VERBOND VAN VERZEKERAARS

16 januari 2025

Graag maken wij gebruik van de mogelijkheid om te reageren op de nieuwe consultatieversie ‘DNB SIRA Good Practices’

Onze algemene conclusie is dat het document een goed hulpmiddel biedt voor het SIRA-proces. Het geeft met de diverse praktijkvoorbeelden meer en beter inzicht in de wensen van DNB en de vastleggingen daarvan. Wij zien het stuk als een belangrijke verbetering ten opzichte van de vorige versie. Het zou waardevol zijn als het document nog concreter wordt met meer procesmatige voorbeelden die voor een grote groep instellingen relevant zijn. Hieronder zullen wij daar nader op ingaan.

Ons antwoord op de algemene consultatievraag van DNB luidt bevestigend. Wij vinden dat het document voldoende duidelijk maakt dat het handvatten biedt, een leidraad is, praktijkvoorbeelden geeft en ruimte biedt om een eigen invulling te geven afhankelijk van de situatie. Dit blijkt volgens ons voldoende uit het door DNB gehanteerde woordgebruik op diverse plekken in het document.

<u>Algemene feedback / vragen</u>

- Veel praktijkvoorbeelden in de Good Practices gaan over bankinstellingen. Graag zien wij ook praktijkvoorbeelden en uitwerkingen voor schade- en/of levensverzekeraars.
- Op zich is het duidelijk wat de scope van de SIRA is en wie deze moeten doen, namelijk vergunning houdende instellingen. Meer duiding voor de procesmatige aanpak voor onderdelen in een grote groepsstructuur (inclusief centrale afdelingen) zou echter ook waardevol zijn.
- Het document laat met de praktijkvoorbeelden zien hoe je de risicoanalyse kan onderbouwen met data, wat in onze ogen een goede verbetering is van het SIRA-proces en de SIRA-analyse. De gegeven voorbeelden bevatten alleen/vooral harde, feitelijke data. Omdat het hier over integriteitsrisico’s gaat, zien wij ook graag praktijkvoorbeelden van hoe om te gaan met cultuur en gedrag, vooral in de combinatie met de hardere data. Bijvoorbeeld gekoppeld aan uitkomsten van cultuuronderzoek onder medewerkers, meldingen aan klokkenluiders etc.
- Op diverse plaatsen geeft het document aan dat de SIRA op ‘continue basis’ dient uitgevoerd te worden, maar onduidelijk blijft wat DNB daarbij precies verwacht of wat DNB daar voor good practice op ziet. Wellicht kan hier iets over worden toegevoegd?
- Sommige good practices klinken logisch maar bevatten algemeenheden door de gebruikte werkwoorden, b.v. ‘betrekken van’, ‘creëren’. Is het mogelijk dit aan te scherpen door het resultaat te beschrijven (wat levert dat ‘betrekken’ concreet op’, bijvoorbeeld aan de hand van een voorbeeld van input vanuit verschillende invalshoeken)?
- Bij een aantal good practices -bijvoorbeeld bij de betaaldienstverlener- blijft de vraag “hoe”? Hoe weet je via welke (buitenlandse) platformen je klant actief is in crypto?

Feedback/vragen per slide

Slide 3:

- De invulling van het begrip integriteit kan naar onze mening duidelijker. Er worden wel voorbeelden gegeven van integriteitsdossiers, maar het blijft onduidelijk waar de selectie op gebaseerd moet worden. Dit bemoeilijkt de toepassing van het SIRA-framework buiten de nu gegeven voorbeelden.
- Integriteit wordt hier ook over de Pw en Wvb getrokken terwijl deze wetgeving voornamelijk uitvoerend van aard is. Dit impliceert dat alle uitvoeringsbeginselen die gesteld kunnen worden onder de noemer integer bestuur vanuit de Wft en Solvency II binnen de scope getrokken worden. Deze interpretatie komt later in het document verder niet direct terug.
- Er wordt gesteld dat de SIRA gebruikt kan worden ter informatie of als sturingsdocument door het bestuur. Deze vrijblijvendheid strookt niet met andere uitingen in het document (slide 8: de SIRA is de hoeksteen van integriteitsmanagement, sheet 32 Betrokkenheid Raad van Bestuur) en het belang dat DNB hecht aan de SIRA in haar toezicht.

Slide 3 en 4:

- Op slides 3 en 4 wordt een paar keer de SIRA als document genoemd. Op slide 4 zelfs als een (dynamisch) document. Andere uitingen in het Good Practices document geven aan dat de vastlegging vormvrij is en naar eigen keuze te realiseren. Dat lijkt tegenstrijdig. Er kan duidelijker onderscheid worden gemaakt tussen de SIRA als assessment, als dynamisch proces versus hoe die SIRA vervolgens aantoonbaar kan worden gemaakt. Op slide 3 wordt aangegeven dat dat met meerdere documenten kan. Belangrijk om te weten dat de SIRA verbonden kan zijn met allerlei andere (risk) assessments en risk rapportages en voor sommige bedrijven onderdeel is van een groter risk management framework (met alle risico's, financial en non financial). → Zie ook de feedback bij slide 8.

Slide 4:

- De Wwft behandelt geen terrorisme financiering zoals deze onder de SW valt.

Slide 7:

- 'DNB gaat ervan uit dat instellingen deze bronnen (beleidsuitingen) meenemen in de SIRA'. In de Good Practices wordt niet aangegeven hoe dit kan worden aangetoond/vastgelegd. Dit kan naar onze mening alleen/vooral procesmatig worden aangetoond, vooral omdat het om veel wet- en regelgeving gaat en de hele Legal wereld dan in de SIRA wordt getrokken. Kan DNB meer duidelijkheid geven of zij ook op deze lijn zitten?
- Risicogerichte benadering: hoe toepasbaar op integriteitsrisico's waar naleving van wet- en regelgeving noodzakelijk is? Zowel in de aandacht voor de verschillende wetten als in de naleving daarvan is weinig keuzevrijheid. Graag meer duidelijkheid geven wat hier nu wordt bedoeld en hoe met wet- en regelgeving toch een risicogerichte benadering is toe te passen?

Slide 8:

- 'De SIRA is daarmee een belangrijke bouwsteen, zo niet de hoeksteen van het integriteitsrisicomanagement'. Vanuit het DNB-toezichtperspectief snappen wij deze uitspraak. Vanuit een managementperspectief is het SIRA-proces en assessment een onderdeel van een groter riskmanagementproces, framework en assessment: van Strategisch Risk Assessment, naar High Level Risk Assessment en diverse (op onderwerp) Detailed Risk Asssessments, inclusief de verschillende riskrapportages.

Kan de Good Practices meer aandacht geven aan het feit dat de SIRA-onderdeel is van dit grotere geheel? Het lijkt nu het enige, ultieme proces en assessment. Wellicht kan DNB bij par 1.1 duidelijk maken dat integriteitsrisico's 1 van de risicogebieden zijn die instellingen kunnen raken en waar DNB toezicht op houdt

Slide 10:

- In de eerste good practice (het groene blok) staat de compliance officer als uitvoerende partij genoemd. Dit komt daarna in diverse groene blokken zo terug. Het lijkt daardoor of de SIRA een proces is van de 2e lijn Compliance. Naar onze mening moet hier het 3 lines of defence model op een juiste manier worden toegepast. De 1e lijn (namens/voor de Raad van Bestuur) voert een SIRA uit, de 2e lijn Compliance reviewt en challenget en geeft een opinie over het proces en de inhoud en de 3e lijn (internal audit) audit het hele proces inclusief de samenwerking 1e en 2e lijn. Ook worden de Raad van Bestuur en de 3e lijn nog wel eens genoemd als uitvoerende of als bron, wat zorgt voor onduidelijkheid in rollen en verantwoordelijkheden.
- Bij verschillende instellingen is het een proces geweest om betrokkenheid/awareness/verantwoordelijkheid bij de SIRA te ontwikkelen. Daarmee doelen wij op verantwoordelijkheid van het management en daarvan afgeleid 1e lijn, ondersteund door riskfunctie en compliance, met in het bijzonder de reflectie rol op proces en kwaliteit van de SIRA van Compliance. SIRA werd gezien als risk aangelegenheid of compliance activiteit. Door bij de Good Practice Compliance als proces verantwoordelijke op te nemen wordt een ongelukkig signaal afgegeven. Wij zouden hier liever een zin zien als 'Een door de organisatie aan te wijzen functie of functionaris': dat laat ruimte voor organisatie specifieke invulling. Of, zoals later wordt geschreven 'degene die verantwoordelijk is voor de SIRA'. Elke kans op interpretatie van SIRA als sec risk of compliance aangelegenheid/verantwoordelijkheid moet worden voorkomen. Bij hoofdstuk 6 komt de monitoring rol van bijvoorbeeld compliance wel terug, en dat kan niet samen met verantwoordelijkheid voor uitvoering.

Slide 18:

- Bij 'witwas indicatoren' voor een levensverzekeraar wordt het gebruik van een externe bron (EBA) als good practice genoemd. Door de laatste alinea in dit voorbeeld kan de indruk worden gewekt dat enkel op basis van het raadplegen van de EBA guideline geconcludeerd kan worden dat het een laag risico is. Dit voorbeeld kan verder worden aangescherpt.

Slide 26:

- Er wordt hier gesproken over een SIRA voor een specifiek onderwerp, namelijk het wel of niet zakendoen in Zuid-Amerika. Naar onze mening is dat een specifiek detailed risk assessment (met grote focus ook op integriteit). Om verwarring te voorkomen met SIRA als totaal proces en totaal assessment hier een andere term voor gebruiken of uitleggen? Wij zijn het wel eens met het feit dat diverse specifieke detailed risk assessments input zijn voor de overall SIRA. Misschien schrijven: "tijdens uitvoeren van DE SIRA". Met daarbij de toelichting dat het een specifieke SIRA kan zijn, een gangbare integrale SIRA of een riskassessment in welke vorm dan ook.