ISO 19600 over compliance management: geen excuses meer

Dr. mr. ir. Richard Hoff[1]

1. Inleiding

Op 15 december 2014 publiceerde de International Organization for Standardization (ISO) de ISO-richtlijn 19600: Compliance management systems – Guidelines.[2] Met deze richtlijn wil ISO guidance geven over compliancemanagementsystemen. Een ISO-richtlijn heeft het karakter van een advies en is geen formele norm. Bij een ISO-norm is er een aantal formele elementen waaraan een organisatie moet voldoen om een ISO-certificaat te kunnen krijgen.[3] De richtlijn ISO 19600 is dus geen certificeerbare ISO-norm.

De richtlijn is het resultaat van het werk van een ISO-werkgroep waaraan dertien landen hebben deelgenomen, waaronder Nederland (via de NEN normcommissie compliance-management).

Het kunnen beschikken over een internationale standaard voor compliancemanagement is de laatste jaren in belang toegenomen, met name vanwege de significante invloed en de extraterritoriale werking van wet- en regelgeving. ISO zelf merkt in de introductie van de richtlijn op dat ISO 19600 niet alleen organisaties in staat stelt om inhoud te geven aan compliance en om verplichtingen en verwachtingen na te komen, de richtlijn is volgens ISO ook een benchmark: "In a number of jurisdictions, the courts have considered an organization's commitment to compliance through its compliance management system when determining the appropriate penalty to be imposed for contraventions of relevant

1 Richard Hoff is toezichthouder bij het Expertisecentrum Integriteitstrategie van De Nederlandsche Bank. Hij schrijft dit artikel op persoonlijke titel.

2 ISO 19600:2014.

3 Zie: C.J.L. De Wannemaeker, 'De nieuwe ISO-compliancerichtlijn: een geïntegreerde benadering van compliance stevig verankerd in de nieuwste ISO-managementsystematiek', in: *Tijdschrift voor Compliance,* december 2014, p. 360. Zie ook: D. Hortensius & M. Veltheer, '"Risk-based" compliance management met ISO 19600', in: *Tijdschrift voor Compliance,* april 2015, p. 83.

laws. Therefore, regulatory and judicial bodies can also benefit from this International Standard as a benchmark."

Hoewel ISO 19600 geen certificeerbare norm is, maakt ISO wel duidelijk wat in haar ogen redelijke (formele) verwachtingen zijn ten aanzien van een effectief compliance-managementsysteem ('benchmark'). Dit kan ook juridisch van belang zijn. Zoals ISO zelf ook opmerkt: rechters wegen in de beoordeling van de situatie mee hoe een organisatie invulling geeft aan compliance.[4]

2. ISO 19600:2014

Het is van belang te beseffen dat ISO 19600 richtlijnen geeft voor een management-systeem. Volgens ISO zelf beschrijft een managementsysteem "the set of procedures an organization needs to follow in order to meet its objectives." De inhoud zal iedere organisatie zelf moeten inbrengen.

ISO 19600 beschrijft compliancemanagement als een vorm van risicomanagement. Dit sluit goed aan bij de Nederlandse context, waar in wetgeving wordt gesproken over integriteitsrisico's en het beheersen daarvan. In deze benadering is compliance een onder-deel van het proces van interne beheersing, waarbij compliance ziet op normbeheersing (value control).[5]

Compliance wordt in ISO 19600 gedefinieerd als "meeting all the organization's compliance obligations". Non-compliance is "non-fulfilment of a compliance obligation". Van belang is dan te weten wat een 'compliance obligation' is. ISO 19600 kiest hierin een ruime benadering en vat onder 'compliance obligation' zowel 'compliance requirements' als 'compliance commitments' (zie de figuur hieronder).

<table>
<tr><th colspan="2">Compliance Obligations</th></tr>
<tr><td>Compliance requirements:
requirements that an organization has to comply with</td><td>Compliance commitments:
requirements that an organization chooses to comply with</td></tr>
<tr><td colspan="2">Requirement: need or expectation that is stated, generally implied or obligatory</td></tr>
</table>

4 Zie ook: R.J. Hoff, *De integere onderneming, de bedrijfscode en het recht (diss. Twente)*, Waddinxveen: Nederlands Compliance Instituut en Zeist: Uitgeverij Kerckebosch 2006, p. 183-195.

5 Zie ook: J. Emanuels, Interne Beheersing: in control of in de krant? Beschouwing over een crisis, inaugurele rede Groningen, 2005.

Met deze definities sluit de ISO-richtlijn wederom aan op de Nederlandse context van het integriteitsrisico. De Nederlandse wetgever verwacht van organisaties (m.n. financiële ondernemingen) dat zij hun integriteitsrisico's beheersen. Dit is meer dan het naleven van de wet (dat ook!); het gaat ook om, kort gezegd, het voldoen aan gerechtvaardigde verwachtingen.[6] Een van die verwachtingen zal bijvoorbeeld zijn het naleven van de eigen gedragscodes.

Het is dan ook logisch dat ISO 19600 in feite het complianceproces laat beginnen met het begrijpen van de context van de organisatie. Dit betreft onder meer:

- relevante issues die van belang zijn voor de organisatie, de doelstellingen en de compliancerisico's;
- eisen, wensen en verwachtingen van stakeholders;
- regulatory context.

Risk-based benadering

Verder dient een organisatie volgens ISO 19600 in hoofdzaak de volgende stappen te doorlopen, die overigens zijn afgeleid van het risicomanagementproces volgens ISO 31000 en die ook daarnaast niet verrassen:[7]

1. bepalen van de 'compliance obligations';
2. bepalen van de compliancerisico's;
3. nemen van beheersmaatregelen of controls.

Bepalen compliance obligations	De organisatie dient de relevante verplichtingen te identificeren alsmede de invloed op activiteiten, producten en diensten. ISO 19600 noemt de nodige bronnen waaruit verplichtingen kunnen voortvloeien, bijvoorbeeld: • wet- en regelgeving; • vergunningen; • rechterlijke uitspraken; • gedragscodes; • industriestandaarden. Van belang is dat ISO 19600 stelt dat organisaties processen moeten hebben om wijzigingen hierin te detecteren en de impact daarvan te bepalen. De richtlijn geeft voorbeelden van hoe men actueel kan blijven, o.a. aangesloten zijn bij professionele groepen, bezoeken van seminars en monitoring van de diverse bronnen.

6 Zie bijvoorbeeld: artikelen 3:10, 3:17 Wet op het financieel toezicht (Wft).

7 D. Hortensius & M. Veltheer, '"Risk-based" compliance management met ISO 19600', in: *Tijdschrift voor Compliance,* april 2015, p. 84.

Bepalen compliancerisico's	ISO 19600 ziet de compliance risk assessment als de basis voor de implementatie van het compliancemanagement-systeem en voor de allocatie van mensen en middelen ter zake. De richtlijn onderscheidt twee stappen. a. De organisatie dient compliancerisico's te identificeren "by relating its compliance obligations to its activities, products, services and relevant aspects of its operations in order to identify where noncompliance can occur. The organization should identify the causes for and consequences of noncompliance." b. De organisatie dient compliancerisico's te analyseren. Hier overweegt de organisatie kans en impact.
Nemen beheersmaatregelen	Om risico's te beheersen dienen beheersmaatregelen genomen te worden. Hieraan vooraf gaat de risico-evaluatie. Daarbij wordt de hoogte van de geïdentificeerde compliance-risico's vergeleken met wat de organisatie acceptabel vindt (risk appetite). Dit vormt de basis voor de (noodzaak voor) controls en de prioriteitstelling. Afhankelijk van de omvang van de compliancerisico's wordt gekozen voor meer of minder vergaande beheersmaatregelen en voor meer of minder intensieve monitoring. Volgens ISO 19600 betekent een risicobenadering niet het gecalculeerd niet-naleven van regelgeving ('we betalen de boete wel'), wel leidt het tot focus op de belangrijkste nalevingsverplichtingen.[8]

Een compliance risk assessment moet periodiek plaatsvinden, en ook bij het optreden van events, zoals nieuwe producten en/of activiteiten, gewijzigde compliance obligations, non-compliance, gewijzigde externe omstandigheden.

Zoals hiervoor al is aangegeven sluit het gedachtegoed van ISO 19600 aan bij het gedachtegoed van de Nederlandse wetgever ter zake. Voor financiële ondernemingen kent de Wft c.a. namelijk al geruime tijd de verplichting tot het uitvoeren van een systematische integriteitrisicoanalyse. Gezien het feit dat DNB onlangs heeft moeten vaststellen dat meer dan 80% van de analyses niet voldoet en dat er vele instellingen zijn die niet over een integriteitrisicoanalyse beschikken, is het opmerkelijk en van belang dat ISO 19600 dit aspect expliciet benoemt. Dat mag als een onderstreping gelden. Immers, zonder integriteitrisicoanalyse kan een organisatie de integriteitgerelateerde

8 D. Hortensius & M. Veltheer, '"Risk-based" compliance management met ISO 19600', in: *Tijdschrift voor Compliance,* april 2015, p. 84.

verplichtingen niet risicogebaseerd naleven. De integriteitrisicoanalyse is een voorwaarde voor een toereikende inrichting van de integere bedrijfsvoering.[9]

Controlcyclus

ISO 19600 gaat vervolgens gedetailleerd in op de beheersmaatregelen, de controlcyclus en op het documenteren daarvan. Kort gezegd beschrijft de richtlijn het volgende.

Planning	Bij planning gaat het erom om acties te definiëren die de compliancerisico's adresseren. De richtlijn geeft daarbij aan dat planning ook omvat hoe de acties in het geheel van het managementsysteem worden geïntegreerd en hoe de effectiviteit van de acties wordt gemeten. Om de compliancedoelen te bereiken zal de organisatie moeten bepalen wat gedaan moet worden, welke mensen en middelen daarvoor nodig zijn, wie verantwoordelijk is en wanneer de realisatie voltooid is.
Operation	De vereiste acties worden vertaald in processen, controls en procedures, en deze dienen geïmplementeerd te worden. Dit vereist planning en control op operationeel niveau. De richtlijn noemt de nodige voorbeelden van controls en procedures, en benadrukt dat deze onderhouden en periodiek getest moeten worden met het oog op de effectiviteit. De richtlijn besteedt apart aandacht aan het outsourcen van processen en de implicaties daarvan vanuit compliance-perspectief.

9 DNB heeft hier onlangs een document met good practices over gepubliceerd (De Nederlandsche Bank, De integriteitrisicoanalyse. Meer waar dat moet, minder waar dat kan, 2015). Hierin komt overigens dezelfde systematiek als die van de ISO-richtlijn naar voren.

Performance evaluation	Op het onderdeel 'performance evaluation' gaat ISO 19600 diep in. Dit geeft aan dat de richtlijn veel belang hecht aan dit onderdeel. Met name het onderdeel 'monitoring' krijgt de nodige aandacht. Compliance monitoring wordt daarbij gedefinieerd als: 'the process of gathering information for the purpose of assessing the effectiveness of the compliance management system and of the organization's compliance performance.' Aspecten als informatiebronnen, informatieverzameling, analyse, indicatoren, (inhoud van) rapportages en record-keeping worden door de richtlijn in dit kader behandeld. Voorts geeft de richtlijn aan dat de organisatie regelmatig een audit moet uitvoeren met betrekking tot het compliance-managementsysteem en, belangrijk, dat het topmanagement het compliancemanagementsysteem – inclusief de performance – regelmatig moet evalueren.
Improvement	Volgens ISO dient het systeem voorzieningen te bevatten voor continue verbetering. Dat begint bij het nemen van corrigerende maatregelen in geval van non-compliance. De richtlijn legt ook de vinger op de noodzaak om in een dergelijk geval na te gaan wat de oorzaken zijn (root cause analysis). Dit kan leiden tot de nodige acties ter verbetering, die vervolgens geïmplementeerd moeten worden. De voort-gang en effectiviteit dienen daarbij vastgesteld te worden. ISO 19600 besteedt ook aandacht aan escalatieprocedures. Rapportage aan hogere organen of aan autoriteiten kan in sommige gevallen van non-compliance nodig zijn, en het compliancemanagementsysteem moet hierin voorzien. Opvallend is dat de richtlijn aangeeft dat een compliance-managementsysteem een soort klokkenluidervoorziening moet bevatten. Medewerkers moeten vertrouwelijk (vermoedens van) normschendingen kunnen melden, zonder dat dit negatieve gevolgen voor hen heeft.

Leadership en governance

De ISO-richtlijn besteedt relatief veel aandacht aan 'leadership and commitment'. Een goed functionerend compliancemanagementsysteem staat of valt met het juiste leiderschap en met een duidelijk commitment van het topmanagement. De richtlijn werkt uit hoe dat vorm kan krijgen en zichtbaar dient te worden. Dit dient onder meer terug te komen in het beleid en in verantwoordelijkheid.

De richtlijn heeft ook de nodige aandacht voor de governance. Actieve betrokkenheid van het bestuur en de interne toezichthouders (raad van commissarissen) acht de richtlijn van cruciaal belang. Tevens zullen deze organen de juiste besluiten moeten nemen met het oog op compliance – de richtlijn geeft aan wat hierin ten minste verwacht mag worden. Verder wordt redelijk gedetailleerd aandacht besteed aan de compliance officer c.q. compliancefunctie, diens positie, taken, verantwoordelijkheden en onafhankelijkheid. De richtlijn stelt daarbij wel dat het management verantwoordelijk moet zijn voor compliance. Overigens vermeldt de richtlijn hier wederom vertrouwde zaken.[10]

Awareness en cultuur

ISO 19600 benoemt ook het belang van awareness en training, en ook hier benoemt de richtlijn niet alleen het belang, maar geeft zij ook voorschriften ter zake. Daarnaast gaat de richtlijn in op de compliancecultuur en op factoren die de cultuur in positieve zin beïnvloeden.

Hortensius en Veltheer melden dat Nederland gepoogd heeft om gedragsbeïnvloedende factoren te benoemen in de richtlijn. Hoewel dat niet expliciet gelukt is, menen zij dat de relevante factoren – die bijvoorbeeld aansluiten bij de zeven elementen voor een integere bedrijfscultuur zoals gedefinieerd door DNB – terug zijn te vinden in ISO 19600. En wel in voldoende mate om organisaties handvatten te bieden om cultuur en gedrag voor compliance en integer handelen te structureren.[11] Elementen van gedrag en cultuur zijn in de richtlijn met name terug te vinden waar het gaat over leiderschap & commitment, verantwoordelijkheden en awareness. In dit laatste onderdeel worden gedrag en cultuur als afzonderlijke onderdelen toegelicht. Hierbij worden onder meer genoemd: waarden, voorbeeldgedrag van het management, consistentie in de toepassing van normen en training & communicatie.

3. Afsluitende opmerkingen

ISO 19600:2014 biedt veel. De richtlijn is compleet, en vastgesteld kan worden dat als een organisatie aan deze richtlijn voldoet er sprake is van een hoogwaardig compliancemanagementsysteem. Mooi is dat de richtlijn ook aansluit bij de Nederlandse context. Daarbij is de richtlijn niet vernieuwend; bekende inzichten met diverse invalshoeken worden gestructureerd op een rij gezet. De prestatie om dat in een richtlijn van minder dan dertig pagina's te vatten mag gehonoreerd worden, en daarbij is het krachtig. Er is

10 Zie bijvoorbeeld: Basel Committee on Banking Supervision, Compliance and the compliance function in banks, Bank for International Settlements: 2005.

11 D. Hortensius & M. Veltheer, '"Risk-based" compliance management met ISO 19600', in: *Tijdschrift voor Compliance,* april 2015, p. 85.

geen excuus meer: het moge bekend zijn hoe een effectief compliancemanagement-systeem opgezet en geïmplementeerd wordt en welke randvoorwaarden daarvoor gelden.

Een interessante vraag is natuurlijk of een organisatie met het volgen van de ISO-richtlijn ook voldoet aan de wettelijke vereisten, bijvoorbeeld die uit de Wft. Dat is niet zo te zeggen. Men kan redelijk veilig aannemen dat aan bepaalde formele vereisten wel voldaan zal zijn. Echter, het daadwerkelijke commitment dient van de organisatie zelf te komen; het is moeilijk in te zien waarom de ISO-richtlijn daar meer succesvol in zou zijn dan de wet. Daarbij geldt dat ISO een raamwerk definieert, de organisatie bepaalt nog altijd de inhoud. Als dat laatste niet goed op orde is, dan is de uitkomst van het compliancemanagementsysteem eveneens onder de maat. Met andere woorden: het materieel op orde hebben van een beheersingskader wordt met deze richtlijn, zoals bij alle richtlijnen, niet per definitie gerealiseerd.

Dit alles benadrukt de noodzaak dat de organisatie zelf de verschillende verplichtingen en gerechtvaardigde verwachtingen goed in kaart moet brengen. Ook zal de integriteit-risicoanalyse op orde moeten zijn alsmede de (inhoudelijke) follow-up daarvan in termen van activiteiten, beheersing en prioriteitstelling.

Ten slotte worden integriteit en compliance vooral zichtbaar in de activiteiten en transacties van elke dag en in het beleid dat in de praktijk gevoerd wordt. Daarin komt het aan op het hebben van een oordeel. Geen compliancemanagementsysteem is opgewassen tegen het 'geen mening' van bijvoorbeeld de compliance officers of tegen het 'begrijpen van de juiste prioriteiten'. De vele cases, bijvoorbeeld die van BNP Paribas die elders in dit Jaarboek wordt beschreven, getuigen daarvan.