten) als in het 'willen': de cultuur (awareness)[13].

Hoog betrouwbare organisaties zien fixatie op alleen regels (zonder rekening te houden met de factor mens) als een zeer groot risico, te weten het gevaar van schijnzekerheid. Onderstaand twee voorbeelden:

Voorbeeld 1: creditcard

Bij een wijziging van de gegevens van een creditcard wordt altijd volgens een vast protocol een aantal controlevragen gesteld. In het onderhavige geval waren alle controlevragen goed beantwoord en op het formulier afgevinkt. Toch was er iets misgegaan met als gevolg het leeghalen van de rekening. Bij het afluisteren van het bandje waarop het gesprek was opgenomen, hoorde men dat het ging om de creditcard van een vrouw, terwijl de persoon aan de andere kant van de lijn een man was. Dit signaal was door de focus op de vragen van het formulier niet opgemerkt.

12 Zie ook in dit verband ook kritische succesfactor 6: Zicht op risico's en bereidheid deze te accepteren (bijlage 1).
13 Zie in dit verband ook de twee assen van het spinnenwebdiagram (bijlage 2)

Voorbeeld 2: Ajax-AZ:

Om supporters van het veld te weren is een indrukwekkende gracht om het hele veld aangelegd. In de praktijk is dit erg onhandig omdat dit een hindernis vormt voor de supporters in rolstoelen die aan de rand van het veld mogen plaatsnemen. Om dit te ondervangen is een houten vlonderbrug geplaatst over de gracht. De vraag is in hoeverre er voldoende 'awareness' was voor deze zwakte in de beveiliging om supporters te verhinderen het veld op te gaan? Had niet één, maar twee suppoosten opgesteld moeten worden? Hadden zij hun aandacht niet alleen op de tribune moeten richten i.p.v. af en toe naar het veld te kijken? Kortom: Zich permanent bewust zijn van het risico dat met de vlonderbrug toegang tot het veld gecreëerd was! Uiteindelijk kennen we het gevolg: ondanks de gracht was het mogelijk dat een supporter toegang kreeg tot het veld en de keeper van AZ met een karatetrap kon belagen.

Het verdere verhaal is evenzeer bekend: de AZ keeper verdedigde zich en gaf nadat de supporter op de grond lag nog twee ferme trappen (noodweer?noodweerexces?). In ieder geval voldoende reden voor de scheidsrechter om de AZ keeper een rode kaart te geven en van het veld te sturen. Na afloop werd duidelijk dat de scheidsrechter niet anders kon doen, omdat er strikte instructies voor scheidsrechters van de KNVB waren de regels strikt toe te passen. Regels zijn regels. AZ liep van het veld, vanwege de onrechtvaardigheid van de rode kaart en de wedstrijd werd gestaakt. Hoewel in eerste instantie vanuit de KNVB en de scheidsrechtersorganisatie de scheidsrechter geprezen werd om het strikt toepassen van de regels, bleek al snel dat maatschappelijk de rode kaart niet geaccepteerd werd in een dergelijke (onvoorziene) situatie. Vragen als: en als de aanvaller een mes zou hebben gehad, had de keeper dan ook niet hebben mogen reageren? De onafhankelijke aanklager van de KNVB trok om deze overwegingen de rode kaart in, de KNVB kon weinig anders dan de wedstrijd in zijn geheel over laten spelen ten overstaan van alleen kinderen en hun begeleiders en AZ won. Dit had anders en bevredigender kunnen verlopen als de scheidsrechter wel ruimte had gehad om op grond van zijn professionele inschatting naar omstandigheden te handelen en in dit geval af te wijken van de regels. Wellicht een leerpuntje voor de KNVB?

Gezien de bovenstaande voorbeelden is de vraag hoe overheidsorganisaties met dit soort situaties omgaan? Hoe stellen controllers en auditors zich op? Als een organisatie bewust om goede redenen van de regels is afgeweken om de doelstelling te realiseren, geven we dan een compliment of een gele kaart? Als een organisatie er bovenop zit, de risico's goed in de gaten houdt en dus fouten (die altijd gebeuren) goed in het snotje heeft, die zelf actief meldt en kijkt hoe deze in de toekomst verbeterd kunnen worden, geven we dan een compliment (omdat ze goed in control zijn) of een gele kaart (omdat er fouten gemaakt zijn)?

In zijn proefschrift 'Hoe vertellen we het de Tweede Kamer? concludeert Enthoven (2010) dat informatie over risico's en beleidsalternatieven in de huidige politieke cultuur van coalitie en oppositie onderdeel is van het politieke spel. Het accepteren van risico's die horen bij het instemmen met bepaalde beleidsvoorstellen vindt daardoor veelal niet expliciet, maar hooguit impliciet plaats. Als iets misgaat staat dan de discussie over het incident voorop (hoe heeft dit kunnen gebeuren) en niet de in het verleden gemaakte beleidskeuze en de inherente risico's van die beleidskeuze.

De vraag die in dit soort gevallen steeds terugkeert is of we bereid zijn risico's te accepteren. Kunnen we accepteren dat er dingen mis kunnen gaan of niet?

Een voorbeeld hoe het ook kan (Noorwegen):

Ondanks de verschrikkelijke gebeurtenissen in Noorwegen heeft men daar niet besloten om te proberen dit soort situaties in de toekomst te voorkomen met allerlei maatregelen in de vorm van regels en controles (wat in Nederland wel de reactie was op de vuurwerkramp in Enschede en de Nieuwjaarsbrand in Volendam). In Noorwegen staat het gevoel van een grote mate van vrijheid als groot goed centraal. De Noren willen niet anders met elkaar om gaan. Ze zijn dus bereid op dit punt een zeker risico te accepteren. Wel wil men leren van de gebeurtenissen: Wat kan beter binnen de huidige structuren. De focus ligt daarbij op meer alert zijn (gericht op voorkomen) en effectiever acteren als iets dergelijks zich in de een of andere vorm weer zou voordoen (gericht op verkleining gevolgen).

Wellicht valt op dit punt nog iets te leren van Noorwegen als een uitgesproken 'high trust society'[14]?

Afsluitend wordt hieronder de wijze waarop men met elkaar omgaat op een vliegdekschip langs de negen kritische succesfactoren van vertrouwen gelegd:

- Duidelijkheid (KSF 1)

De 'tight controls', de regels die essentieel zijn, zijn duidelijk gedefinieerd. Helder zijn ook de reden en het belang van deze regels. Iedereen is doordrongen van zijn verantwoordelijkheid ten aanzien van het volgen van deze regels die qua aantal zo beperkt mogelijk zijn, maar tezamen wel de kern van het proces bepalen.

- Deskundigheid (KSF 2)

Er wordt permanent geïnvesteerd in verhoging van de kwaliteit/deskundigheid zowel individueel als collectief. Medewerkers moeten optimaal toegerust zijn voor hun taak. Over hun deskundigheid hoe te handelen in de voorkomende situaties, mag geen twijfel bestaan.

- Gemeenschappelijk belang (KSF 3)

Veiligheid (de vliegtuigen veilig te laten opstijgen en landen) staat centraal en is een gemeenschappelijk belang en verantwoordelijkheid voor een ieder. Alle medewerkers zijn schakels binnen het geheel. Een ieder kent zijn bijdrage aan het geheel en weet wat er kan misgaan als hij zijn taak niet goed uitvoert. Op dit punt is iedereen ongeacht rang en stand gelijk.

- Goed gevoel (KSF 4)

Er is sprake van een grote mate van saamhorigheid. Samen elke keer weer de klus goed klaren. Daarom worden successen als team gedeeld om het onderlinge goede gevoel te verstevigen.

- Open informatie-uitwisseling (KSF 5)

Directe en open communicatie staat centraal. Essentiële informatie onmiddellijk melden via korte, duidelijke communicatielijnen. Liever een aantal keren een melding die niet juist bleek, dan één keer informatie achtergehouden die essentieel bleek. Beloon mensen die 'slecht' nieuws melden. Niet 'geen nieuws is goed nieuws', maar 'geen nieuws is slecht nieuws'.

- Inzicht in risico's en risicoacceptatie (KSF 6)

Vooraf zijn de risico's goed in kaart gebracht. Daarbij wordt ook rekening gehouden hoe te handelen als iets niet helemaal goed gaat, bij voorbeeld: extra gas geven bij een landing

14 Fukuyama, 1995

om zo bij een probleem voldoende snelheid te hebben voor een doorstart. Er is een sterke gerichtheid op het signaleren en melden van risico's, ook van zwakke signalen.

- Mogen controleren (KSF 7)

Permanent wordt het essentiële proces gemonitord en gecontroleerd of alles goed ging en wat de volgende keer extra aandacht verdiend. Dit wordt gezien het belang door iedereen volstrekt normaal gevonden. Het is een onderdeel van de risico-awareness. Aandacht mag niet verslappen.

- Bespreken incidenten en leren (KSF 8)

De organisatie is gericht op leren en verbeteren. Ook op kleine incidenten wordt direct gereageerd, omdat dan nog bijgestuurd kan worden. Daarom is het direct melden - ook van kleine incidenten - ontzettend belangrijk. Vervolgens wordt het incident uitvoerig besproken en geanalyseerd om er voor de volgende keer van te leren.

- Sancties/consequenties bij bewuste inbreuken (KSF 9)

Het bewust voor je houden van informatie/niet melden van is binnen deze organisatie volstrekt onacceptabel. Op dat punt moet een ieder zich houden aan duidelijke instructies. Als iemand dat niet doet, is het direct 'Einde oefening'.

Conclusie: Een hoog betrouwbare organisatie scoort op alle negen kritische succesfactoren voor vertrouwen een 4 of hoger (op een schaal van 1 tot 5).

4. Ervaringen met de negen kritische succesfactoren en de vertrouwenscan (René Witte en Robert Vos)

a. Gebruiksmogelijkheden van de negen kritische succesfactoren en de vertrouwenscan

In 2010 en 2011 heeft een aantal overheidsorganisaties gebruik gemaakt van het referentiekader van de negen kritische succesfactoren dat is opgenomen in de publicatie 'vertrouwen geven en in control zijn gaat dat samen' (april 2009) en de op dat referentiekader gebaseerde concrete tool (de vertrouwenscan) die is gepresenteerd in de publicatie 'vertrouwen geven en in control zijn; Hoe doe je dat' (december 2010). Het referentiekader van de negen kritische succesfactoren en de vertrouwenscan bieden een aantal gebruiksmogelijkheden waarmee in de afgelopen twee jaar ervaring is opgedaan.
Deze gebruiksmogelijkheden zijn:

- Presentatie/workshop

Bij een presentatie wordt met name het referentiekader van de negen kritische succesfactoren toegelicht. Bij een workshop wordt tevens de vertrouwenscan[15] door iedere deelnemer voor een bestaande relatie (die de deelnemer in principe zelf mag bepalen) ingevuld en geanalyseerd met het spinnenwebdiagram[16].

Doelstelling van de presentatie is om een algemeen inzicht te verkrijgen in wat vertrouwen is, hoe het werkt en van welke kritische succesfactoren deze afhankelijk is. Bij een workshop is de aanvullende doelstelling dat iedere deelnemer dit inzicht naar de eigen omgeving vertaald door de vertrouwenscan in een eigen praktijksituatie toe te passen.

- (Self)assesment

In een (self)assment wordt de relatie tussen twee organisaties in kaart gebracht met behulp van de vertrouwenscan. Dit kan eenzijdig gebeuren (hoe kijkt de ene organisatie tegen de andere organisatie aan), maar ook tweezijdig (hoe kijken de twee organisaties over en weer tegen elkaar aan). Een (self)assesment kan voorafgegaan worden door een presentatie als voorbereiding op het (self)assesment. Het (self)assesment kan door de organisatie zelf worden uitgevoerd of door een bureau van buiten. Voor het (self)assesment kan gebruik gemaakt worden het formulier van de vertrouwenscan dat ingevuld wordt tijdens interviews.

Doelstelling van het (self)assesment is het verkrijgen van inzicht in het niveau van vertrouwen en de daaraan ten grondslagliggende factoren alsmede het reflecteren op die uitkomsten, gericht op mogelijkheden om de relatie te verbeteren.

- In het kader van een audit

Bij het gebruik van de vertrouwenscan in het kader van een audit gaat het om een beoordeling van het vertrouwensniveau door een auditdienst. Vertrouwen wordt dan gezien als een 'soft control' in het kader van de interne beheersing. Het zal dan veelal gaan om een operational audit in opdracht van het management. Voor de audit kunnen de negen kritische succesfactoren als de auditvariabelen (te beoordelen beheerselementen) gezien worden. Wel zal in het algemeen nog een nadere uitwerking (definiëring) van de negen kritische

15 Het formulier van de vertrouwenscan met daarin opgenomen de negen kritische succesfactoren is opgenomen in bijlage 1. Voor een toelichting moge verwezen worden naar het boekje 'Vertrouwen geven en in control zijn. Hoe doe je dat?'.

16 Het spinnenwebdiagram is opgenomen in bijlage 2. Voor een toelichting moge verwezen worden naar het boekje 'Vertrouwen geven en in control zijn. Hoe doe je dat?'.

succesfactoren dienen plaats te vinden gericht op de beantwoording van de door het management geformuleerde centrale auditvraag . Het onderzoek zal in principe uitgevoerd kunnen worden door het houden van interviews aan de hand van het formulier, eventueel aangevuld met andere onderzoeksmethoden zoals een enquête of documentenonderzoek .

Doelstelling van de audit is het verkrijgen van onafhankelijke beoordeling van het aanwezige vertrouwensniveau binnen een organisatie of tussen twee organisatieonderdelen ten behoeve van het management. De specifieke doelstelling (de centrale auditvraag) dient dan ook in nauw overleg met het management (opdrachtgever) geformuleerd te worden.

- In het kader van de bepaling van de controle aanpak (toezicht)

Ten slotte kunnen de negen kritische succesfactoren gebruikt worden als uitgangspunt voor een checklist voor toezichthouders bij de bepaling van de mate waarin van vertrouwen in de richting van de onder toezichtgestelde gebruik gemaakt kan worden als onderdeel van een risicogericht systeemtoezicht . Het verdient dan wel aanbeveling de negen kritische succesfactoren nader te concretiseren aan de hand van de specifieke eisen die in het kader van het toezicht gesteld worden.

Doelstelling van de checklist is dan een hulpmiddel voor het bepalen van de verwachting dat een onder toezichtgestelde zich houdt aan de gestelde eisen.

b. Ervaringen met het gebruik van de negen kritische succesfactoren en de vertrouwenscan

Op het congres van 19 januari 2012 heeft een viertal organisaties hun ervaringen met de negen kritische succesfactoren en de vertrouwenscan gedeeld met de aanwezigen[17].

Deze organisaties zijn:

- De Hoofddirectie Financiën en Control (HDFC) en de directie Planning & Control van de Koninklijke Marechaussee van het ministerie van Defensie

Aandacht voor vertrouwen is binnen Defensie ontstaan door het ontwikkelen van een nieuwe visie op control. In de relatie tussen centraal FEZ en de verschillende lagen van control gaat veel tijd en capaciteit verloren omdat over en weer controles plaatsvinden op bijvoorbeeld de juistheid van de gebruikte cijfers, ook is vaak toestemming nodig voorhandelingen waar kleine risico's mee gemoeid zijn. Dit maakt het werk ook minder plezierig. Door meer te werken op basis van (gerechtvaardigd) vertrouwen is het mogelijk te sturen op hoofdlijnen en risico's.

In een pilot in de vorm van een tweezijdig selfassesment is de relatie tussen de Hoofddirectie Financiën en Control (HDFC) en de Directie Planning & Control van de Koninklijke Marechaussee onderzocht onder begeleiding van een werkgroep waarin beide directies vertegenwoordigd waren. Na een schriftelijke introductie zijn meerdere interviews bij beide directies gehouden. De uitkomsten zijn eerst afzonderlijk per directie opgesteld en voorgelegd in de vorm van een powerpointpresentatie. Vervolgens zijn de hoofdpunten gepresenteerd en besproken in een gezamenlijk overleg.

De interviews leveren nuttige informatie op, maar niet altijd direct iets nieuws. Wel vormen de negen kritische succesfactoren een gemeenschappelijk, gestructureerd kader

17 De Interne Auditdienst van OCW was door omstandigheden verhinderd. De ervaringen van OCW zijn hieronder wel opgenomen op basis van een schriftelijke inbreng.

om vertrouwen met elkaar te kunnen bespreken. De gezamenlijke bespreking is de basis geweest voor een volgende stap: een convenant. De bedoeling is dat op basis van meer vertrouwen er minder centraal wordt opgelegd en meer aan elkaar wordt overgelaten. Het convenant geeft duidelijkheid op papier, maar het gaat vooral om duidelijkheid over wederzijdse verwachtingen en het gezamenlijk vast stellen van de belangrijke risico's. Een belangrijke afspraak is dat formele rapportages zinvol zijn, maar dat actieve communicatie op momenten dat er belangrijke risico's zijn essentieel zijn om het vertrouwen te handhaven.

De verwachting is dat Defensie in de toekomst met het instrument verder gaat. Op dit moment vindt echter een ingrijpende reorganisatie van de gehele audit- en controlfunctie bij Defensie plaats. Dit zal leiden tot nieuwe verhoudingen die zich eerst moeten uitkristalliseren.

- De Interne Auditdienst van de Nederlandse Voedsel- en Waren Autoriteit (NVWA)

Ten tijde van de fusie van de PD, VWA en AID is voor de nieuwe organisatie NVWA een nieuwe missie en managementvisie vastgesteld. Centraal in de managementvisie van de NVWA staat: "samen gaan en staan voor resultaat", waarbij de medewerkers van de NVWA vertrouwen krijgen en verantwoordelijkheid nemen ten aanzien van de te verrichten inspanningen en waar en wanneer deze worden uitgevoerd. Uit diverse signalen werd duidelijk dat het voor veel leidinggevenden nog helemaal niet zo duidelijk is, wat nou 'vertrouwen' is binnen het werk, of binnen het team. Daarbij werd de vraag gesteld hoe je bij het geven van vertrouwen toch in control kunt zijn. Aangezien 'vertrouwen' één van de pijlers is van het programma **H**et **N**ieuwe **W**erken (HNW), is besloten om in 2011 een audit uit te voeren bij één team van de NVWA. In dit geval een team dat belast is met het uitvoeren van inspecties op landbouwbedrijven. Het team bestond uit 15 medewerkers. Daarbij is gebruik gemaakt van de negen kritische succesfactoren en de vertrouwenscan op basis.

Het doel van het uitvoeren van de audit is het verkrijgen van inzicht in de mate van vertrouwen binnen het team. Het betrof daarbij alle onderlinge relaties, zowel tussen teamleden onderling als tussen medewerker en teamleider teneinde :
- de teamleden individueel meer inzicht te geven in wat vertrouwen is en waarom vertrouwen zo belangrijk is;
- het team als geheel inzicht te geven in de mate van vertrouwen binnen het team en de factoren die dit (positief/negatief) beïnvloeden. Het daarbij aanreiken van aanknopingspunten om de teamleden met elkaar daarover (inclusief mogelijkheden tot verbeteringen) in discussie te laten gaan.

en tevens:
- vast te stellen of het instrument breed ingezet kan worden binnen de NVWA;
- vast te stellen of de vertrouwenscan informatie kan genereren voor de topleiding (uitkomsten zijn wellicht bruikbaar voor het Programma Het Nieuwe Werken);
- de IAD van de NVWA in de gelegenheid te stellen ervaring op te doen met het gebruik van de vertrouwenscan als onderzoeksinstrument;
- Het projectbureau audit- en beheersingsvraagstukken van het Ministerie van Financiën ervaring te laten opdoen met de vertrouwenscan als instrument binnen het Rijk.

Na een introductie door een presentatie zijn er door het onderzoeksteam 15 interviews afgenomen. De uitkomsten zijn vervolgens verwerkt en aan het team teruggekoppeld. Na validatie (herkenning van de uitkomsten) is door het team gerapporteerd aan de opdrachtgever (de Inspecteur Generaal) in de vorm van een onderzoeksrapport.

Kijkend naar de doelstellingen is de Interne Auditdienst van mening dat de verwachtingen zijn gerealiseerd:

- Er is een beeld verkregen van de mate van vertrouwen. Het verkregen beeld bevestigde het gevoel van de meeste leden van het team. Uit het onderzoek kwam naar voren dat de meeste teamleden dezelfde aspecten noemden die ze belangrijk vonden in de relatie met de teamleden.
- het team als geheel heeft meer inzicht gekregen hoe je het begrip vertrouwen hanteerbaar kunt maken. De IG van de NVWA is enthousiast, met name omdat met de scan het ongrijpbare tastbaar gemaakt kan worden. De resultaten van het project zijn aanleiding om de vertrouwenscan meer te gaan gebruiken binnen de NVWA.
- De scan gaf ook inzicht in externe ontwikkelingen die op het team afkomen die mogelijk een inbreuk kunnen vormen op het niveau van vertrouwen.

- Dienst Zeeland van Rijkswaterstaat (RWS)

Sinds enige jaren maakt RWS gebruik van contractvormen waarop systeemgerichte contractbeheersing wordt toegepast. Hierdoor verandert de toezichtrelatie tussen RWS en de opdrachtnemer van traditioneel toezicht (het over schouder meekijken bij de opdrachtnemer) naar het steunen op het kwaliteitssysteem van de opdrachtnemer.
De opdrachtnemer krijgt hierdoor een andere rol: meer verantwoordelijkheid en het aantoonbaar beheersen van het werk. Voor de medewerkers van RWS verandert ook de rol. De medewerkers sturen niet op het werk zelf, maar houden meer toezicht op afstand. Dit betekent gedoseerd loslaten en op basis van risicomanagement toetsen uitvoeren op diverse niveau's (systeem, proces en product). Vertrouwen speelt hierbij een cruciale rol.

RWS Dienst Zeeland heeft via een workshop kennisgemaakt met vertrouwenscan. In het project herstel Steenbekledingen Ooster- en Westerschelde (projectbureau Zeeweringen) werden mogelijkheden gezien om de vertrouwensrelatie tussen Zeeweringen en haar opdrachtnemers vanuit het gezichtpunt van Zeeweringen (eenzijdig) in kaart te brengen op basis van de negen kritische succesfactoren. Hierbij is gekozen voor een begeleid self assesment. In 7 interviews met de sleutelpersonen binnen Zeeweringen (projectleiders en contractmanager) zijn de negen kritische succesfactoren langsgelopen in de relatie tussen hen en de sleutelpersonen van de opdrachtnemers (uitvoerders/projectleiders). Het object van vertrouwen was de aantoonbare beheersing van de uitvoering van het werk door de opdrachtnemers. De gesprekken waren open. Vertrouwen als onderwerp vonden de gesprekspartners zeer interessant en men was graag bereid om over de ervaringen te vertellen. De uitkomsten van de scan zijn gezamenlijk besproken. De spinnenwebdiagrammen gaven een goed inzicht in laag scorende kritische succesfactoren. Ook werden de onderlinge verschillen tussen de opdrachtnemers goed zichtbaar. Op basis hiervan is gediscussieerd hoe het gedeelde belang en de aandacht voor soft controls vergroot kan worden. De scan op zichzelf levert geen nieuwe dingen en ook geen directe oplossingen op. Het helpt wel om zaken te benoemen en goed in kaart te brengen. Dit levert een mooi startpunt op voor het verder ontwikkelen van vertrouwen. De deelnemers hebben deze aanpak aan andere groepen aanbevolen.

- Regio Rijnmond van de Belastingdienst

Bevorderen van de compliance is het hoofddoel van de Belastingdienst. Sinds een aantal jaren worden in het kader van Horizontaal Toezicht convenanten afgesloten met belastingplichtige organisaties, waarbij uitgegaan wordt van vertrouwen. Tijdens het congres heeft een vertegenwoordiger uit het segment middelgrote tot zeer grote ondernemingen aangegeven dat er veel aandacht is voor de grondbeginselen transparantie, begrip en vertrouwen. Dit vergt kennis over deze abstracte begrippen. Benaderen vanuit een uitsluitend

juridische en controletechnische grondslag is onvoldoende. In het toezicht bij de grotere ondernemingen wordt aan de hand van interviews vastgesteld of er een houding bij de belastingplichtige organisatie is die het mogelijk maakt om op basis van genoemde begrippen een vertrouwensrelatie aan te gaan. Onderwerpen hierbij zijn strategie, fiscale functie, aandacht voor AO/IB en IT en ander extern toezicht. Wanneer de wil bij een onderneming er is en de verwachting dat de onderneming de fiscaliteit in voldoende mate kan (gaan) beheersen, dan volgt een convenant. Vervolgens wordt aandacht besteed aan het kunnen. Dit vereist dat de verwachtingen over en weer goed met elkaar besproken moeten worden. Voor de onderneming betekent het dat zij haar verantwoordelijkheid moet pakken om te komen tot aanvaardbare aangiften.

Het omgaan met vertrouwen maakt op deze wijze een vast onderdeel uit van het dagelijks werk. Het is belangrijk de medewerkers daarvoor goed uit te rusten. In de diverse werkverbanden binnen en buiten Regio Rijnmond zijn de negen kritische succesfactoren uit het boek *Vertrouwen geven en in control zijn; Hoe doe je dat?*(2010)besproken en dan vooral wat dat betekent in het werkveld van de Belastingdienst. Het referentiekader van de negen kritische succesfactoren wordt gebruikt voor de verdieping van het inzicht in vertrouwen en hoe dat werkt. Het gaat om te komen tot gerechtvaardigd vertrouwen met de inzet van de juiste mix van hard en soft controls. De negen kritische succesfactoren worden in de besprekingen vertaald naar het handhavingmodel van de Belastingdienst. Dit heeft tot gevolg gehad dat in meerdere regio's een impuls is gegeven aan de invulling van het begrip vertrouwen naar de praktijk met daarbij zowel aandacht voor de hard als de soft controls die in de negen kritische succesfactoren worden aangegeven.

- De Interne Auditdienst van het ministerie van OCW

Het gebruik van de vertrouwenscan was een follow up van een onderzoek naar het opdrachtmanagement tussen het bestuursdepartement en DUO door AD OCW (afdeling Onderzoek en Advies). Uit dat onderzoek was gebleken dat de informatie-uitwisseling tussen uitvoering en beleid in het algemeen onvoldoende efficiënt en effectief noch plezierig verliep onder andere vanwege een tekort aan vertrouwen op verschillende plekken en niveaus in de organisatie. Het referentiekader was Speed of Trust (Covey, 2006). De onderzoekers adviseerden naast het verbeteren van structuren, processen en procedures om werk te maken van het verbeteren van vertrouwen. Om dit te concretiseren zijn een beleidsdirectie en hun counterparts bij DUO gevraagd om als pilot mee te doen om te onderzoeken of en hoe dit instrument zou kunnen bijdragen aan (inzicht in) meer vertrouwen. De pilot was sterk gericht op ervaring opdoen ('lerenderweg'). Er zijn uiteindelijk 12 interviews gehouden (zes bij de beleidsdirectie en zes bij de uitvoeringsorganisatie). Het waren open gesprekken en de geïnterviewden waardeerden de mogelijkheid om op het eigen werk te kunnen reflecteren. De uitkomsten zijn gepresenteerd in een gezamenlijke bespreking van de beleidsdirectie en DUO-medewerkers (validatie) waarbij ook het referentiekader van de negen kritische succesfactoren en facilitatietools van Speed of Trust zijn gebruikt (o.a. kaartsets met de 13 gedragingen van vertrouwenwekkend gedrag). Vervolgens is gerapporteerd aan opdrachtgever en nabesproken met de opdrachtgever (DUO-manager) en een lijnmanager van de beleidsdirectie.

De gekozen aanpak van 'lerenderweg' leverde veel flexibiliteit op, maar had als nadeel dat tijdens de interviews nog veel uitgelegd moest worden. Dat maakte dat bij de presentatie van de uitkomsten de bal erg bij de onderzoekers lag. Inhoudelijk leverden de interviews en de bijeenkomst inzicht in de relatie tussen de twee directies op alsmede een aantal aanknopingspunten om hier wat mee te doen. Voor de auditdienst was het een goede ervaring om op het thema vertrouwen verder te kunnen gaan als wederom om zo'n onderzoek door de opdrachtgever gevraagd wordt.

c. De do'en de don'ts

Door de forumleden zijn een aantal do's en don'ts geformuleerd. Deze zijn:

- Zorg voor een goede introductie van de interviews

Voor een goed resultaat is een goede introductie van de interviews van belang. Zorg ervoor dat de geïnterviewden de achtergrond van de vertrouwenscan op zijn minst globaal kennen. Dit kan uitgebreider door het houden van een introductiepresentatie of minder uitgebreid door een introductiebrief (met bijgevoegd een artikel over de vertrouwenscan). Dit voorkomt dat tijdens de interviews de geïnterviewden met allerlei vragen over vertrouwen in algemene zin en/of de methodiek van de vertrouwenscan komen, waardoor er onvoldoende tijd is om de negen kritische succesfactoren zelf langs te lopen. Bij een goede introductie blijkt het normaal gesproken zeer wel mogelijk de interviews binnen één uur (met in enkele gevallen een uitloop van een kwartier) af te ronden.

- Zorg voor een duidelijke doelstelling en - indien van belang - steun vanuit de leiding

Duidelijk moet zijn waarom de vertrouwenscan wordt toegepast. Daarbij moeten ook de verwachtingen die men van de vertrouwenscan heeft, vooraf goed zijn doorgesproken. Het meten van het niveau van vertrouwen moet geen doel op zich zijn. Het uiteindelijke doel kan bij voorbeeld het verlagen van de interne bureaucratie en/of het verbeteren van de relatie zijn. De betrokkenen moeten hier dan wel bewust van zijn en daar ook expliciet stappen in willen zetten. Steun/draagvlak vanuit de leiding speelt dan vaak een belangrijke rol. Ook is het aan te bevelen de wijze van terugkoppeling van de interviewresultaten - eerst in het eigen organisatie-onderdeel en daarna gezamenlijk - , goed af te spreken. Voorkomen moet worden dat je als onderzoeker/uitvoerder van de vertrouwenscan zelf teveel geassocieerd wordt met de inhoudelijke doelstelling en uitkomsten. De winst van de scan is dat alle aspecten die van belang zijn voor vertrouwen op een rij worden gezet en dat er een structuur ontstaat voor de discussie over vertrouwen. Het is de verantwoordelijkheid van de onderzoeker/uitvoerder daarvoor zorg te dragen.

- Zorg voor het gebruik van de juiste woorden bij de negen kritische succesfactoren

Een punt van voorbereiding kan zijn de woorden die gebruikt worden in de kritische succesfactoren langs te lopen op de woorden die in de specifieke omgeving gebruikt worden (het eigen jargon). Bij voorbeeld: bij kritische succesfactor 6 is het in het ene geval beter om het woord 'controleren' en in het andere geval 'kritisch (door)vragen' te gebruiken. Ander voorbeeld: bij kritische succesfactor 9 is het in het ene geval beter om het woord 'sancties' en in het andere geval 'consequenties aan verbinden' te gebruiken, etc. Het is voor de geïnterviewden storend wanneer niet-passende woorden worden gebruikt. Dit kan leiden tot minder betrokkenheid tijdens de interviews.

- Zorg voor een veilige omgeving

De vragen naar aanleiding van de negen kritische succesfactoren kunnen gevoelige zaken raken. Zorg in die situatie voor een veilige setting zodat de deelnemers aan de scan zich open durven uit te spreken. Door het benadrukken dat de informatie vertrouwelijk wordt behandeld en alleen intern wordt gebruikt, kunnen open gesprekken bevorderd worden. Het kan aanbeveling verdienen expliciet af te spreken dat de geïnterviewde het verslag ter goedkeuring krijgt voorgelegd, dit verslag niet verspreid wordt en door de onderzoekers uitsluitend gebruikt wordt voor het samenstellen van een totaalbeeld dat niet tot personen herleidbaar is. Een veilige omgeving is ook noodzakelijk bij de terugkoppeling van

de resultaten aan de groep(en). Als er mensen van verschillende hiërarchische niveau's bij elkaar zijn tussen wie ook rapportagelijnen bestaan en er sprake is van gevoeligheden, dan is een hoog kwaliteitsniveau van procesbegeleiding aan te bevelen voor een vruchtbare bijeenkomst.

- Doe interviews bij voorkeur met zijn tweeën

In de praktijk blijkt het prettig te werken om interviews met z'n tweeën af te nemen. Hierdoor verloopt het gesprek efficiënter: je kunt elkaar aanvullen en je vangt ook de meeste informatie op (rolverdeling: de een stelt in principe de vragen; de ander maakt aantekeningen en bewaakt de proceskant). Luister altijd met actieve belangstelling naar de gegeven antwoorden. Er is vaak een grote motivatie om te vertellen hoe men het werk doet, als iemand daarin interesse toont. Interviews leveren vaak waardevolle 'bijvangst' op (niet alleen informatie over hoe gedacht wordt over de andere organisatie, maar ook over hoe binnen de eigen organisatie gewerkt wordt en waarom). Bedenk dat er geen goed of foute antwoorden zijn. Het gaat om het verkrijgen van een goed beeld hoe men in de praktijk tegen de relatie met de ander aankijkt. Verder helpt het als de interviewers zich verdiept hebben in de specifieke situatie van de organisatie zodat je weet welke ex- en interne factoren een rol spelen. Het interview kan afgesloten worden met een 'exit'-vraag : Wat vond je ervan? Wat kan je zelf doen aan vertrouwen? Dit levert soms verrassende antwoorden die goed gebruikt kunnen worden bij de follow-up.

- Stel de rapportage met grote zorgvuldigheid op/houd bij een presentatie rekening met gevoeligheden

Stel de rapportage samen op basis van gespreksverslagen die bij voorkeur geaccordeerd zijn. Zorg ervoor dat de bevindingen altijd onderbouwd kunnen worden aan de hand van de ingevulde formulieren. Gebruik bewoordingen als: een grote meerderheid, een minderheid, enkelen etc. Kies voor genuanceerde bewoordingen wanneer er sprake is van gevoelige zaken, zonder te kern van de boodschap te verhullen (bij voorbeeld: 'een minderheid is minder gelukkig met…' i.p.v. 'een minderheid is ontevreden over…'). Dit zelfde geldt ook bij een presentatie. Het gaat erom dat de deelnemers aan de vertrouwenscan zich in de uitkomsten herkennen en als basis nemen voor een gesprek over het niveau van vertrouwen. De presentatie is eigenlijk de spiegel die de respondenten en de organisatie wordt voorgehouden om in positieve zin te kunnen reflecteren (doelstelling is verbeteren, niet afrekenen). Het spinnenwebdiagram is een prima hulpmiddel ter ondersteuning van de presentatie en helpt om de rode draad vast te houden.
Bij tweezijdig uitgevoerde assesments is het verstandig het beeld dat over de ander gegeven wordt eerst goed af te stemmen met de organisatie die daarvoor geïnterviewd is (en te toetsen op gevoeligheid) voordat het ter beschikking gesteld wordt/gepresenteerd wordt aan de ander. Bij het onderzoek van 'vertrouwen binnen een team' is het team anoniem, maar de teamleider niet. Om reden van zorgvuldigheid zijn de uitkomsten hier eerst gepresenteerd aan de teamleider en pas daarna aan het hele team.

- Zorg voor een follow up.

Het is van belang om na de vertrouwenscan de aandacht voor meer vertrouwen te blijven vasthouden. De vertrouwenscan geeft geen panklare oplossing. Het geeft wel inzicht in welke richting je een eventuele oplossing zou moeten zoeken. Dit is vaak een kwestie van cultuur die niet met een keer een vertrouwenscan verandert. Van belang is dat de uitkomsten van het onderzoek aanzetten tot actie bij de betrokkenen. Bovendien is vertrouwen permanent in beweging. Iedere nieuwe ervaring draagt bij aan een positieve of negatieve ontwikkeling van het vertrouwen. Het is van belang op dit punt geen verkeerde verwach-

tingen te wekken. Het gaat erom permanent aandacht aan het niveau van vertrouwen te geven, en niet eenmalig. Het gevaar is aanwezig dat in gevallen dat de vertrouwenscan een positief beeld geeft, vertrouwen geen blijvende aandacht krijgt. Juist ook in goede relaties dienen betrokkenen bewust te zijn dat met name externe invloeden een inbreuk kunnen geven op het niveau van vertrouwen. Het is derhalve van belang dat de betrokken het vermogen hebben of creëren om blijvende aandacht te hebben voor mogelijke inbreuken en hierop kunnen reageren.

- Wees voorzichtig met de vertrouwenscan tijdens reorganisaties

Het advies is het instrument van de vertrouwenscan voorzichtig te gebruiken in reorganisaties. Tijdens reorganisaties kunnen de onderlinge relaties te veel in beweging zijn en nog niet zijn uitgekristalliseerd. Dit kan leiden tot defensieve of strategische antwoorden. Of men weet het gewoon niet omdat men in de nieuwe constellatie nog geen ervaringen heeft opgedaan. Voorkom derhalve dat dit soort bijzondere omstandigheden de onderzoeksresultaten beïnvloeden. Wel kunnen bij een reorganisatie de vragen van de vertrouwenscan als nulmeting dienen wanneer vertrouwen een belangrijk aspect bij de reorganisatie vormt. Dan dienen de vragen van de vertrouwenscan op die randvoorwaarde te worden toegespitst.

- Niet onnodig zwaar instrumenteel opzetten

De vertrouwenscan (houden van interviews/uitwerking in een rapportage) is een intensieve werkwijze, zeker als daaraan extra eisen vanwege de zorgvuldigheid/gevoeligheid gesteld worden. Het is van belang het proces van de vertrouwenscan niet onnodig zwaar (instrumenteel) op te zetten of te vaak te herhalen. Verder moet worden gekeken naar een optimaal rendement ten opzichte van de inspanningen. Hoe kunnen de uitkomsten verbreed worden zodat de hele organisatie er iets van kan leren. Hoe kan een wijziging in 'mindset' van de medewerkers bewerkstelligd worden: internalisatie van de negen kritische succesfactoren als permanente aandachtspunten om de relatie met andere personen of organisaties een goede inhoud te geven.

- Zie vertrouwen niet louter als bezuinigingsinstrument (reden om 'eenzijdig' controle-inspanningen te verminderen)

Covey (2006) geeft aan dat vertrouwen zorgt voor meer snelheid en minder kosten. Cools (2005) benadrukt dat het in een sfeer van vertrouwen gewoon prettiger werken is en dat de motivatie en prestaties omhoog gaan. Redenen genoeg om in te zetten op meer vertrouwen. Hierbij past wel de kanttekening dat het propageren van vertrouwen met alleen als doelstelling te bezuinigen op de controlecapaciteit, averechts kan werken als daardoor de naleving vermindert en het aantal inbreuken stijgt (zie het openbaar vervoer in Amsterdam). Het inzetten op vertrouwen vergt investeringen, vooral in relationele sfeer en nalevingsbereidheid, zoals bij voorbeeld aandachtspunt is bij Horizontaal Toezicht. Alleen als de randvoorwaarden voor vertrouwen (de negen kritische succesfactoren) voldoende ingevuld zijn - waarvan **mogen** controleren er één is (KSF 6) - is het verantwoord de controle-inspanningen te verminderen vanwege de aanwezigheid van gerechtvaardigd vertrouwen. Maar zelfs dan zullen 'reality checks' en controles bij concrete signalen uitgevoerd moeten blijven worden[18]

- Afsluitend: Vertrouwen kan je niet verplichten of opleggen. Je kan vertrouwen wel op weg helpen. Je moet het alleen wel willen.

18 Zie in dit verband ook de dimensies controlekans, detectiekans en selectiviteit van de 'Tafel van Elf' (2010).

Het vergt vaak lef om vertrouwen te geven. Bereidheid om een zeker risico te accepteren is niet hetzelfde als blind vertrouwen. Zoals één van de forumleden zei: 'Wat je bij vertrouwen vooral moet doen is 'aan tafel zitten'! Persoonlijke communicatie verkleint de onderlinge afstand. Geen schriftelijke verhandelingen over en weer als het ook anders kan. Problematiek op transparante wijze aan de voorkant bespreken. Agendeer vooral ook de relationele aspecten. Wees duidelijk over de verwachtingen over en weer. Dit betekent ook het bespreken van de wederzijdse verantwoordelijkheden. Wat je vooral niet moet doen is te snel oordelen. Het devies is: Stel je oordeel uit! De verleiding bestaat om op een inbreuk direct in te springen met regels en controle. Tot slot het gaat natuurlijk niet om blind vertrouwen. Het gaat om gerechtvaardigd vertrouwen als basis om van daaruit monitoring en metatoezicht houden'[19].

De vertrouwenscan is echter nog geen vanzelfsprekend (aanvullend) instrument in het repertoire van alle auditors, controllers en opdrachtgevers. Een ervaring van één van de forumleden: de auditdienst vroeg in verband met een jaarlijkse controle of er intern onderzoek had plaatsgevonden ten aanzien van systeemgerichte contractbeheersing. Na het sturen van het plan van aanpak van de vertrouwenscan bleek dat de auditdienst alleen geïnteresseerd was in harde controle-informatie, niet in informatie die meer de relationele kant betrof.

Zoals de forumleden op de laatste vraag vanuit de zaal gezamenlijk antwoorden: meer uitgaan van vertrouwen is vooral een kwestie van gewoon doen. Het referentiekader van de negen kritische succesfactoren en de vertrouwenscan kan daarbij behulpzaam zijn. Maar je moet het wel zelf willen.

19 In de terminologie van Covey (2006): Smart Trust.

5. Afsluiting

'Vertrouwen geven, maar toch in control zijn' gaat niet uit van blind vertrouwen. Controle en gebruik maken van ervaringen zijn onlosmakelijk verbonden met gerechtvaardigd vertrouwen: 'Ga daarbij uit van de grote groep die geneigd is zich aan de regels te houden. Geef die vertrouwen, maar heb tegelijk wel oog voor de risico's'. Of zoals een eigenares van een winkel in een drukke winkelstraat het uitdrukte: 'Als ik iedere klant als een dief zou zien, zou ik snel mijn winkel kunnen sluiten. De meeste mensen zijn goede klanten en daar drijf ik op. Natuurlijk zijn er ook mensen die diefstal plegen. Uiteraard ben ik daar alert op en neem ik allerlei voorzorgsmaatregelen, maar dat mag niet ten koste gaan van hoe ik mijn goede klanten tegemoet treed'.

Deze benadering is de rode draad in de drie verschenen publicaties over dit thema, waarvan dit de derde en afsluitende is. In deze laatste publicatie is de verbinding gelegd tussen vertrouwen en systeemgericht toezicht: toezicht waarbij je vertrouwen hebt in het (management)systeem van de ander. Maar ook hier: geen blind vertrouwen, maar gerechtvaardigd vertrouwen. Het management control systeem van de organisatie moet wel een voldoende mate van volwassenheid kennen, of te wel in voldoende mate voldoen aan de negen kritische succesfactoren voor vertrouwen.

Daarnaast is uiteengezet hoe hoog betrouwbare organisaties functioneren in situaties waarin niets mis mag gaan vanwege de vergaande consequenties die dit zal hebben. Kunnen vertrouwen is daar essentieel, maar wel in de vorm van behoedzaam vertrouwen: vertrouwen dat als je het relateert aan de negen kritische succesfactoren overal een score van minimaal een 4 op een schaal van 1 tot 5 te zien geeft.

Tenslotte zijn de ervaringen met de negen kritische succesfactoren als referentiekader en de vertrouwenscan als concrete tool opgenomen. Conclusie: de negen kritische succesfactoren geven goed inzicht hoe vertrouwen werkt en waar het van afhankelijk is. De vertrouwenscan geeft aan waar een organisatie op dit moment in een relatie op het punt van vertrouwen staat: welke factoren op een goed niveau aanwezig zijn en welke factoren achterblijven. Daar zou een organisatie binnen de mogelijkheden gericht aan kunnen werken als die organisatie meer uit wil gaan van vertrouwen en toch in control zijn. Het gaat daarbij om een evenwichtige mix van zowel 'willen' en 'kunnen' als van 'hard controls' en 'soft controls'.

Als iedereen een klein stapje naar meer gerechtvaardigd vertrouwen zet, zetten we misschien met z'n allen gezamenlijk een grote stap.

Bijlage 1: het formulier van de vertrouwenscan

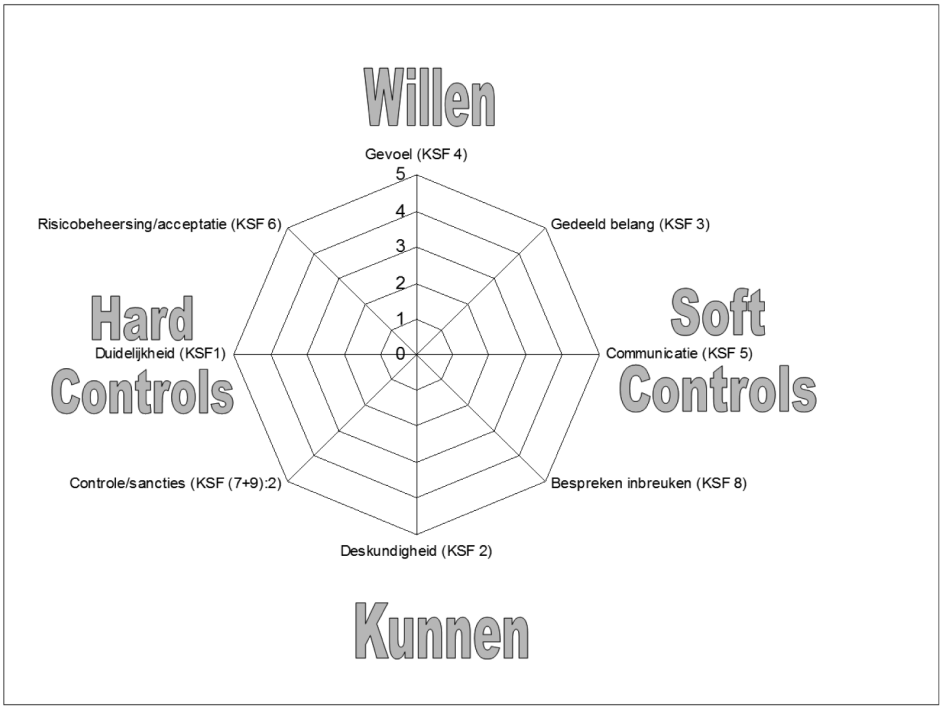
Figuur 3 Formulier Vertrouwen (model A)

Naam		Score	KSF	Algemeen beeld
Organisatie		1	KSF niet aanwezig	Vertrouwen/herstelvermogen afwezig
Datum gesprek		2	KSF onvoldoende aanwezig	Vertrouwen/herstelvermogen onvoldoende aanwezig
Subject van vertrouwen		3	KSF voldoende aanwezig	Vertrouwen/herstelvermogen voldoende aanwezig
Object van vertrouwen		4	KSF in goede mate aanwezig	Vertrouwen/herstelvermogen in goede mate aanwezig
		5	KSF volledig aanwezig	Vertrouwen/herstelvermogen volledig aanwezig

	KSF	Toelichting	Score
1.	Er bestaat bij de andere partij duidelijkheid over de essentiële verwachtingen.		
2.	De andere partij bezit de vereiste kwaliteit en om de verwachtigen waar te kunnen maken		
3.	Partijen hebben en houden een gedeeld belang		
4.	Er is (en blijft) een positief beeld (gevoel) over de andere partij		
5.	Er is een goede informetie-uitwisseling (open communicatie)		
6.	Er bestaat goed zicht op de risico's en zijn bereid deze te accepteren (risk-appetite)		
7.	Over de essentiële elementen die bepalen of de verwachtingen waargemaakt worden, mogen nadere vragen gesteld worden		
8.	De oorzaak van een verstoring wordt als die zich voorgedaan heeft, geanalyseerd en besproken		
9.	Er zijn effectieve sancties bij kwade opzet		

Algemeen beeld vertrouwen		Score
• Wat is de mate van vertrouwen en waarop is het vertrouwen gebaseerd (typering)? • Wanneer wordt het vertrouwen geschaad en hoe wordt dan het vertrouwen weer hersteld (herstelvermogen)?		

Bijlage 2: het spinnenwebdiagram



Literatuurlijst

- Argyris, C. en D. Schon, Organizational Learning: A Theory of Action Perspective. Reading, Mass. Addison-Wesley,1978.
- Belastingdienst, Vertrouwen, handleiding voor mensenwerk. Gedragslab, Utrecht, 2009.
- Benninga R., Nyenrode Alumni Magazine, Breukelen, 2007.
- Better Regulation Commission, Rsi, Responsibility and Regulation; Who's Risk is this Anyway? October 2006.
- Braithwaite, V., Defiance in taxation and governance, resisting and dismissing authority in a democracy. Cheltenham: Edward Elgar 2009.
- Bryan, B., M. Goodman en J. Schaveling, Systeemdenken, ontdekken van organisatiepatronen, Academic Service, Den Haag, 2006.
- Bree, M.A. de, Waste and Innovation. Berghauser Pont Publishers, Amsterdam, 2006.
- Bree M.A. de, Hoe Rijksinspecties omgaan met systeemtoezicht. Tijdschrift voor Toezicht, September 2010.
- Bree, M. A. de, Ontwikkelingen in systeemtoezicht in: Symposiumbundel Managementsystemen en Toezicht (blz. 51-60), Erasmus Instituut Toezicht & Compliance, Rotterdam, juni 2011.
- Bruine, H. de, P.D.F. Noordhoek en J. Tjon Tam Pau, Hoog betrouwbaar organiseren. M&O nummer 3, mei/juni 2010.
- Centrum voor Criminaliteit en Veiligheid (CCV), De Tafel van Elf, Utrecht, 2010.
- Cools, K., Controle is goed, vertrouwen nog beter. Van Gorcum, 2005.
- Covey S.M.R., The speed of trust, Business Contact, 2008.
- Fukuyama, F., (1995) Trust. Simon & Schuster Inc., New York.
- Gabriël-Breukers, S.K., Hulp bij Handhaving, WLP, Nijmegen, 2008.
- Goffau, L.A. de, Vertrouwen in horizontaal toezicht, Grafimedia Almere, Almere, 2008, ISBN 978-90-73081-47-5.
- Gunningham, N., en D. Sinclair, Regulation and the Role of Trust: reflections from the Mining Industry, Journal of Law & Society, 2009.
- Helderman, J.K., en M.E. Honing, Systeemtoezicht. Boom Juridische Uitgevers, 2009.
- Helderman,J.K., en M.E. Honing, Voor wie en wat is systeemtoezicht zinvol? Tijdschrift voor het Toezicht, 2010 (1) 2.
- Hollnagel, E., Extending the Scope of the Human Error in Erik Hollnagel (ed) Safer Complex Industrial Environments, A Human Factors Approach, CRC Press, Boca Raton, 2010.
- Huizinga, K. en M.A. de Bree, Introduction system based supervision environment and safety for large companies. VROM Inspectie, 2009.
- Inspectie Verkeer en Waterstaat, Afwegingskader systeemtoezicht. Den Haag, 2008.
- Meerman, P. & Wolfs, R. Projectverslag Systeemgericht Toezicht. Provincie Noord-Brabant, 2010.
- Ministerie van Financien, Brief d.d. 22 december 2004 inzake Rapport Interdepartementaal Beleidsonderzoek: regeldruk en controletoren, Tweede Kamer, vergaderjaar 2004-2005, 29950, nr. 1.
- Nooteboom, B., Vertrouwen. Vormen, grondslagen, gebruik en gebreken van vertrouwen. Academic Service, 2002.
- Parker, C., Regulatory-Required Corporate Compliance Program Audits, Law & Policy, Vol. 25 no. 3, July 2003.
- Perrow, C., Normal Accidents. Princeton University Press, Princeton,1999.
- Resar, R., Making Noncatastrophic Health Care Processes Reliable: Learning to Walk before Running in: Creating High Reliability Organizations, Health Research and Educational Trust, 1677-1689, 2006.

- Six, F.E., Meer vertrouwen of meer controle. Openbaar Bestuur, juni/juli 2009.
- Six, F., Vertrouwen in Toezicht. Tijdschrift voor Toezicht,(1) 4, 2010.
- VROM Inspectie, Juridische aspecten systeemgericht toezicht. Den Haag, 2009.
- Vos, R.O. en R.J. Witte, Vertrouwen en in control zijn; Gaat dat samen? Ministerie van Financiën, Den Haag, april 2009.
- Vos, R.O. en R.J. Witte, Vertrouwen en in control zijn; Hoe doe je dat? Ministerie van Financiën, Den Haag, december 2010.
- Weick, K.E. en K. M. Sutcliffe, Management van het Onverwachte. BBNC, Rotterdam, 2011

colofon
Ministerie van Financiën
Directie Begrotingszaken
Postbus 20201
2500 EE Den Haag

Oplage 1000
februari 2012

tekst ministerie van Financiën
vormgeving Jeannette Segaar, Rijksacademie voor Financiën, Economie en Bedrijfsvoering
productie Repro van de Kamp

In het kader van de doelstelling van vermindering regeldruk en controletoren is de directie Begrotingszaken van het ministerie van Financiën in 2009 gestart met het project 'vertrouwen geven, maar toch in control zijn'. Daarin staat de vraag centraal: onder welke voorwaarden kan je meer uitgaan van vertrouwen (en dus komen tot lagere controle kosten en een plezierigere werksfeer), en toch in control zijn (omdat er sprake is van gerechtvaardigd vertrouwen). Dit project sluit nauw aan bij de doelstelling van de activiteiten in IOFEZ verband in het kader van 'Minder gedoe'.

In het kader van dit project is allereerst op basis van een bestudering van de wetenschappelijke literatuur een referentiekader ontwikkeld voor het 'vertrouwen geven, maar toch in control zijn': de negen kritische succesfactoren. In de publicatie 'Vertrouwen geven en in control zijn; Gaat dat samen?' (april 2009) worden de negen kritische succesfactoren uitvoerig toegelicht. Op het congres van 25 juni 2009 waarin deze eerste publicatie gepresenteerd werd, bleek een grote behoefte te bestaan aan het verder uitwerken van dit referentiekader in een concrete tool.

Dit is de aanleiding geweest voor de tweede publicatie 'Vertrouwen geven en in control zijn; Hoe doe je dat? (december 2010) en het gelijknamige congres op 19 december 2010. Daarin werd de vertrouwenscan als tool gepresenteerd. De presentatie van deze tool leidde tot veel vragen over ervaringen met het toepassen van de vertrouwenscan. Deze vragen hebben geleid tot het organiseren van een derde en laatste congres over vertrouwen, nu met als thema 'Vertrouwen geven en in control zijn; En nu doen!' op 19 januari 2012. Tijdens dit congres is uitvoerig ingegaan op de ervaringen van vier organisaties die gebruik gemaakt hebben van het referentiekader van de negen kritische succesfactoren en de vertrouwenscan. Tevens werd op dit congres aandacht besteed aan systeemtoezicht en hoog betrouwbaar organiseren in relatie tot vertrouwen. In deze derde publicatie treft u een impressie aan van dit congres op basis van de verschillende bijdragen, met enige aanvullingen om tot een compleet afsluitend beeld te komen.