

Good practice
Integrity Risk Appetite

DeNederlandscheBank

EUROSYSTEEM

Inhoud

Inleiding	3
1 SIRA als basis voor risicobeheersing	4
2 Vormgeving van de integrity risk appetite	5
3 De-risking	8
4 Status van deze good practice	9

Inleiding

DNB heeft de afgelopen jaren nadrukkelijk aandacht gevraagd voor de kwaliteit van systematische integriteitsrisicoanalyses (SIRA's) als basis voor een goede risicobeheersing. Belangrijk onderdeel van de risicobeheersingscyclus is dat financiële instellingen doorlopend bewuste keuzes maken over integriteitsrisico's (witwassen, terrorismefinanciering, corruptie, etc.): welke risico's wilt u als financiële instelling accepteren, welke risico's moeten vermeden of verkleind worden door beheersmaatregelen te treffen. Deze keuzes kan uw instelling het beste maken als u een heldere integrity risk appetite geformuleerd heeft. DNB sluit hiermee aan bij het FSB rapport '*Principles for An Effective Risk Appetite Framework*', van 18 november 2013. Ook eerder al hebben wij aandacht gevraagd voor de financial risk appetite, in het kader van het onderzoek Effectiviteit risicobeheer¹.

DNB geeft hierbij nadere informatie over de integrity risk appetite, naar aanleiding van de bevindingen uit het huidige, in 2016 gehouden, verkennende onderzoek naar de invulling van de integrity risk appetite. Doel van dit verkennende onderzoek was om vast te stellen in welke mate financiële instellingen hun risk appetite op het terrein van integriteitsrisico's hadden geëxpliciteerd, en of zij daadwerkelijk bewuste keuzes maakten over de omgang met de verschillende integriteitsrisico's die zijn verbonden aan het bedrijfsmodel en de uitoefening van de bedrijfsactiviteiten. Zoals aangekondigd in juni 2016 en in latere nieuws-

brieven hebben we met name onderzocht of de uitkomsten van de SIRA getoetst werden aan de integrity risk appetite en de betrokkenheid en rol van medewerkers/afdelingen bij de totstandkoming ervan.

Uit ons onderzoek is gebleken dat veel financiële instellingen niet duidelijk kunnen maken hoe zij hun integrity risk appetite expliciteren en welke functie deze binnen hun organisatie kan vervullen. Om te helpen bij het vormgeven en invullen van een goede integrity risk appetite, geven we in deze brochure nadere toelichting. Wij staan in dit verband ook stil bij het onderwerp de-risking, één van de manieren om als financiële instelling met integriteitsrisico's om te gaan. Bij de-risking wordt er, in de definitie die ook de Financial Action Task Force (FATF) gebruikt, categoriaal afscheid genomen van cliënten omdat er sprake is van onaanvaardbare integriteitsrisico's, maar zonder dat hier een individuele risicoafweging heeft plaatsgevonden.

¹ In te zien via <https://www.dnb.nl/publicatie/publicaties-dnb/nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-mei-2014/dnb307212.jsp>.

1 SIRA als basis voor risicobeheersing

4

In dit hoofdstuk gaan wij nader in op de rol van de SIRA binnen het proces van risicobeheersing van een financiële instelling.

Beheerste en integere bedrijfsvoering

Iedere financiële instelling moet een integere en beheerste bedrijfsvoering waarborgen; dat is vastgelegd in de bepalingen die in hoofdstuk 4 staan weergegeven. Een integere bedrijfsvoering vereist dat uw instelling maatregelen treft om te voorkomen dat zij of haar medewerkers betrokken raken bij witwassen, terrorismefinanciering, corruptie en belangenverstremgeling, wetsovertredingen en/of andere handelingen die maatschappelijk onbetamelijk zijn, waardoor het vertrouwen in uw instelling of de financiële markten kan worden geschaad. Daarnaast moet de bedrijfsvoering beheerst zijn. Dit houdt mede in dat u de bedrijfsvoering moet afstemmen op de aard, omvang, complexiteit en risico's van de activiteiten van de instelling. Als onderdeel van de integere en beheerste bedrijfsvoering ten slotte, moeten financiële instellingen als de uwe door middel van de SIRA de integriteitsrisico's identificeren en vervolgens passende maatregelen treffen om deze risico's te beheersen.

Zonder een SIRA kan uw instelling de integriteitswetgeving niet op adequate wijze risicogebaseerd naleven. Dus moet u ook voldoende kennis van de inherente integriteitsrisico's in huis hebben, opdat u op basis hiervan gegronde aannames kunt doen om tot een adequate risicobeheersing te komen. DNB heeft in augustus 2015 de brochure 'De integriteitsrisicoanalyse. Meer waar dat moet,

minder waar dat kan' gepubliceerd om handvatten te bieden hoe de SIRA opgesteld kan worden. In deze brochure hebben wij stapsgewijs aangegeven op welke manier een financiële instelling een SIRA kan opstellen. In die brochure is overigens ook al het begrip integrity risk appetite geïntroduceerd. De SIRA is, zo schrijven we daar, een zo objectief mogelijke beoordeling van de inherente risico's, die bepalend is voor de risicobeheersing. De integrity risk appetite geeft aan wat een financiële instelling bereid is te accepteren qua integriteitsrisico.

De integrity risk appetite bepaalt u idealiter voorafgaand aan de SIRA. Bij voorkeur stelt u vooraf vast welke risico's u acceptabel vindt nadat eventuele beheersmaatregelen zijn toegepast, maar ook welke risico's u überhaupt niet zou willen lopen. In de praktijk zal er echter vaak sprake zijn van een iteratief proces: bijvoorbeeld door ontwikkelingen in relaties met klanten, veranderingen in doelstellingen van de onderneming, het beschikbaar komen van nieuwe beheersmaatregelen of wijzigingen in de verwachtingen van externe stakeholders, maar ook geopolitieke ontwikkelingen, zult u de integrity risk appetite doorlopend bijstellen. Door de uitkomsten van de SIRA te toetsen aan uw integrity risk appetite, bepaalt u continu of uw instelling de risico's die uit de SIRA komen wil accepteren, beperken of vermijden, met de wettelijke verplichtingen als minimale vereisten. Vervolgens richt u, afhankelijk van de keuze welke risico's acceptabel zijn (en welke niet), de benodigde beheersingsmaatregelen in. Of uw instelling besluit te stoppen met bepaalde activiteiten, omdat u de keuze maakt ook de restrisico's niet te accepteren (en dus overgaat tot de-risking).

2 Vormgeving van de integrity risk appetite

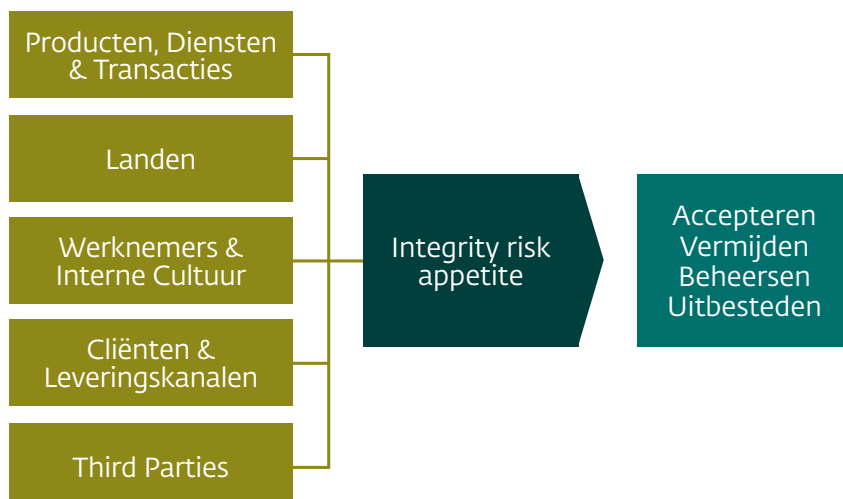
DNB vindt het belangrijk dat uw instelling bij het vormgeven van de integrity risk appetite nadenkt over drie aspecten van de integrity risk appetite:

- de reikwijdte van de integrity risk appetite
- de verantwoordelijkheid van het senior management voor het vaststellen, uitdragen en monitoren van de integrity risk appetite
- de operationele inbedding van de integrity risk appetite in de bedrijfsvoering en de rolverdeling tussen de verschillende lines of defense.

Deze punten worden hieronder nader toegelicht.

Reikwijdte integrity risk appetite

In de integrity risk appetite wordt idealiter per soort activiteit en/of product aangegeven welk soort risico relevant is en welke appetite daarbij past. Idealiter wordt hier op het niveau van verschillende scenario's over nagedacht. Dit vraagt dus om betrokkenheid van alle disciplines binnen uw organisatie die bij deze aspecten betrokkenheid hebben. Schematisch ziet het gebruik van een integrity risk appetite er daarmee als volgt uit:



Zoals eerder aangegeven is het vaststellen en onderhouden van de integrity risk appetite in de praktijk veelal een iteratief proces. Dat betekent dat dit proces dus periodiek (en wanneer daar aanleiding voor is) herhaald wordt.

Verantwoordelijkheid senior management

Het senior management (met name de bestuurders) draagt de eindverantwoordelijkheid voor het risico-profiel van de financiële instelling. Dit betekent dat zij de keuzes maken om bepaalde risico's wel of niet te accepteren, vermijden, beheersen of uit te besteden. Om de rol van het senior management duidelijk te maken, kan ook verwezen worden naar de beschrijving die de Financial Stability Board hiervoor heeft opgesteld. De verantwoordelijkheden behelzen onder andere:

- zorgen voor congruentie tussen de integrity risk appetite en de strategische doelstellingen van de financiële instelling op korte en (midden) lange termijn.

6

- de periodieke review van de integrity risk appetite versus het daadwerkelijke risicoprofiel van de financiële instelling (en de onafhankelijke controle daarvan).
- zorgdragen voor het testen en monitoren van de effectiviteit van beheersingsmaatregelen en het effectueren van eventuele maatregelen wanneer er buiten de integrity risk appetite wordt geopereerd.
- zorgen voor een goede implementatie van de integrity risk appetite binnen de gehele organisatie, en heldere interne en externe communicatie over de integrity risk appetite.

Laatstgenoemd onderdeel is een zeer essentiële verantwoordelijkheid. Door de integrity risk appetite zo concreet mogelijk te formuleren en hieraan zowel intern als extern voldoende aandacht en bekendheid te geven, zet uw organisatie een eerste stap richting naleving.

Operationele inbedding

De integrity risk appetite komt in alle aspecten van de bedrijfsvoering terug. Zowel bij de primaire processen van uw financiële instelling (kredietverlening, verzekeren etc.) als bij de secundaire processen (inkoop, personeelsbeleid etc.). In procesbeschrijvingen en procedures is het dan ook logisch dat uw instelling zich bij ieder specifiek proces of procedure de vraag stelt of er risico's bestaan dat er buiten de integrity risk appetite wordt gehandeld. Hieronder volgen enkele voorbeelden van hoe de integrity risk appetite terugkomt in de operatie van een financiële instelling:

- Een betaalinstelling besluit extra beheersingsmaatregelen te treffen bij dienstverlening aan bepaalde sectoren, omdat daar sprake is van verhoogde integriteitsrisico's, bijvoorbeeld naar aanleiding van DNB-publicatie over witwasrisico's in de sport.
- Een pensioenfonds kiest ervoor om in een bepaald hoogrisicoland wel beleggingen te hebben. Het fonds maakt daartoe aanvullende afspraken met zijn vermogensbeheerder, om scherp op specifieke risico's te letten die aan het hoogrisicoland zijn verbonden.
- Een bank besluit in verband met een aanstaande majeure reorganisatie extra beheersingsmaatregelen te treffen ten aanzien van haar interne cultuur, om zo integriteitsschendingen te voorkomen als gevolg van mogelijk afnemende motivatie/loyaliteit van medewerkers.
- Een verzekeraar besluit geen verzekeringen meer aan te bieden via bepaalde intermediairs, om zo het risico op overtreding van sanctieregelgeving beter te kunnen beheersen.
- Een trustkantoor besluit geen betrokkenheid meer te accepteren van derden bij het faciliteren van bepaalde transacties, omdat het risico op belangenverstrengeling bij transacties met betrokkenheid van derden te groot is.

Een ander voorbeeld dat we tijdens onderzoek zijn tegengekomen, betrof de dienstverlening van een bank aan een groep klanten. Bij deze klantengroep zag de bank verhoogde integriteitsrisico's op het gebied van acceptatie en monitoring. Het betrof dienstverlening aan een relatief kleine groep

klanten, die slechts een klein deel van de omzet en winst van de bank genereerde. Door deze geringe omvang was het voor de bank financieel onaantrekkelijk om alle beheersmaatregelen in te richten en uit te voeren die noodzakelijk waren om de integriteitsrisico's naar een acceptabel niveau terug te brengen, met een individuele risicoafweging en –mitigatie. De bank was echter ook van mening dat het niet juist zou zijn om deze groep klanten als geheel geen diensten meer te verlenen. Daarom besloot de bank om de dienstverlening aan deze sector onder te brengen bij een specialistisch team. Binnen dit team worden reeds bestaande processen en procedures van andere afdelingen gebruikt, die een voldoende controle op integriteitsrisico's beter waarborgen. Door een specifieke groep hoog-risico klanten te bedienen via een specialistisch team heeft de bank haar dienstverlening aan deze groep klanten kunnen voortzetten, binnen de grenzen van haar eigen integrity risk appetite.

Rolverdeling three lines of defense

De risico's in kaart brengen en passende beheersingsmaatregelen ontwikkelen, vergt dat u input krijgt van meerdere organisatieonderdelen, zoals compliance, risk, audit, productontwikkeling, beleid, sales en dergelijke. Ook om het gekozen beleid in te bedden en de procedures daadwerkelijk in praktijk te brengen is deze betrokkenheid weer nodig. Dit laatste sluit aan bij de vereisten uit het Bpr Wft, waarin in artikel 10, derde en vierde lid, wordt aangegeven dat de financiële instelling alle relevante organisatieonderdelen op de hoogte moet stellen van het beleid en de procedures en dat de instelling voor de uitvoering daarvan zorg moet dragen.

Elke line of defense heeft daarbij wel haar eigen verantwoordelijkheid ten aanzien van de integrity risk appetite.

De eerste lijn formuleert de integrity risk appetite voor haar specifieke bedrijfs onderdeel, waarbij die uiteraard in lijn is met de integrity risk appetite van de gehele financiële instelling. Zij levert hiervoor ook een voldoende onderbouwing aan, bijvoorbeeld met scenario's en data-analyse. Tot slot stuurt de eerste lijn op juiste toepassing van de geformuleerde integrity risk appetite. De tweede lijn is, naast haar betrokkenheid bij het formuleren van de integrity risk appetite, verantwoordelijk voor het toetsen van de integrity risk appetite aan geldende wet- en regelgeving, maar ook voor het onafhankelijk van de eerste lijn monitoren van de toepassing van de integrity risk appetite binnen de dagelijkse operatie. De derde lijn voert onafhankelijke audits uit, om het senior management de zekerheid te verschaffen dat alle bedrijfs onderdelen conform de geformuleerde integrity risk appetite opereren.

3 De-risking

8

Tot slot vraagt DNB in deze publicatie aandacht voor de-risking. Dit betreft, zoals we al eerder beschreven, een specifieke vorm van het toepassen van de integrity risk appetite, waarnaar we in ons onderzoek naar integrity risk appetite ook hebben gekeken. De-risking is feitelijk een gevolg van een streng toegepaste integrity risk appetite. Bij de-risking vermijdt een instelling risico's, door om integriteitsredenen groepen cliënten categoriaal af te stoten en/of uit te sluiten, zonder hierbij een individuele risico-afweging te maken. Dit is conformde FATF-definitie, die van de-risking spreekt wanneer financial institutions terminate or restrict business relationships with categories of customers.

DNB heeft onderzoek gedaan naar de vraag in hoeverre de-risking plaats vindt in Nederland. Het gevaar bestaat namelijk niet alleen dat klanten ten onrechte van financiële diensten worden uitgesloten, maar ook dat daardoor activiteiten uit het zicht van het financiële systeem verdwijnen en zich verplaatsen naar ongereguleerde kanalen.

In ons onderzoek hebben we geconcludeerd dat categorale uitsluiting om integriteitsredenen niet op grote schaal voorkomt in Nederland. Als een instelling cliënten weigert, dienstverlening befrist of afscheid neemt van cliënten, is dat veelal op basis van een individuele afweging over die specifieke cliënten. Betaalinstellingen, trustkantoren en in mindere mate banken en geldtransactiekantoren hanteren wel lijsten met onacceptabele cliënten en activiteiten, maar deze zijn grotendeels ingegeven door wet- en regelgeving, contractuele verplichtingen en andere

redenen dan integriteitsrisico's. DNB blijft aandacht houden voor de ontwikkelingen op het gebied van de-risking, zowel in de financiële sector in Nederland als op internationaal gebied.

In enkele gevallen lijkt er sprake te zijn van onjuiste interpretatie van de risicogebaseerde aanpak in wet- en regelgeving. Zoals in de DNB Leidraad WWFT en SW (par. 3.4) staat aangegeven, betekent een inherent verhoogd risico niet automatisch dat uw instelling dit type cliënten categoriaal moet weigeren. Van u wordt gevraagd van geval tot geval te beoordelen of de integriteitsrisico's gerelateerd aan (verhoogd risico) klanten en/of activiteiten te mitigeren zijn. Alleen wanneer blijkt dat een voorgenomen of bestaande relatie en/of activiteit te risicovol is, is beëindiging of weigering van de cliënt en of activiteit op zijn plaats.

Diverse financiële instellingen geven aan dat (potentiële) cliënten er ook zelf aan kunnen bijdragen dat zij (categoraal) uitgesloten worden. Door bij het acceptatieproces open en transparant te zijn, door adequate en duidelijke informatie aan te leveren over de activiteiten die zij voeren en door informatie te verschaffen over de wijze waarop de cliënt zelf (indien van toepassing) cliëntonderzoek uitvoert, kan de financiële instelling een betere analyse maken van het integriteitsrisico van een (potentiele) cliënt.

4 Status van deze good practice

Good practice van de Nederlandsche Bank N.V. van 28 september 2017, houdende een leidraad met betrekking tot Integrity Risk Appetite [citeertitel 'Good practice Integrity Risk Appetite']

Disclaimer

Deze good practice geeft niet verplichtende aanbevelingen voor de toepassing van voorschriften betrekking hebbende op de integere en beheerste bedrijfsvoering van met name banken, pensioenfondsen, verzekeraars, betaalinstanties en trustkantoren (hierna: financiële instellingen).

Met behulp van deze good practice draagt De Nederlandsche Bank N.V. haar opvattingen uit over de door haar geconstateerde of verwachte gedragingen in de beleidspraktijk, die naar haar oordeel een goede toepassing inhouden van de regels waarop deze good practice betrekking heeft.

Met deze good practice beoogt De Nederlandsche bank N.V. te bereiken dat financiële instellingen het daarin gestelde, de eigen omstandigheden in aanmerking nemende, in hun afweging betrekken, zonder dat zij verplicht zijn dat te doen. De good practice geeft inzicht in de door DNB geconstateerde of te verwachten gedraging in de beleidspraktijk, is indicatief van aard en sluit daarmee niet uit dat voor instellingen een afwijkende, al dan niet strengere toepassing van de onderliggende regels is geboden. De afweging betreffende de toepassing berust bij deze instellingen zelf.

Gerelateerde wet en regelgeving

Deze Good Practice heeft betrekking tot de volgende wet- en regelgeving:

- artikelen 3:10 en 3:17 Wet op het financieel toezicht (Wft) juncto artikel 10 Besluit prudentiële regels Wft (Bpr Wft)
- artikel 19 Besluit financieel toezichtskader pensioenfondsen (Bftk) juncto artikel 14 Besluit uitvoering Pensioenwet (BuP)
- artikel 10 Wet toezicht trustkantoren (Wtt) juncto artikel 4 Regeling integere bedrijfsvoering Wtt (RIB Wtt)

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl