Nederlands Compliance Instituut
Jan Leentvaarlaan 61-63
3065 DC ROTTERDAM
Per email: p. westdijk@compliance-instituut.nl

De Nederlandsche Bank
Postbus 98
1000 AB Amsterdam
Per email: consultatie@dnb.nl

Rotterdam, 16 januari 2025

Betreft: Reactie consultatie DNB SIRA Good Practices

Beste mevrouw, meneer,

Hierbij reageer ik namens het Nederlands Compliance Instituut op uw consultatie van de "DNB SIRA Good Practices".

Wij verwelkomen deze nieuwe good practices voor de SIRA. De voornaamste reden hiervoor is dat met deze nieuwe versie vooral de status van deze good practices duidelijker is geworden. Het is de bedoeling dat dit een handreiking is met betrekking tot de manier waarop instellingen hun SIRA zouden kunnen uitvoeren. Het is expliciet geen regel die rigide gevolgd moet worden. Zoals wij opmaken uit het document, ligt de kern in het zélf definiëren en beschrijven van de organisatie, producten, klanten en dergelijke. Vervolgens is het ook de taak om zelf daaruit de inherente integriteitsrisico's te destilleren. Hiermee worden de inspanningen gericht op de organisatie zelf en wordt niet (meer) gekunsteld gezocht naar een manier om de 'standaardrisico's' naar de eigen organisatie toe te schrijven. Dit verhoogt naar onze mening de waarde van de inspanningen en de uiteindelijke kwaliteit van het eindproduct. Dat ondersteunt ook het oorspronkelijke doel: de SIRA als beleids- en sturingsdocument. Met de nieuwe guidance wordt de SIRA het actuele risicoprofiel van de instelling en daarmee een ijkpunt voor het beoordelen van wijzigingen in de context en hun invloed op het risicoprofiel.

Naar onze mening biedt de pragmatische toon van de nieuwe good practices goede guidance voor instellingen en hun adviseurs en ook duidelijkheid in de discussie tussen instellingen en hun toezichthouders. Hiermee beantwoorden we dan ook de expliciet gestelde consultatievraag[1] bevestigend.

[1] De consultatievraag luidt: "DNB streeft ernaar in de SIRA Good Practices handvatten te bieden die bijdragen aan een risicogebaseerde invulling van de verplichtingen uit wet- en regelgeving. Is in het consultatiedocument overal voldoende duidelijk dat de good practices indicatief zijn en het instellingen vrij staat om een andere invulling te kiezen, zolang men voldoet aan wet- en regelgeving?"

Onderstaand gaan wij meer in detail in op enkele observaties van de consultatieversie:

1) In de inleiding (vanaf pagina 3) wordt een expliciete relatie gelegd tussen de SIRA en de wettelijke vereisten vanuit de Wft. Wij zien bij klanten dat ook andere integriteitsaspecten in de SIRA worden opgenomen, die onder het begrip 'maatschappelijk onbetamelijke handelingen' zouden kunnen worden geschaard. Enige toelichting op dit begrip en wellicht ook mogelijke voorbeeldscenario's kan instellingen helpen om dergelijke onderwerpen ook mee te (gaan) nemen in hun organisatierisicoprofiel. Dit zien wij als zeer wenselijk.
2) In het derde hoofdstuk (pagina 10) legt u de voorbereiding van de SIRA bij de compliance officer. Hierbij neemt u in uw beschrijving een aantal (potentiële) taken op, waaronder het bepalen van een plan van aanpak. Hier blijkt niet duidelijk waar de verantwoordelijkheid van de compliance officer eindigt. Men zou kunnen lezen dat deze de initiator en aanjager is terwijl het, ons inziens, wenselijk is dat juist een eerste lijn hier de verantwoordelijkheid draagt. Dit zou explicieter benoemd mogen worden.
3) Het derde hoofdstuk (vanaf pagina 10) beschrijft vele risicofactoren, toegespitst op de verschillende soorten instellingen. Het valt ons op dat de factor 'mens' hierbij beperkte aandacht krijgt. Inherent aan ondernemen is de inzet van personeel. Mensen kunnen zich niet-integer gedragen en dit geldt niet alleen voor leden van het bestuur van de instelling. Wij zijn van mening dat een instelling zich zou moeten afvragen of en in welke mate, in welke situaties en wanneer gedrag van medewerkers een integriteitsrisico kunnen vormen. Bij menselijke besluitvorming of een hoge exposure tot informatie of (geldelijke) waarden zou dat bijvoorbeeld een risicofactor kunnen zijn.
4) Het document besteedt expliciet aandacht aan de rol van compliance en audit, bijvoorbeeld op de pagina's 7, 10, 11, 12, 17, 29 en 31. We zien echter geen expliciete aandacht voor de functie van Risk Management. Mogelijk is dit een toevoeging die licht werpt op de mogelijke verhoudingen en verdeling van taken, rollen en bevoegdheden.
5) Is het in navolging van het vorige punt van feedback wellicht een idee om in dit kader meer toelichting te geven op de wenselijkheid van de onafhankelijke rol van bijvoorbeeld de compliance officer? In de praktijk blijft er veel vraag naar de werkelijke betekenis van dit woord, zeker als in de good practices zou blijven staan dat de compliance officer de SIRA voorbereidt. We verwachten in de praktijk dat de vervolgstap van 'voorbereiden' naar het in onze ogen zeer onwenselijke 'uitvoeren' erg klein zou kunnen worden.
6) In algemene zin valt op dat in het good practice document een groot aantal voorbeelden in de groene blokken soms zeer gedetailleerd is uitgewerkt. Vanuit het oogpunt van uitleg en toelichting in deze guidance is dat verklaarbaar. Voor grote en/of complexe instellingen kan deze mate van detaillering leiden tot een grote inspanning om alle risicoscenario's op een dergelijk detailniveau uit te werken. Wij zijn van mening dat dit ongewenst kan zijn, aangezien hierdoor het inzicht in en overzicht van de integriteitsrisico's niet wordt gediend. Ook zou deze grote mate van detaillering toch weer de neiging kunnen stimuleren om deze voorbeelden rule-based te interpreteren en (blind) te volgen. Mogelijk kan een expliciete herhaling van het beginsel van risicogebaseerd analyseren hier een zinvolle toelichting vormen.

7) De individuele good practice voorbeelden zijn in alle hoofdstukken grotendeels toegespitst op een bepaald type instelling; dit bevordert de duidelijkheid van de desbetreffende good practice. Mogelijk nadelig effect hiervan is echter dat alleen de good practice voorbeelden van het ‘eigen’ type instelling als guidance worden gebruikt, waardoor zinvolle informatie vanuit een good practice van een ander type instelling minder aandacht krijgt. Mogelijk kan in de formulering of lay-out hierop worden gewezen.
8) Veel integriteitsrisico’s hebben betrekking op zaken die al in wet- en regelgeving zijn opgenomen. Er zijn bijvoorbeeld uitgebreide richtlijnen met betrekking tot maatregelen die genomen moeten worden ter voorkoming of bestrijding van witwassen. Wellicht kunt u in de SIRA good practice opnemen wat de invloed van dergelijk wettelijk geformuleerde bestaande maatregelen op de SIRA is en hoe instellingen hiermee rekening kunnen houden in het proces van totstandkoming van de SIRA.

Met bovenstaande feedback heb ik gepoogd concrete verbetermogelijkheden aan te geven. Vanzelfsprekend ben ik graag tot nadere toelichting bereid. U kunt mij hiervoor rechtstreeks benaderen.

Ik geef hierbij toestemming voor het vermelden van mijn naam, functie en bedrijfsnaam bij de inhoudelijke reactie.

Met vriendelijke groeten,

Peter Westdijk

Senior Compliance Officer Nederlands Compliance Instituut