# DNB SIRA Good Practices

## Consultatieversie

DeNederlandscheBank

EUROSYSTEEM

# Inhoudsopgave


1 Inleiding

2 Integriteits-risicomanagement

3 Risico-identificatie

4 Risicoanalyse

5 Risicobeheersing

6 Risicomonitoring en herziening

Bijlage

# 1 Inleiding

## 1.1 Integriteitstoezicht DNB

Integriteit is – naast soliditeit – een voorwaarde voor een gezond en betrouwbaar financieel stelsel. De Nederlandsche Bank (DNB) houdt integriteitstoezicht op een breed scala aan (financiële) instellingen. Het integriteitstoezicht van DNB is met name gebaseerd op de Wet op het financieel toezicht (Wft), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), de Sanctiewet 1977 (Sw), de Pensioenwet (Pw), de Wet verplichte beroepspensioenregeling (Wvb) en de Wet toezicht trustkantoren 2018 (Wtt 2018) (hierna tezamen: integriteitswetgeving).[1]

Een schone en integere financiële sector begint bij schone en integere financiële instellingen. DNB ziet erop toe dat instellingen de bedrijfsvoering zodanig inrichten dat daarmee een beheerste en integere uitoefening van het bedrijf wordt gewaarborgd. In de kern gaat het bij het waarborgen van een integere uitoefening van het bedrijf om de beheersing van de integriteitsrisico's waaraan de instelling is blootgesteld. De Wft schrijft voor dat het ten aanzien van integriteit met name gaat om het tegengaan van:

- belangenverstrengeling;
- het begaan van strafbare feiten of andere wetsovertredingen door de financiële onderneming of haar werknemers, die het vertrouwen in de financiële onderneming of in de financiële markten kunnen schaden;
- relaties met cliënten die het vertrouwen in de financiële onderneming of in de financiële markten kunnen schaden;
- andere maatschappelijk onbetamelijke handelingen van de instelling of haar medewerkers die het vertrouwen in de financiële onderneming of in de financiële markten ernstig kunnen schaden.

Deze aspecten van een integere bedrijfsvoering zijn nader uitgewerkt in algemene maatregelen van bestuur, zoals het Besluit prudentiële regels Wft. In specifieke wetgeving, met name de Wwft, de Wtt 2018 en de Sw, zijn meer gedetailleerde verplichtingen opgenomen ter voorkoming van betrokkenheid bij witwaspraktijken, financiering van terrorisme en overtreding van sanctieregelgeving.

## 1.2 De SIRA

Ter waarborging van de integere uitoefening van het bedrijf dragen instellingen zorg voor een systematische analyse van integriteitsrisico's (SIRA).[2] Hiertoe licht de instelling op continue basis de eigen organisatie door om te bezien bij welke bedrijfsonderdelen er gevaar op integriteitsrisico's bestaat. De instelling zal op basis van deze risicoanalyses preventief maatregelen moeten nemen ter beheersing van haar integriteitsrisico's.

De SIRA is daarmee een belangrijk instrument voor het waarborgen van een integere bedrijfsvoering. Vanwege dit karakter kan de SIRA op verschillende manieren worden vastgelegd. Dit kan bijvoorbeeld een document zijn waarin de resultaten en de methodiek van de verschillende stappen worden vastgelegd. De SIRA kan ook in meerdere documenten vastliggen, het gaat er om dat de vastlegging past bij de werkwijze van de instelling. Het bestuur van een instelling kan de SIRA gebruiken om zich enerzijds te laten informeren over de aard en omvang van de integriteitsrisico's en anderzijds als sturingsdocument om prioriteiten te stellen met betrekking tot de te treffen beheersmaatregelen.

1 Daarnaast houdt DNB integriteitstoezicht op instellingen die actief zijn in Caribisch Nederland. Voor dit toezicht geldt eigen wet- en regelgeving.
2 Artikel 10 Besluit prudentiële regels Wft (Bpr), Artikel 10 Besluit toezicht trustkantoren (Btt 2018).

## 1.3 Verhouding Wwft-risicobeoordeling tot de SIRA

De Wwft bepaalt dat een instelling maatregelen neemt om haar risico's op witwassen en financieren van terrorisme vast te stellen en te beoordelen (de Wwft-risicobeoordeling). Daarbij staan de maatregelen in verhouding tot de aard en de omvang van de instelling. Bij het maken van de Wwft-risicobeoordeling houdt de instelling op grond van de Wwft in ieder geval rekening met de risicofactoren die verband houden met het type cliënt, product, dienst, transactie en leveringskanaal en met landen of geografische gebieden. Verder bepaalt de Wwft dat een instelling de resultaten van de Wwft-risicobeoordeling vastlegt, deze actueel houdt en deze resultaten desgevraagd aan de toezichthouder verstrekt.[3]

De SIRA ziet op integriteitsrisico's in brede zin. De Wwft-risicobeoordeling ziet meer in het bijzonder op het risico op witwassen en financieren van terrorisme – zie hiervoor de DNB Q&As en Good Practices Wwft.[4] De SIRA heeft dus een breder bereik dan de Wwft-risicobeoordeling. Het ligt voor de hand, hoewel dit niet verplicht is, dat de Wwft-risicobeoordeling onderdeel is van de SIRA als de instelling tevens verplicht is om een SIRA op te stellen.[5]

## 1.4 Aanleiding, status en opbouw van dit document

### 1.4.1 Aanleiding voor de herziening van de SIRA Good Practices

Met de SIRA Good Practices wil DNB de onder haar toezicht staande instellingen handvatten bieden voor het opstellen en het gebruik van een SIRA.

DNB heeft in 2015 haar eerste *good practices* gepubliceerd voor het opstellen van een SIRA.[6] Deze kwam tot stand nadat DNB had geconstateerd dat veel instellingen niet over een SIRA beschikten. Van de SIRA's die DNB wel onderzocht voldeed meer dan 80% niet.

Sindsdien ziet DNB dat vrijwel alle instellingen een SIRA hebben opgesteld. DNB heeft in de afgelopen jaren echter geconstateerd dat instellingen zich bij het opstellen van de SIRA in veel gevallen slechts richten op het invullen van de elementen die DNB in haar *good practices* heeft aangereikt. De eigen reflectie op de van toepassing zijnde integriteitsrisico's blijft daarbij in veel gevallen beperkt. Doordat instellingen rigide vasthouden aan het SIRA-proces zoals opgenomen in de *good practices* van 2015, worden ook nieuwere inzichten en mogelijkheden in de praktijk vaak niet meegenomen. Door deze 'mechanische benadering' bestaat vaak onvoldoende inzicht in de integriteitsrisico's die de instelling concreet loopt. De instelling is daardoor ook niet in staat om haar integriteitsrisico's aantoonbaar en effectief te mitigeren.

Hoewel veel instellingen inmiddels beschikken over een SIRA, ziet DNB dus dat de SIRA vaak niet of onvoldoende wordt gebruikt als een (dynamisch) document voor het identificeren, analyseren en mitigeren van integriteitsrisico's. Dit heeft DNB doen besluiten tot een herziening van de SIRA Good Practices.

### 1.4.2 Status SIRA Good Practices

Uit onze toezichtpraktijk is naar voren gekomen dat de SIRA Good Practices uit 2015 als normenkader wordt beschouwd waarbij er weinig tot geen ruimte wordt gelaten voor eigen invulling of interpretatie. Om dit beeld te ontkrachten wordt bij deze herziening duidelijk gemaakt dat er niet een specifieke aanpak wordt voorgeschreven.

Deze SIRA Good Practices geeft praktijkvoorbeelden en aandachtspunten die gebruikt kunnen worden bij het opstellen van de SIRA en de Wwft-risicobeoordeling.

3 Artikel 2b Wwft.
4 DNB Q&As en Good Practices Wwft, §2.1.
5 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 43.
6 DNB (2015), *De integriteitsrisicoanalyse. Meer waar dat moet, minder waar dat kan.* Met de publicatie van deze nieuwe *good practices* is het document uit 2015 vervallen.

*Good practices* bevatten suggesties of aanbevelingen voor onder toezicht staande instellingen. Het zijn voorbeelden van mogelijke toepassingen die naar het oordeel van DNB goede invulling geven aan de verplichtingen uit wet- en regelgeving. *Good practices* zijn indicatief van aard en instellingen zijn vrij om een andere toepassing te kiezen, zo lang men voldoet aan de wet- en regelgeving.

Voor een nadere toelichting op de status van de beleidsuitingen van DNB, zie de Leeswijzer beleidsuitingen DNB op Open Boek Toezicht.

Deze SIRA Good Practices vervangt de *good practices* uit 2015.[7] DNB heeft nog meer beleidsuitingen gepubliceerd over integriteitswetgeving. Op Open Boek Toezicht is een overzicht opgenomen van alle (algemene, dan wel sectorspecifieke) beleidsuitingen van DNB inzake integriteitswetgeving.[8]

De SIRA Good Practices zijn bedoeld als praktisch en actueel hulpmiddel voor een instelling om invulling te geven aan het opstellen van de SIRA, op basis waarvan effectieve beheersmaatregelen genomen kunnen worden.

### 1.4.3 Opbouw van de SIRA Good Practices

De 'SIRA Good Practices' is als volgt opgebouwd. In dit hoofdstuk 1 worden de context en het juridisch kader geschetst. In hoofdstuk 2 komt de basis van het 'integriteitsrisicomanagement' aan de orde, waaronder een cyclus van processtappen die in de praktijk over het algemeen worden toegepast om te komen tot een adequate en actuele SIRA. In de hoofdstukken daarna worden *good practices* beschreven met betrekking tot de verschillende processtappen die bij het opstellen en onderhouden van de SIRA onderscheiden kunnen worden.

## 1.5 Juridisch kader

### 1.5.1 Wft, Pw en Wtt 2018: Systematische analyse van integriteitsrisico's (SIRA)

Instellingen dienen een adequaat beleid te voeren dat een integere uitoefening van hun bedrijf waarborgt.[9] Instellingen moeten dit beleid opstellen en uitvoeren aan de hand van een systematische analyse van de voor hen relevante integriteitsrisico's.[10]

#### Wet- en regelgeving

De volgende wet- en regelgeving is met name relevant voor een systematische analyse van de integriteitsrisico's (voor zover van toepassing):

- artikel 3:10 Wft, jo. artikel 10 Bpr[11]
- artikel 14 Wtt 2018 jo. artikel 10 Btt 2018[12]
- artikel 143 Pw, artikel 138 Wet verplichte beroepspensioenregeling en artikel 19 Besluit financieel toetsingskader pensioenfondsen
- artikel 2b Wwft, 2c Wwft.

Integriteitsrisico is op de volgende manieren gedefinieerd:

- *Voor instellingen die onder de Wft vallen*: Een gevaar voor aantasting van de reputatie of bestaande of toekomstige bedreiging van vermogen of

7 DNB (2015), *De integriteitsrisicoanalyse. Meer waar dat moet, minder waar dat kan.*
8 https://www.dnb.nl/voor-de-sector/open-boek-toezicht/thema-s/toezicht-op-financieel-economische-criminaliteit-integriteitstoezicht/
9 Artikel 3:10 Wft (afwikkelonderneming, betaalinstelling, clearinginstelling, elektronischgeldinstelling, entiteit voor risico-acceptatie, bank, kredietunie, premiepensioeninstelling, verzekeraar, wisselinstelling of bijkantoor als bedoeld in artikel 3:10 lid 1, 3:11, 3:12, 3:12a, 3:13 of 3:14 van de Wft.), artikel 14 Wtt (trustkantoor), artikel 143 Pw (pensioenfonds).
10 *Stb.* 2006, 519, p. 104 en *Stb.* 2011, 673, p. 19.
11 Artikel 3:10 Wft en artikel 10 Bpr zijn van toepassing op een betaalinstelling, clearinginstelling, elektronischgeldinstelling, entiteit voor risico-acceptatie, bank, kredietunie, premiepensioeninstelling, verzekeraar, wisselinstelling of bijkantoor als bedoeld in artikel 3:10 lid 1, 3:11, 3:12, 3:12a, 3:13 of 3:14 van de Wft.
12 Artikel 14 Wtt 2018 en artikel 10 Btt 2018 zijn van toepassing op trustkantoren.

resultaat als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is voorgeschreven.[13]
- *Voor trustkantoren*: Risico van ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is bepaald alsmede risico van betrokkenheid van het trustkantoor of zijn medewerkers bij handelingen die op een dusdanige wijze ingaan tegen hetgeen volgens het ongeschreven recht in het maatschappelijk verkeer betaamt, dat hierdoor het vertrouwen in het trustkantoor of in de financiële markten ernstig kan worden geschaad.[14]

Instellingen doorlopen een aantal stappen om de omstandigheden en gebeurtenissen die gevolgen kunnen hebben voor de integere uitoefening van het bedrijf van de instelling te herkennen en te beheersen:[15]
- een systematische analyse van integriteitsrisico's, inclusief periodieke bijwerking daarvan;
- het ontwikkelen van beleid en van procedures en maatregelen die het beleid concretiseren;
- de uitvoering, systematische toetsing en bijstelling van het beleid en van de procedures en maatregelen.

Hierbij is allereerst van het belang dat de instelling zelf op systematische wijze een analyse maakt van haar integriteitrisico's. Hiertoe licht de instelling op continue basis de eigen organisatie door om te bezien bij welke bedrijfsonderdelen er gevaar op integriteitrisico's bestaat. Met behulp van deze analyse formuleert de instelling haar beleid (procedures en maatregelen) en past zij dit indien nodig aan om de integere uitoefening van het bedrijf blijvend te waarborgen.[16]

'Systematisch' impliceert een cyclisch proces: het betekent dat instellingen de inventarisatie, analyse en de (toetsing van de effectiviteit van de) beheersing periodiek moeten doorlopen. Risico's zijn immers niet statisch. Zowel interne als externe factoren kunnen ervoor zorgen dat risico's voor een instelling veranderen. Zo kunnen de activiteiten van een instelling uitgebreid worden of veranderen, kunnen zich bepaalde trends voordoen binnen het financieel-economische verkeer, of kan wet- en regelgeving aangepast worden.[17]

### 1.5.2 Beleidsuitingen

Ten aanzien van specifieke integriteitsrisicogebieden, in het bijzonder witwassen, financieren van terrorisme en sancties, hebben DNB en andere autoriteiten handreikingen uitgegeven, waaronder de *Q&A en Good Practices Wwft* van DNB.[18] Waar relevant dient de SIRA Good Practices in samenhang met deze handreikingen te worden gelezen.

De European Banking Authority (EBA) heeft daarnaast verschillende relevante richtsnoeren, opinies, rapporten en overige uitingen opgesteld die relevant zijn voor banken en andere sectoren. DNB is, samen met de andere Europese autoriteiten die zijn vertegenwoordigd in de verschillende gremia van de EBA, betrokken bij de totstandkoming van deze beleidsuitingen en neemt deze uitingen mee in haar toezicht. Doel van de richtsnoeren van de EBA is een zo consistent en uniform mogelijke toepassing van normen in de Europese regelgeving in alle EU-lidstaten.

De richtsnoeren van de EBA zijn gericht aan toezichthouders en in sommige gevallen ook direct aan instellingen, maar hebben niet dezelfde status als bindende Europese regelgeving. Ze bevatten een toelichting voor de invulling en toepassing van Europese regelgeving. Toezichthouders en

13 Artikel 1 Bpr.
14 Artikel 1 Wtt 2018.
15 Artikel 10 Bpr, Artikel 10 Btt 2018, Artikel 19 Besluit financieel toetsingskader pensioenfondsen.
16 *Stb.* 2006, 519, p. 104.
17 *Stb.* 2018, 463, p. 28.
18 Zie DNB Q&As en Good Practices Wwft.

instellingen dienen zich tot het uiterste in te spannen om aan die richtsnoeren te voldoen.[19] Dat betekent ook dat DNB, waar relevant, verwijst naar beleidsuitingen van de EBA. De beleidsuitingen van de EBA zijn met name relevant voor de Wwft-risicobeoordeling, bijvoorbeeld de ML/*TF Risk Factors Guidelines* en de *Guidelines on the role and responsibilities of the AML/CFT compliance officer*.

Tot slot zijn er verschillende andere internationale beleidsuitingen die relevant kunnen zijn voor de invulling en toepassing van de SIRA, bijvoorbeeld van de Financial Action Task Force (FATF) en het Basel Committee on Banking Supervision (BCBS), bijvoorbeeld de beleidsuiting *Compliance and the compliance function in banks* van het Basel Committee on Banking Supervision (BCBS).

DNB gaat ervan uit dat instellingen deze bronnen meenemen bij de SIRA en bij het opstellen en toepassen van hun beleid, procedures en maatregelen om de door hen geïdentificeerde risico's effectief te beheersen. DNB kiest ervoor om, in gevallen waar relevante internationale beleidsuitingen bestaan, hiernaar te verwijzen in plaats van deze over te nemen. Op die wijze wordt geborgd dat instellingen altijd recente bronnen kunnen gebruiken.

## 1.6 Risicogebaseerde benadering

Zoals hiervoor al is opgemerkt gaat het bij het waarborgen van een integere uitoefening van het bedrijf in de kern om de beheersing van de integriteitsrisico's waaraan de instelling is blootgesteld. Het waarborgen van een integere bedrijfsvoering gaat daarmee uit van een risicogebaseerde benadering.

Een risicogebaseerde benadering houdt in dat de inzet en intensiteit van procedures en maatregelen afhankelijk zijn van de omvang van het risico. Een beperktere inzet in geval van lage risico's schept de ruimte om capaciteit en aandacht te richten op hogere risico's. Zo kunnen schaarse middelen juist daar worden ingezet waar het meeste resultaat is te behalen. Een hoog bewustzijn van relevante risico's bij instellingen is essentieel voor een passende, effectieve en efficiënte aanpak van integriteitsrisico's. Ook is dit van belang bij het voorkomen van onnodige belasting van cliënten, en het tegengaan van uitsluiting en (indirecte) discriminatie.

19 Voor richtsnoeren geldt een 'comply or explain'-procedure, waarbij toezichthouders zoals DNB moeten aangeven of zij zich committeren aan de richtsnoeren in hun toezicht. DNB neemt in haar (periodiek geactualiseerde) overzicht 'Toepassing Richtsnoeren en aanbevelingen van de Europese toezichthoudende autoriteiten' op Open Boek Toezicht op welke richtsnoeren zij in acht neemt bij de toepassing van de relevante toezichtwet- en regelgeving (Toepassing Richtsnoeren en aanbevelingen van de Europese toezichthoudende autoriteiten).

# 2 Integriteitsrisicomanagement

## Integriteitsrisicomanagement begint bij de SIRA

Integriteitsrisicomanagement gaat in de kern om de beheersing van de integriteitsrisico's waaraan de instelling is blootgesteld. Dat begint bij het identificeren en analyseren van de aan de orde zijnde integriteitsrisico's: welke risico's zijn dat, hoe kunnen deze zich manifesteren en waar, en welke eventuele gevolgen zou dat hebben – dat is in het kort wat een SIRA behelst. De SIRA is daarmee een belangrijke bouwsteen, zo niet de hoeksteen, van het integriteitsrisicomanagement. Integriteitrisico's kunnen daarbij voortvloeien uit activiteiten, relaties en handelingen van bijna alle geledingen van een instelling.

### Beheersing van integriteitsrisico's

Een instelling zal haar integriteitsrisico's niet alleen documenteren, maar deze ook afdoende moeten beheersen. De instelling stelt daarom op basis van de SIRA beleid, procedures en maatregelen in werking ter beheersing van haar integriteitsrisico's. De beheersing richt zich op het verminderen van de kans op optreden van een risico en op het beperken van negatieve gevolgen mocht een risico toch optreden.

### Doorlichten, actualiseren en bijstellen

Verder is het van belang dat de instelling vaststelt dat de beheersmaatregelen voldoen. Hier zijn twee hoofdvragen van belang:

- Zijn de beheersmaatregelen doeltreffend? Hier bepaalt de instelling of de beheersmaatregelen daadwerkelijk de betreffende integriteitsrisico's afdoende beheersen. Uit bijvoorbeeld incidentmeldingen of audits kan blijken dat de beheersing op sommige plekken te zwak of juist te sterk is.
- Zijn er risico's waarmee in de beheersing nog geen rekening is gehouden? Door interne en externe ontwikkelingen kunnen risico's toe- en afnemen, en kunnen er nieuwe risico's ontstaan. Het is van belang dat de beheersmaatregelen van de instelling hierop goed aansluiten.

Kortom, de instelling licht op continue basis de eigen organisatie door om te bezien bij welke bedrijfsonderdelen er gevaar op integriteitrisico's bestaat, en houdt daarbij ook rekening met in- en externe ontwikkelingen. Waar nodig stelt de instelling haar SIRA en haar beheersmaatregelen bij.

### Integere bedrijfsvoering: redelijkerwijs voorkomen van integriteitschendingen

Het is goed om te realiseren dat integriteitsrisicomanagement primair is gericht op het voorkomen van integriteitschendingen. Dat wil niet zeggen dat integriteitschendingen niet kunnen voorkomen. Het wil ook niet zeggen dat een integriteitschending het gevolg is van het falen van de bedrijfsvoering, al kan dat uiteraard wel aan de orde zijn. De beoordeling van de integere bedrijfsvoering richt zich op de vraag of de instelling het redelijkerwijs mogelijke heeft gedaan om integriteitschendingen te voorkomen.

### De SIRA als ankerpunt

De SIRA is daarbij een belangrijk ankerpunt. Zonder een systematische analyse van integriteitsrisico's is immers niet vast te stellen of het beleid, de procedures en de maatregelen van een instelling goed aansluiten op haar integriteitsrisico's. De instelling loopt dan het risico dat zij onvoldoende tegengaat dat zij bijvoorbeeld betrokken raakt bij strafbare feiten, wetsovertredingen of maatschappelijk onbetamelijke handelingen die het vertrouwen in de instelling of in de financiële markten kunnen schaden.

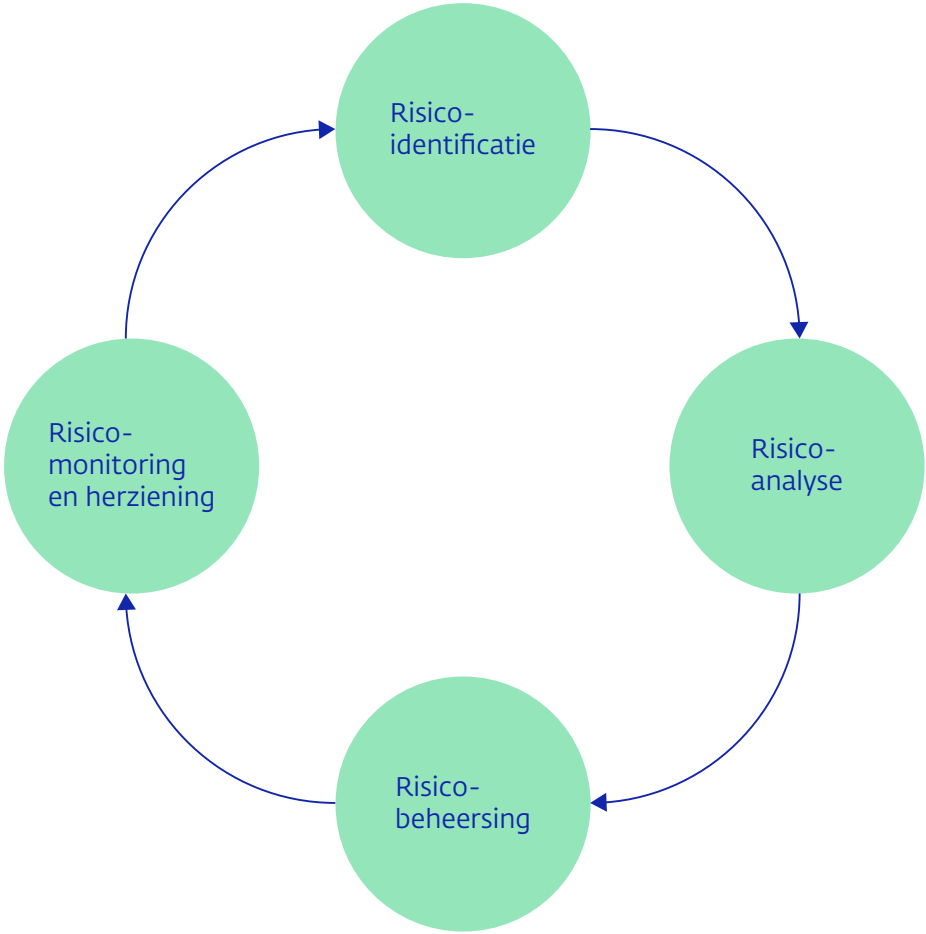
### Cyclus van integriteitsrisicomanagement

DNB heeft de afgelopen jaren veel SIRA's en onderliggende totstandkomings- en herzieningsprocessen bekeken en beoordeeld. Op basis hiervan en met inachtneming van het juridisch kader is een *good practice* met een cyclus van een viertal processtappen geïdentificeerd. Deze stappen zien op het gehele proces van integriteitsrisicomanagement en worden in

de praktijk toegepast om een adequate SIRA te ontwikkelen en actueel te houden. Deze cyclus is weergegeven in onderstaande afbeelding.

De cyclus geeft een logische volgorde van te nemen stappen. De praktijk laat zien dat het proces van integriteitsmanagement ook dynamisch is. Zo kunnen bijvoorbeeld in de fase 'risicoanalyse' of in de fase 'risicobeheersing' nog risico's geïdentificeerd worden die nog niet eerder, in de fase 'risico-identificatie', naar voren waren gekomen. Ook kan er sprake zijn van opkomende of nieuwe risico's waarvoor de cyclus doorlopen wordt.

Het gaat er niet primair om dat de processtappen in de juiste volgorde worden doorlopen. Het gaat er om dat de instelling beschikt over een SIRA met een daarop gebaseerde en passende risicobeheersing waarmee de integere uitoefening van het bedrijf is gewaarborgd.



# 3 Risico-identificatie

## Inleiding

De SIRA is een instellingspecifieke analyse van de integriteitsrisico's die voor de instelling relevant zijn. Een goed beeld van de organisatie en het bedrijf van de instelling is dan ook het startpunt. Het uitvoeren van de SIRA begint daarmee met het in kaart brengen van het organisatierisicoprofiel.

In een organisatierisicoprofiel worden de integriteitsrisico's geïdentificeerd zoals die zich voordoen op verschillende niveaus binnen de instelling, inclusief de elementen die kunnen bijdragen aan de mate waarin deze risico's zich voordoen. Het bevat een kwantitatieve en kwalitatieve analyse van de risicofactoren waaraan de instelling blootstaat. Risicofactoren zijn bijvoorbeeld het type dienstverlening, de cliëntenportefeuille en de daaraan gekoppelde transacties, leveringskanalen, geografische gebieden, tekenbevoegdheden, uitbestedingsrelaties etc.

De risico-identificatie, met het opstellen van een organisatierisicoprofiel, is een kennisintensieve stap – het vergt kennis en expertise. Dit betreft enerzijds kennis van de organisatie en anderzijds kennis van integriteitsrisico's en de manifestatie daarvan.

### Ratio

Met het organisatierisicoprofiel heeft de instelling een goed beeld van de integriteitsrisico's die binnen de verschillende onderdelen kunnen spelen en de factoren waardoor de instelling blootgesteld kan worden aan deze risico's. Op basis van het organisatierisicoprofiel kan de instelling de geïdentificeerde integriteitsrisico's nader analyseren – dit komt aan de orde in hoofdstuk 4.

## Good practices

### Good practice – Voorbereiding voor de SIRA

Een instelling start haar periodieke SIRA proces. Alvorens het proces in te gaan en om zicht te ontwikkelen op potentiële integriteitsrisico's bereidt de compliance officer het proces eerst voor. Hij onderneemt daartoe onder andere de volgende acties:

- Hij betrekt (externe) expertise om te ondersteunen bij de vraag welke integriteitsrisico's voor deze instelling aan de orde kunnen zijn.
- Door gerichte communicatie en het verkrijgen van *commitment* in de organisatie zorgt hij voor betrokkenheid, draagvlak en voor organisatorische inbreng die in het proces nodig is.
- In overleg met de (externe) deskundige oriënteert hij zich op relevante en gezaghebbende bronnen die behulpzaam kunnen zijn bij het proces. Een overzicht van de belangrijkste bronnen deelt hij in de organisatie, met een korte samenvatting van de inhoud. Dit betreft:
  - Relevante passages uit de memories van toelichting bij Wft, Bpr, Wwft en Sw
  - De SIRA-handreiking van DNB
  - ML/TF Risk Factors Guidelines van de EBA
  - Q&A en Good Practices Wwft en de Leidraad Sw van DNB
  - De National Risk Assessment (NRA) Witwassen
  - Het DNB-rapport Integriteitstoezicht in Beeld
  - Eventueel beschikbare relevante sectorbrede risicoanalyses
  - De Good practices bestrijden corruptie van DNB.
- Ook oriënteert de compliance officer zich op incidenten die zich bij de instelling hebben voorgedaan alsmede op interne rapportages,

audits, klachten en meldingen die zicht kunnen bieden op waar integriteitsrisico's kunnen spelen.
- Samen met de (externe) deskundige stelt hij een plan van aanpak op. Onderdeel van het plan is een intern communicatieplan. Ook voorziet het plan in beheer van de SIRA, o.a. door middel van periodieke actualisering.

## Good practice – Stappen om te komen tot een organisatierisicoprofiel

Een instelling heeft de volgende stappen genomen om te komen tot haar organisatierisicoprofiel:
- Inventarisatie van organisatieonderdelen.
- Per organisatieonderdeel een inventarisatie van:
  - het aanbod van producten/diensten
  - de cliëntenportefeuille
  - aantal, omvang en geografische spreiding van transacties
  - de omvang in FTE
  - de integriteitsgevoelige functies
  - opgetreden incidenten, incl. overzicht van interne en externe klachten
  - maatregelen van toezichthouders
  - uitingen in de media.
- Inventarisatie van de belangrijkste uitbestedingspartners en leveranciers.
- Identificatie van mogelijke integriteitsrisico's, zowel per organisatieonderdeel als voor de instelling als geheel:
  - de verplicht te behandelen risico's, met name de risico's op betrokkenheid bij witwassen, financieren van terrorisme, (nationale, Europese of andere internationale) sancties, belangenverstrengeling en maatschappelijk onbetamelijk handelen
  - de risico's die samenhangen met de integriteit van beleidsbepalers en medewerkers
  - de risico's die geïndiceerd worden door gebeurtenissen en incidenten uit het verleden.

Bij de identificatie betrekt de instelling ook de van toepassing zijnde factoren die van invloed kunnen zijn op deze risico's.

## Good practice – Organisatierisicoprofiel levensverzekeraar, witwasrisico

De compliance officer van een levensverzekeraar stelt een organisatierisicoprofiel op. Met betrekking tot het witwasrisico heeft zij de volgende risicofactoren in beeld gebracht:
- Met betrekking tot de producten komen volgende factoren concreet terug in het organisatierisicoprofiel:
  - aantal overlijdensrisicoverzekeringen, zonder kapitaalopbouw
  - aantal polissen met kapitaalopbouw
  - aantal polissen met een premie van meer dan 2.500 euro per jaar.
- Met betrekking tot de leveringskanalen constateert ze dat de instelling alleen directe verkoop doet, en niet via tussenpersonen werkt.
- Met betrekking tot de cliënten worden de volgende factoren in aanmerking genomen, waarbij op voorhand al is vastgesteld dat de instelling geen zakelijke cliënten bedient. Deze factoren komen concreet terug in het organisatierisicoprofiel:
  - aantal particuliere cliënten uit NL
  - aantal particuliere cliënten uit andere EU-landen
  - aantal particuliere cliënten buiten de EU.

## Good practice – Organisatierisicoprofiel, sanctierisico

De directie van een bank geeft opdracht om het organisatierisicoprofiel met betrekking tot het sanctierisico te actualiseren. De verantwoordelijke binnen de eerste lijn geeft hier uitvoering aan, in samenwerking met een sanctie-expert. Voor het organisatieonderdeel 'Trade Finance' betrekt hij een expert van die afdeling. Samen brengen zij de volgende risicofactoren in beeld:

- Aantal cliënten 'Trade Finance'.
- Aantal cliënten met import- of exportrelaties naar Rusland. *Dezelfde analyse wordt gemaakt voor andere gesanctioneerde gebieden zoals Noord Korea, Iran en Myanmar.*
- Met het oog op sanctie-ontwijking: aantal cliënten met import- of exportrelaties naar gebieden die grenzen aan Rusland. *Dezelfde analyse wordt gemaakt voor andere gesanctioneerde gebieden zoals Noord Korea, Iran en Myanmar.*
- Aantal cliënten die strategische goederen en/of dual-use goederen leveren.
- Transactievolume naar Rusland afgelopen kwartaal. *Dezelfde analyse wordt gemaakt voor andere gesanctioneerde gebieden zoals Noord Korea, Iran en Myanmar.*
- Met het oog op sanctie-ontwijking: transactievolume naar gebieden die grenzen aan Rusland afgelopen kwartaal. *Dezelfde analyse wordt gemaakt voor andere gesanctioneerde gebieden zoals Noord Korea, Iran en Myanmar.*

## Good practice – Betrekken kennis en expertise

Bij het opstellen van het organisatierisicoprofiel neemt degene die verantwoordelijk is voor de SIRA het initiatief om de verschillende bedrijfsonderdelen en *lines of defence* te betrekken. Hierdoor ontstaat een integraal beeld van de organisatie, met onder meer goed inzicht in de governance, de producten die gevoerd worden, de cliënten, de transacties en waar de instelling geografisch actief is. Bovendien wordt expertise op het gebied van compliance en integriteit betrokken om integriteitsrisico's te helpen identificeren en relevante risicofactoren te duiden.

## Good practice – Risicofactoren en data-analyse

In het kader van de risicoanalyse met betrekking tot witwassen maakt de instelling een uitsplitsing van haar cliëntportefeuille. Zodoende krijgt ze meer zicht op de in haar portefeuille aanwezige risicofactoren. Bij de risicofactoren worden onder meer bepaalde rechtsvormen, hoogrisicolanden, -sectoren, -producten of -kanalen en cashbetalingen in beeld gebracht. De volgende onderdelen zijn in deze uitsplitsing onder meer betrokken:

**Cliënten**

- Aantal cliënten per Nederlandse rechtsvorm zoals stichtingen en eenmanszaken.
- Aantal cliënten per buitenlandse rechtsvorm zoals Ltds, S.A.s, en LP en LLPs.
- Aantal cliënten per cliëntsegment zoals particulier, midden- en kleinbedrijf (mkb) en grootzakelijk.
- Aantal cliënten per homogene cliëntgroep zoals minderjarigen, studenten, ouderen en personen die onder curatele staan.

- Aantal cliënten per hoogrisicosector zoals de online gok- en adult entertainment industrie.
- Aantal cliënten dat actief is in cash-intensieve sectoren
- Aantal cliënten in sectoren waarnaar de opsporings- en overheidsdiensten onderzoek hebben gedaan, zoals sectorbrede- en thema-onderzoeken.
- Aantal cliënten dat partnershipconstructies onderhoudt met andere instellingen zoals sub-merchants.

**Producten en diensten**

- Aantal cliënten dat hoogrisicoproducten afneemt/gebruikt zoals cash deposito's, trade finance, anonieme betaalmethoden en prepaid betaalkaarten.
- Aantal cliënten dat gebruik maakt van hoogrisicodiensten zoals cryptodiensten.
- Aantal cliënten dat een hoog aantal betaal- of creditcards heeft aangevraagd.
- Aantal (buitenlandse) cliënten dat Nederlandse IBANs afneemt bij een elektronischgeldinstelling.

**Geografie**

- Aantal cliënten dat actief is in hoogrisicolanden.
- Aantal cliënten gevestigd binnen of buiten Nederland.
- Aantal cliënten gevestigd in offshore jurisdicties of hoogrisicolanden.

**Leveringskanalen**

- Aantal cliënten dat gebruik maakt van specifieke (hoog risico) leveringskanalen zoals brokers, Independent Asset managers of Point of Sale terminals.
- Aantal bijkantoren.

**Transacties**

- Aantal en totaalvolume aan cashtransacties (uitgesplitst per cliëntgroep).
- Aantal en totaalvolume aan inkomende en uitgaande internationale transacties van en naar hoogrisicolanden of hoogrisicobanken.
- De top 10 hoogrisicolanden en/of -banken op basis van transactievolume worden in beeld gebracht en er wordt nader onderzocht of dit aansluit bij de cliëntenportefeuille.
- Significante afwijkingen van transactiestromen naar specifieke hoogrisicolanden of -sectoren ten opzichte van het voorgaande jaar worden in beeld gebracht en er wordt onderzocht of deze verschillen verklaarbaar zijn.

## Good practice – Risicofactoren en data-analyse bij trustkantoor

In het kader van de risicoanalyse met betrekking tot witwassen maakt een trustkantoor een uitsplitsing van zijn cliëntportefeuille. Zodoende krijgt het meer zicht op de in zijn portefeuille aanwezige risicofactoren. Bij de risicofactoren worden onder meer bepaalde rechtsvormen, hoogrisicolanden, -sectoren, -producten of -kanalen in beeld gebracht. De volgende onderdelen zijn in deze uitsplitsing onder meer betrokken:

**Zakelijke relatie/cliënten**

- Aantal doelvennootschappen (DV's) per hoogrisicosector
- Aantal DV's waarbij sprake is van een complexe structuur (>5 lagen)
- Aantal DV's met een trust in de structuur
- Aantal DV's waarbij sprake is van een PEP
- Aantal cliënten/DV's waarbij sprake is van belastingvoordeel door vestiging in Nederland
- Aantal DV's waarbij een DAC6 melding is gedaan t.b.v. de structuur
- Aantal DV's waarbij sprake is van een structuur met elementen die anonimiteit bevorderen (nominee, STAK etc.)
- Aantal DV's dat kwalificeert als stichting
- Aantal DV's met zelfstandige buitendirecteuren

- Aantal DV's zonder bevoegdheid op de rekening/zicht op de rekening
- Aantal DV's waarbij sprake is van circulaire elementen qua entiteiten/eigenaarschap.

**Geografie**
- Aantal DV's dat actief is/een deelneming heeft in hoogrisicolanden
- Aantal DV's dat actief is in offshore jurisdicties
- Aantal DV's waarbij sprake is van meerdere offshore jurisdicties
- Aantal DV's waarbij sprake is van circulaire elementen qua structuur en landen
- Aantal UBO's uit hoogrisicolanden.

**Leveringskanalen**
- Aantal cliënten aangebracht door een feeder
- Aantal cliënten aangebracht door een belastingadviseur.

**Combinatie van risico's**
- Aantal DV's dat actief is/een deelneming heeft in hoogrisicolanden én hoogrisicosector
- Aantal DV's waarbij sprake is van een zelfstandig bevoegde buitendirecteur én geen bevoegdheid rekening/zicht op de rekening
- Aantal DV's met een rechtsvorm in de structuur die anonimiteit in de hand werkt én onderdelen van de structuur met vestiging op offshore jurisdicties.

**Sancties**
- Aantal DV's actief in landen waar sancties van kracht zijn
- Aantal cliënten/UBO's/DV's waarbij sprake is van gesanctioneerde entiteiten/personen
- Aantal DV's waarbij sprake is van strategische en/of dual-use goederen.

**Transacties**
- Aantal DV's waarbij sprake is van transacties zoals bedoeld in artikel 35 Wtt 2018
- Aantal DV's waarbij sprake is van transacties 0-1 mln, 1-10 mln, 10-100 mln, 100-500 mln, >500 mln
- Aantal DV's waarbij sprake is van een aan de FIU gemelde transactie
- Transacties waarbij er sprake is van een kenbaar verlies.

**Bestuur/personeel**
- Aantal UBO's van het trustkantoor woonachtig in een hoog risicoland
- Relevante nevenfuncties van bestuursleden.

## Good practice – Identificatie risico op belangenverstrengeling

Met betrekking tot het risico op belangenverstrengeling komt in het organisatierisicoprofiel een aantal risicofactoren naar voren. Dit betreft onder meer de volgende:
- Op het niveau van het bestuur kunnen bestuurders de instelling zelfstandig binden tot een bedrag van 25 miljoen euro.
- Daarnaast stelt de instelling vast dat de bestuurders diverse nevenfuncties hebben waardoor andere belangen mee kunnen spelen in de besluitvorming. Zo is er een bestuurder die verschillende nevenfuncties heeft bij partijen waarmee de instelling een commerciële relatie onderhoudt. Hieronder is ook een partij waarmee de instelling een significante sponsoringrelatie heeft.

## Good practice – Identificatie risico op (indirecte) discriminatie

Een bank realiseert zich dat bij de uitvoering van haar beleid met betrekking tot de Wwft en de Sanctiewet er sprake kan zijn van onbedoelde bijeffecten, zoals uitsluiting en discriminatie. De bank heeft kennis genomen van een aantal relevante onderzoeken (een onderzoek van het ministerie van Financiën en een onderzoek van DNB).[20] De bank heeft ook in kaart gebracht welke klachten zijn ingediend bij de bank over het ervaren van discriminatie bij de toepassing van maatregelen die de bank toepast met betrekking tot het voorkomen van witwassen en de naleving van sanctiemaatregelen.

Op basis hiervan identificeert de bank het risico dat cliënten, ongewild, (indirect) gediscrimineerd worden bij het uitvoeren van cliënten-onderzoek. De bank besluit een uitgebreidere risicoanalyse te doen om vast te stellen bij welke stappen en elementen in het CDD, TM en Sanctieproces de bank een verhoogd risico loopt dat cliënten onbedoeld gediscrimineerd worden of discriminatie ervaren. Op basis van deze analyse zal de bank passende maatregelen nemen om het risico op (ervaren) discriminatie te mitigeren.

## Good practice – Identificatie risico's en factoren trustkantoor

Een trustkantoor doet een analyse van zijn portefeuille. Daaruit komen relevante risico's en risicofactoren naar voren:

1. Het trustkantoor ziet dat het kwetsbaar is voor witwassen via vastgoed. Het heeft een aantal doelvennootschappen met een zelfstandig bevoegde buitendirecteur in combinatie met activiteiten in de hoogrisicosector vastgoed. Ook stelt het trustkantoor vast dat bij de helft daarvan sprake is van meerdere vennootschappen in de structuur waarbij de UBO in al die vennootschappen betrokkenheid heeft. Dit wijst op een verhoogd risico op witwassen met vastgoed door bijvoorbeeld ABC-transacties.
2. Het trustkantoor heeft een aantal doelvennootschappen met operationele activiteiten in landen die geografisch dichtbij landen liggen waarop sancties van kracht zijn, en hiermee nauwe politieke banden onderhouden. Dit wijst op mogelijke blootstelling aan het ontwijken van sanctiemaatregelen.
3. Ook identificeert het trustkantoor potentiële betrokkenheid bij corruptie en de ontvangst van uit corruptie afkomstige gelden. Het kantoor heeft een aantal doelvennootschappen met activiteiten in landen met een slechte score in de Corruption Perceptions Index (CPI) in combinatie met activiteiten in een branche die gevoelig is voor corruptie. Dit betreft in dit geval een staatsbedrijf en een bedrijf dat actief is in de mijnbouw. Ook stelt het trustkantoor vast dat er sprake is van betrokkenheid van een PEP.

20 Zie: www.rijksoverheid.nl/documenten/publicaties/2024/04/19/rapport-kmpg-en-i-o-research-naar-ervaren-discriminatie. Zie ook: www.dnb.nl/media/ozsdxez4/78730-2400217-dnb-brochure-tegengaan-van-discriminatie_tg-pdfa.pdf.

## Good practice – Identificatie risico's en factoren betaaldienstverlener

Een betaaldienstverlener doet een analyse van haar portefeuille. Daaruit komen relevante risico's en risicofactoren naar voren:

1. De betaaldienstverlener identificeert dat zij mogelijk betrokken kan zijn bij de omzeiling van sanctiemaatregelen. Zij heeft namelijk een analyse uitgevoerd van de risicofactoren in haar MKB-portefeuille met betrekking tot transactiestromen. De instelling heeft hierbij inzichtelijk gemaakt wat het totale aantal en volume aan inkomende een uitgaande internationale transacties naar hoogrisicolanden is, en hoe dit zich verhoudt tot de cijfers van voorgaande jaren. Hieruit blijkt dat het transactievolume naar een bepaald hoogrisicoland sterk is gestegen sinds er sancties zijn ingesteld ten aanzien van een buurland daarvan.
2. Op grond van een analyse van haar cliëntenportefeuille identificeert de betaaldienstverlener specifieke factoren met betrekking tot witwasrisico's. De instelling ziet in haar cliëntenportefeuille een sterke toename van cliënten die actief zijn in cryptohandel via niet geregistreerde buitenlandse platformen – er is een groep cliënten met grote transactievolumes richting deze platformen. Tevens identificeert de instelling een aantal cliënten dat actief is in de gokindustrie en een sterk stijgend transactievolume heeft laten zien.
3. Om meer zicht te krijgen op mogelijke blootstelling aan het witwasrisico vanwege de risicofactor 'cash' voert de betaaldienstverlener een analyse uit van het cashgebruik door haar retailklanten. De instelling maakt inzichtelijk welke cliënten meer dan een bepaald bedrag aan contanten storten per jaar. Dit doet zij voor een aantal verschillende grenswaarden (20.000 euro, 50.000 euro en 100.000 euro). De instelling identificeert een aantal cliënten waar het gestorte bedrag aan cash vele malen hoger is dan het jaarinkomen van de betreffende cliënt.

## Good practice – Ontplooien nieuwe activiteit

Een instelling zoekt actief naar groeimogelijkheden, en naar mogelijkheden om de cliëntrelaties te versterken en te verdiepen. De instelling overweegt om een nieuwe activiteit te ontplooien. Als onderdeel van het besluitvormingsproces laat de instelling een integriteitsrisicoanalyse uitvoeren. Deze 'SIRA voor de nieuwe activiteit' maakt inzichtelijk welke integriteitsrisico's aan de orde zijn bij het operationaliseren, implementeren en voeren van de mogelijke nieuwe activiteit. Deze integriteitsrisicoanalyse ligt mede ten grondslag aan de besluitvorming over het al dan niet aangaan van de nieuwe activiteit en onder welke voorwaarden.

# 4 Risicoanalyse

## Ratio

Na het maken van het organisatierisicoprofiel, zoals beschreven in het voorgaande hoofdstuk, beschikt de instelling over een overzicht van de voor haar relevante integriteitsrisico's. Om passende beheersmaatregelen te kunnen ontwikkelen en te kunnen toepassen, en om daarin prioriteiten te kunnen stellen, is het van belang dat de instelling een risicoanalyse uitvoert. Zij analyseert de geïdentificeerde risicofactoren en integriteitsrisico's en maakt een inschatting van de materialiteit en de frequentie waarop de geïdentificeerde risico's zich mogelijk manifesteren.

Hoe de risicoanalyse wordt uitgevoerd is afhankelijk van de instelling en het risico. In sommige gevallen zal de nadruk liggen op kwantitatieve verdiepende data-analyse en in andere gevallen en/of bij andere risico's zal het analyseren van belangrijke verschijningsvormen, bijvoorbeeld door scenarioanalyse, het meeste inzicht bieden. Een combinatie van methoden blijkt in de praktijk vaak toegevoegde waarde te bieden. In ieder geval zal na de risicoanalyse voor de instelling duidelijk moeten zijn welke risico's het meeste aandacht behoeven en met welke (soort) beheersmaatregelen zij haar risico's zou kunnen beheersen.

## Good practices

### Good practice – Gebruik externe bronnen

Een bank gebruikt bij de risicoanalyse voor wat betreft de witwas-risico's die zij loopt, naast de NRA, inzichten uit de publicaties van de Financial Action Task Force (FATF), het Anti Money Laundering Centre (AMLC) en andere relevante externe bronnen (zoals risicoanalyses van brancheorganisaties) die inzicht geven in typologieën en indicatoren met betrekking tot integriteitsrisico's.

Dit wordt ook toegepast bij de diverse organisatieonderdelen. De compliance officer voor de afdeling 'Correpondent Banking' maakt voor de analyse bijvoorbeeld gebruik van de FATF-guidance over correspondent banking. Deze FATF-guidance verwijst naar "The risk factors included in the Annex II of the BCBS Guidelines on *Sound management of risks related to money laundering and financing of terrorism*".[21]

Bij de risicoanalyse betrekt de bank op basis daarvan de volgende factoren:
- het inherente risico dat voortvloeit uit de aard van de verleende diensten;
- de kenmerken van (en informatie over) de respondentbank;
- de omgeving/jurisdictie waarin de respondentbank opereert.

Verder heeft de bank in de risicoanalyse bijzondere aandacht voor 'nested correspondent banking'.[22]

21 FATF (2016), *Guidance on correspondent banking services* (Guidance on Correspondent Banking (fatf-gafi.org)), p. 10. Zie verder BCBS (2020), *Guidelines on Sound management of risks related to money laundering and financing of terrorism* (Sound management of risks related to money laundering and financing of terrorism (bis.org)).
22 BCBS (2020), *Guidelines on Sound management of risks related to money laundering and financing of terrorism*, p. 27; www.austrac.gov.au/correspondent-banking-relationships. *Nested correspondent banking*: a bank's correspondent relationship is used by a number of indirect respondent banks ('nested banks') through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

## Good practice – Gebruik witwasindicatoren door geldtransactiekantoor

In het organisatierisicoprofiel van een geldtransactiekantoor is opgenomen dat de vestigingen in toeristische gebieden relatief meer verschillende valuta's verwerken. In dat verband zijn er ook enkele kantoren (in Nederland) waar veel klanten met een Frans woonadres een of meerdere keren per maand transacties laten uitvoeren.

Uit het bij de risicoanalyse betrokken Overzicht Witwasindicatoren van het AMLC blijkt dat het een feit van algemene bekendheid is "dat diverse vormen van criminaliteit gepaard gaan met grote hoeveelheden contant geld in diverse valuta."[23] Op basis hiervan komt het geldtransactiekantoor tot de analyse dat de witwasrisico's die samenhangen met het plaatsen van contant geld hoger zijn bij transacties met grote hoeveelheden contant geld in diverse valuta's, en dat dit specifieke risico zich met name manifesteert bij vestigingen in de geïdentificeerde toeristische gebieden.

Bij de risicoanalyse betrekt het geldtransactiekantoor ook de ML/TF Risk Factors Guidelines van de EBA. Als factor die kan bijdragen aan een hoger risico staat vermeld: "The customer's needs may be better serviced elsewhere, for example because the money remitter is not local to the customer or the customer's business." Op basis hiervan analyseert het geldtransactiekantoor dat de dienstverlening door de Nederlandse kantoren aan de cliënten met een Frans woonadres een verhoogd risico op witwassen meebrengt.

## Good practice – Gebruik witwasindicatoren door levensverzekeraar

In het organisatierisicoprofiel van een levensverzekeraar komt m.b.t. producten naar voren dat de instelling uitsluitend overlijdensrisicoverzekeringen aanbiedt. De premies worden geïnd vanaf een vaste tegenrekening. De premies zijn gemiddeld circa 1.000 euro per jaar en zijn niet hoger dan 5.000 euro per jaar.

Bij de risicoanalyse betrekt de instelling de ML/TF Risk Factors Guidelines van de EBA. Op basis van Guideline 14.7 analyseert de instelling dat de overlijdensrisicoverzekeringen een laag witwasrisico vormen.

## Good practice – Deelanalyse van het risico op belangenverstrengeling

Een verzekeraar maakt een analyse van het risico van belangenverstrengeling op het niveau van het bestuur.

In haar analyse neemt de instelling als uitgangspunt de vraag hoe bestuurders zichzelf en/of aan hen gerelateerde partijen kunnen bevoordelen met gebruikmaking van hun beslissingsbevoegdheid – de instelling ziet dit als een belangrijke risicofactor. De bestuurder met 'Compliance' in de portefeuille heeft namelijk in een DNB-publicatie gezien dat DNB wijst op het risico van bestuurders met aanzienlijke procuratiebevoegdheden voor het zelfstandig doen van toezeggingen en/of betalingen. Het hanteren van hoge procuratiebevoegdheden

23 Anti Money Laundering Centre, *Overzicht Witwasindicatoren*, p. 4. Bij het opstellen van deze Good practice was de versie februari 2024 de actuele versie: Overzicht-witwasindicatoren-februari-2024.pdf (amlc.nl).

voor een bestuurder brengt een verhoogd risico op belangenverstrengeling mee.[24]

Om dit concreet te maken analyseert de instelling verschillende mogelijke verschijningsvormen hiervan, zoals:

- aan- of verkoop in privé van of aan de instelling (bijvoorbeeld vastgoed of bedrijfsmiddelen)
- een persoonlijk gerelateerd bedrijf inhuren voor opdrachten
- goedkeuren van declaraties die in werkelijkheid privéuitgaven betreffen
- het aanschaffen van bedrijfsmiddelen voor hoofdzakelijk privédoelen, zoals een auto of een vakantiehuis
- dienstverlening met voor de dienstverlener uitzonderlijk gunstige voorwaarden goedkeuren
- laten uitnodigen voor reizen en seminars, en deze accorderen
- beïnvloeding van besluiten die gunstig zijn voor een organisatie waar de bestuurder een nevenfunctie heeft (bijvoorbeeld sponsoring van een gerelateerde partij).

Vanwege de positie in de besluitvorming analyseert de instelling verder dat bestuurders over vertrouwelijke informatie beschikken en ziet daarbij de volgende mogelijke verschijningsvormen van integriteitsrisico's:

- vertrouwelijke informatie doorspelen aan een organisatie waar de bestuurder een nevenfunctie vervult
- voorkennis inzetten ten behoeve van zelfverrijking.

De instelling werkt deze verschijningsvormen nader uit in concrete scenario's om een inschatting te maken van hoe een risico zich kan manifesteren en wat de eventuele impact daarvan dan is. Ook gebruikt de instelling de scenario's om mitigerende maatregelen te ontwikkelen.

## Good practice – Gebruik scenario's – Belangenverstrengeling via inhuur eigen bedrijf bestuurder

Om concreet te maken hoe integriteitsrisico's zich kunnen manifesteren, stelt een instelling scenario's op en beschrijft deze als een serie concrete handelingen.

Op deze manier heeft de instelling een scenario opgesteld inzake de inhuur door de instelling van een eigen bedrijf van een bestuurder. Dit scenario bevat concrete stappen en handelingen:

1. De instelling formuleert een opdracht op basis waarvan een externe partij kan worden aangezocht.
2. Een van de (commercieel) directeuren geeft aan een geschikte partij hiervoor te weten, en deze wel te willen polsen. De directeur is mede-aandeelhouder van de betreffende partij – zij meldt dit belang niet.
3. De betreffende directeur rapporteert naderhand positief over dit verkende contact, geeft aan dat de betreffende partij een kundige en professionele indruk maakt, en dat op korte termijn een offerte voor de werkzaamheden zal volgen.
4. Na ontvangst van de offerte wordt deze door de betreffende directeur geaccordeerd.
5. Naderhand geeft de betreffende directeur bovendien akkoord op betaling van de facturen.

Aan de hand van dit scenario analyseert de instelling dat het voorafgaand aan de besluitvorming van belang is om inzicht te hebben in de eventuele belangen die betrokkenen hebben, en dat deze expliciet aan de orde komen bij het nemen van het besluit. Ook is het van belang dat over de inhuur van derden niet door één persoon besloten kan worden.

24 DNB (2024), *Integriteitstoezicht in Beeld 2024-2025*, p. 15.

## Good practice – Gebruik scenario's – Witwassen via loanback

In haar organisatierisicoprofiel heeft een instelling geconstateerd dat een relatief groot percentage kleinere vennootschappen in haar cliëntenbestand leningen ontvangt van buitenlandse partijen. De instelling identificeert een risico van betrokkenheid bij witwassen via door cliënten toegepaste *loanback* constructies, en werkt dit uit in een scenario:

Met een zogenoemde loanback constructie laat een persoon of entiteit het lijken alsof deze via een lening van een andere partij legaal geld tot zijn beschikking heeft gekregen. Echter, in feite 'leent' men door middel van een gelieerde entiteit (niet legaal verkregen) geld aan zichzelf. De gelieerde entiteit kan bijvoorbeeld deels dezelfde bestuurders of UBO's hebben. De lening vormt een titel voor het ogenschijnlijk legaal ter beschikking hebben van gelden die door criminaliteit zijn verkregen. De volgende handelingen zijn aan de orde:

- Onderneming A is cliënt.
- Een buitenlandse onderneming B verstrekt een lening aan onderneming A. Er gaat een geldstroom van onderneming B naar onderneming A. Deze geldstroom wordt onderbouwd met een leningovereenkomst.
- De leningkenmerken hebben ongebruikelijke aspecten, zoals hogere of lagere rente dan gebruikelijk, geen zekerheden, geen aflossingstermijnen of jaarlijks uitstel van de aflossing.
- Hoewel de leningovereenkomst suggereert dat onderneming A het geleende bedrag zal terugbetalen aan onderneming B, gebeurt dit in werkelijkheid niet. Het geld blijft bij onderneming A en wordt gebruikt voor andere doeleinden.

Aan de hand van dit scenario analyseert de instelling dat het in deze situatie van belang is om diepgaand onderzoek te doen naar mogelijke relaties tussen onderneming A en onderneming B, en om met name goed na te gaan wie de UBO's en bestuurders zijn. Ook is het van belang om voldoende zicht te hebben op de herkomst van de geldstroom die verbonden is aan de lening en om de bedrijfseconomische ratio van de lening en de leningsvoorwaarden na te gaan. Dit alles geldt ook voor vergelijkbare scenario's, waarin bijvoorbeeld geld wordt geleend van een particulier.

## Good practice – Gebruik scenario's – Trade based money laundering

In haar organisatierisicoprofiel heeft een bank t.a.v. haar dienstverlening op het gebied van handelsfinanciering geïdentificeerd dat er een risico bestaat van betrokkenheid bij witwassen via *trade based money laundering*, waarbij cliënten gebruik maken van handelsstructuren om crimineel verkregen geld een legitieme herkomst te geven. De bank maakt een overzicht van mogelijke verschijningsvormen van *trade based money laudering*:

- Onderneming A ontvangt van onderneming B (uit het buitenland) een partij goederen. Deze goederen hebben een niet-marktconforme prijs, de prijs is (veel) te hoog of te laag.
- Onderneming A ontvangt van onderneming B (in het buitenland) een partij goederen die zijn voorzien van facturen en *bills of lading* die inconsistenties vertonen.
  - De prijs of het gewicht op de documenten komt niet overeen.
  - Bij meerdere facturen voor dezelfde achtereenvolgende goederenstromen kunnen ook inconsistenties in factuurnummers, containernummers of BTW-nummers opvallen.
- Onderneming A ontvangt van onderneming B een partij goederen die geïmporteerd wordt via een vliegveld, waarbij de logica om dit via een vliegtuig te vervoeren ontbreekt.
- Onderneming A ontvang van een buitenlandse onderneming B een partij goederen die logischerwijs niet uit dat land afkomstig kan zijn

of waarvan er in het land van onderneming A voldoende laaggeprijsde goederen aanwezig zijn.

De instelling werkt deze verschijningsvormen nader uit in concrete scenario's om een inschatting te maken van hoe een risico zich kan manifesteren en wat de eventuele impact daarvan dan is. Ook gebruikt de instelling de scenario's om mitigerende maatregelen te ontwikkelen.

## Good practice – Data-analyse en referentiegroepen

Bij het analyseren van de cliëntenportefeuille maakt een instelling gebruik van referentiegroepen: groepen cliënten met een aantal overeenkomende kenmerken. Het doel van de analyse is om afwijkend en opvallend gedrag (outliers) te kunnen detecteren met het oog op het witwasrisico. De instelling zorgt er daarom voor dat de groep cliënten in een referentiegroep voldoende homogeen is, en heeft bijvoorbeeld de volgende referentiegroepen gedefinieerd:

- personen die gebruik maken van een studentenbetaalrekening
- minderjarigen die gebruik maken van een kinderrekening
- cliënten die onder curatele staan
- cliënten met slapende rekeningen
- zakelijke cliënten die in dezelfde sector actief zijn, zoals kappers en taxibedrijven.

Op basis van de gedefinieerde referentiegroepen en met gebruikmaking van o.a. de witwasindicatoren van het AMLC stelt de instelling afwijkend en opvallend gedrag (outliers) vast. De gedragingen, die kunnen wijzen op betrokkenheid bij witwasstromen, die de instelling met haar analyse in haar portefeuille waarneemt betreffen bijvoorbeeld:

- cliënten die opvallend meer cash opnemen- en/of storten, wat op basis van het cliëntprofiel niet verklaard kan worden
- cliënten die een (relatief) veel hogere of lagere omzet hebben dan hun *peers*
- cliënten die grotere inkomende- en uitgaande geldstromen naar hoogrisicolanden hebben dan hun *peers*
- cliënten die t.o.v. hun *peers* veel betaalkaarten hebben aangevraagd
- cliënten die relatief meer tikkies ontvangen of uitbetalen dan hun *peers*.

De instelling analyseert dat deze witwasindicatoren concreet bij haar voorkomen. Bij de inrichting van haar transactiemonitoringsysteem houdt de instelling specifiek rekening met deze indicatoren.

## Good practice – Verdiepende data-analyse en key risk indicators bank

Een bank maakt een verdiepende kwantitatieve analyse om de geïdentificeerde integriteitsrisico's uit te diepen en de daadwerkelijke omvang en impact van het risico goed in te kunnen schatten.

Allereerst stelt de bank specifieke onderwerpen vast waar hoge integriteitsrisico's geïdentificeerd zijn en waarop verdiepende analyses benodigd zijn, zoals:

- Transacties met hoogrisicolanden.
- Transacties met hoogrisicosectoren of -instellingen.
- Internationale transacties die onlogisch zijn op basis van het doel en de aard van de zakelijke relatie.
- Cliënten met veel betaalkaarten of creditcards.
- Adressen waar zeer veel cliënten ingeschreven zijn.
- Minderjarigen met grote volumes over de rekening.

- Cliënten met opvallend veel cashgebruik wat op basis van het cliëntprofiel niet verklaard kan worden.

In de verdiepende analyse t.a.v. het opvallende cashgebruik kijkt de instelling zowel naar de kans op als de impact van het optreden van het risico. Hierbij worden onder meer de volgende factoren betrokken:

- Contante stortingen
  1. Hoeveel natuurlijke personen en rechtspersonen storten meer dan EUR X bedrag aan contanten en wat zijn de mogelijke *outliers* hierop?
  2. Hoeveel transacties betreffen dit? Wat is het totale volume? Betreft het een specifieke groep natuurlijke personen of rechtspersonen?
  3. Wat is het geografische profiel van de contante stortingen?
  4. Hoe verhouden de cash stortingen zich tot de *peers* van specifieke cliëntgroepen?
- Contante opnames
  5. Hoeveel natuurlijke personen en rechtspersonen nemen meer dan EUR X bedrag contanten op en wat zijn de mogelijke *outliers* hierop?
  6. Hoeveel transacties betreffen dit? Wat is het totale volume? Betreft het een specifieke groep natuurlijke personen of rechtspersonen?
  7. Wat is het geografische profiel van de contante opnames?
  8. Hoe verhouden de cashopnames zich tot *peers* van specifieke clientgroepen?

In de verdiepende analyse t.a.v. hoogrisicolanden wordt zowel gekeken naar de kans als de impact van het risico. Hierbij kijkt de instelling onder meer naar de volgende factoren:

- Aantal cliënten en volume aan transacties zowel inkomend als uitgaand bij vestigingen in offshore jurisdicties en/of hoog-risicolanden.
- Veranderingen in de tijd in aantal cliënten en volume aan transacties zowel inkomend als uitgaand bij vestigingen in offshore jurisdicties en/of hoogrisicolanden.

Op grond van de uitkomsten van deze analyses kan de instelling bepalen waar kans en impact van de risico's significant zijn. Aan de hand daarvan definieert de instelling *key risk indicators*.

## Good practice – Verdiepende data-analyse en key risk indicators betaalinstellingen en elektronischgeldinstellingen

Een betaalinstelling maakt een verdiepende kwantitatieve analyse om de geïdentificeerde risico's verder uit te diepen en de daadwerkelijke omvang en impact van het integriteitsrisico goed in te kunnen schatten.

Allereerst stelt de instelling specifieke onderwerpen vast waar hoge integriteitsrisico's geïdentificeerd zijn en waarop verdiepende analyses benodigd zijn zoals:

- Producten zoals het gebruik van anonieme betaalmethoden die met contanten opgewaardeerd kunnen worden.
- Producten zoals het aanbieden van digitale *wallets* die met contante gelden of crypto opgewaardeerd kunnen worden.
- Producten zoals het uitgeven van IBANs aan buitenlandse cliënten.
- Cliënten die cashback transacties op andere rekeningen terug willen laten storten.
- Transacties met hoogrisicosectoren of instellingen zoals online *gaming en gambling*.
- Transacties ten behoeve van partnerconstructies.
- Transacties met hoogrisicolanden.

In de verdiepende analyse t.a.v. het gebruik van anonieme betaalmethoden kijkt de instelling naar de kans en de impact van het risico. Hierbij is onder meer naar de volgende factoren gekeken:

- Hoeveel transacties worden uitgevoerd via anonieme betaalmethoden (per cliënt en totaal)?
- Hoeveel cliënten nemen meer dan X aantal verschillende anonieme betaalmethoden af om aan haar eindgebruikers aan te bieden?
- Wat is het volume dat via deze anonieme betaalmethoden loopt (per cliënt en totaal)?
- Betreft het een specifieke groep cliënten die een groot aantal anonieme betaalmethoden afneemt om aan haar eindgebruikers aan te bieden?
- Wat is het geografische profiel van cliënten die deze anonieme betaalmethoden aanbieden aan haar eindgebruikers?

Op grond van de uitkomsten van deze analyse bepaalt de instelling de volgende *key risk indicators:*

- Het X aantal verschillende betaalmethoden dat wordt afgenomen door een cliënt.
- Het X aantal verschillende betaalmethoden dat wordt afgenomen door een cliënt in een hoogrisicoland.
- Het X aantal transacties dat wordt uitgevoerd via anonieme betaalmethoden (per cliënt en totaal).
- Het X volume dat via deze anonieme betaalmethoden loopt (per cliënt en totaal).

## Good practice – Verdiepende data-analyse met risicofactoren en scenario's trustkantoren

Een trustkantoor maakt een verdiepende kwantitatieve analyse om de geïdentificeerde witwasrisico's verder uit te diepen en de daadwerkelijke omvang en impact van dit integriteitsrisico goed in te kunnen schatten.

Het trustkantoor heeft meerdere doelvennootschappen in hoogrisicolanden en hoogrisicosectoren. Het trustkantoor analyseert van al deze doelvennootschappen de transacties aan de hand van de volgende risicofactoren, die volgens door het kantoor bestudeerde externe bronnen relevant zijn:

- Transacties waarbij een PEP is betrokken.
- Transacties waar staatsbedrijven bij zijn betrokken.
- Transacties waarvoor onvoldoende onderbouwende documentatie is aangeleverd om de herkomst/legitimiteit te kunnen duiden.
- Transacties waarbij sprake is van circulaire elementen (zoals circulaire transacties binnen dezelfde groep of transacties van land A, via land B, retour naar land A).
- Transacties waarbij gelieerde ondernemingen betrokken zijn (een onderneming met dezelfde UBO, hetzelfde bestuur, of van familieleden).
- De aanwezigheid van leningsovereenkomsten.

Het trustkantoor werkt deze indicatoren voor zijn portefeuille nader uit in concrete scenario's om een inschatting te maken van hoe en waar een risico zich kan manifesteren en wat de eventuele impact daarvan dan is. Ook gebruikt de instelling de scenario's om, waar nodig per doelvennootschap, mitigerende maatregelen te ontwikkelen.

# 5 Risicobeheersing

## Ratio

De risicoanalyse zoals beschreven in het vorige hoofdstuk levert belangrijke inzichten op voor verschillende afdelingen binnen de organisatie. Deze inzichten bieden in de eerste plaats sturing voor het management. Daarmee wordt de basis gelegd voor het (periodiek te herziene) integriteitbeleid op grond waarvan de instelling haar integriteitsrisico's wil beheersen. De instelling zal daarom op basis van de risicoanalyse beleid, procedures en maatregelen in werking stellen ter beheersing van haar integriteitsrisico's.[25]

Daarmee is het doel van de risicobeheersing gegeven: door de inzet van beheersmaatregelen mitigeert de instelling de integriteitsrisico's die in haar SIRA-proces naar voren komen. De instelling gaat hierbij na of de risico's ook afdoende door haar gemitigeerd kunnen worden. Op basis hiervan kan de instelling het overblijvende risico accepteren, verder beperken door de inzet van aanvullende beheersmaatregelen of vermijden.

Bij risicobeheersing gaat het er om dat de instelling beheersmaatregelen toepast die passend zijn bij het risico. Het is niet alleen van belang dat instellingen bij hogere risico's meer of intensievere maatregelen nemen, het is ook passend dat instellingen de ruimte benutten voor een minder zware inzet bij lage risico's. Dit impliceert dat een weloverwogen risico-afweging ook kan leiden tot een keuze die achteraf gezien toch niet het gewenste resultaat heeft. Dat wil dan niet per definitie zeggen dat de bedrijfsvoering gefaald heeft. Met andere woorden, een goede risicobeheersing betekent niet dat onwenselijke gebeurtenissen niet meer optreden. Het wil wel zeggen dat de instelling het redelijkerwijs mogelijke heeft gedaan om het optreden van een dergelijke gebeurtenis te voorkomen en de negatieve gevolgen adequaat kan beperken mocht een onwenselijke gebeurtenis zich toch voordoen.

## Good practices

### Good practice – Vaststellen beheersmaatregelen op basis van het scenario 'inhuur eigen bedrijf bestuurder'

Een verzekeraar heeft in de risicoanalyse een scenario inzake belangenverstrengeling via inhuur eigen bedrijf opgesteld. Uit de analyse volgt dat dit een materieel risico is.

Het scenario stelt de verzekeraar in staat om passende maatregelen te bepalen om dit risico te beheersen. Op basis hiervan past zij de volgende beheersmaatregelen toe:

- De instelling hanteert een gedragscode waarin staat dat beleidsbepalers belangenverstrengeling of de schijn daarvan dienen te melden.
- De instelling houdt een register van belangen en nevenactiviteiten bij.
- De instelling hanteert criteria voor selectie van externe partijen, en beschikt over een procedure voor de gunning van opdrachten.
- Indien een bestuurder een partij aanbrengt wordt deze bestuurder gevraagd naar de bron van de positieve aanbevelingen van de door hem aangebrachte partij en naar zijn eventuele relatie met de betreffende partij. Het register van belangen en nevenactiviteiten wordt geraadpleegd, en bij grotere opdrachten vindt een aanvullend onderzoek plaats in open bronnen.
- Voordat het gesprek met de externe partij wordt aangegaan, wordt eerst getoetst of de betreffende partij aan de criteria voldoet. Ook

25 Het geheel van beleid, procedures en maatregelen wordt ook aangeduid als 'beheersmaatregelen'.

wordt bepaald hoe en of het gesprek past binnen de bestaande procedures.
- Het inventariserende gesprek wordt gezamenlijk gevoerd (4-ogen principe). De aanbrengende bestuurder neemt niet deel aan het gesprek indien hij een relatie heeft met de betreffende partij.
- Tijdens het gesprek wordt de selectieprocedure toegelicht. Van het inventariserend gesprek wordt een gespreksverslag opgesteld. Het verslag vermeldt de specifieke aanleiding voor het gesprek en de betrokkenheid en/of relatie van de afgevaardigden bij dit onderdeel en deze partij.
- De selectieprocedure wordt doorlopen waarbij meerdere offertes worden opgevraagd, toetsing van partijen plaatsvindt aan de hand van de selectiecriteria, waar mogelijk met meerdere partijen wordt gesproken, en het 4-ogen principe gehanteerd wordt.
- Personen in de selectiecommissie geven schriftelijk hun eventuele relatie(s) aan met de kandidaten. Ook wordt het register met belangen en nevenactiviteiten geraadpleegd. Bij mogelijk conflicterende belangen of de schijn daarvan wordt de betreffende persoon buiten de selectiecommissie geplaatst.
- De bestuurders en eigenaren van de kandidaatpartijen worden in beeld gebracht.
- Er is een duidelijke vastlegging en begrenzing van de vertegenwoordigingsbevoegdheid voor accordering.
- Ten aanzien van het facturatieproces:
  - Er vindt toetsing plaats op de uitvoering van de werkzaamheden.
  - Er wordt een 4-ogen principe gehanteerd op het accorderen (en betalen) van facturen.
  - De procuratiebevoegdheid is vastgelegd en begrensd.

## Good practice – Vaststellen beheersmaatregelen op basis van scenario *loanback* bij een bank of trustkantoor

Uit de risicoanalyse van een instelling volgt dat de betrokkenheid bij een *loanback* scenario een materieel risico is.[26] De instelling gebruikt het door haar opgestelde *loanback* scenario om verschillende mitigerende maatregelen vast te stellen ter beheersing van dit risico.

**Transactiemonitoring**
De instelling stelt business rules op die binnen het transactie-monitoringsysteem verdachte transacties identificeren die kunnen wijzen op een *loanback*-constructie.[27] Deze regels omvatten:
- Detectie van opeenvolgende transacties tussen dezelfde partijen die de normale bedrijfsactiviteiten overschrijden.
- Detectie van grote overboekingen naar de client met als omschrijving 'lening' of gelijkwaardige omschrijvingen – terwijl deze overboekingen niet afkomstig zijn van een reguliere kredietverstrekker.

Drempelwaarden worden ingesteld voor transacties die afwijken van normaal gedrag / het transactieprofiel, waardoor verdachte activiteiten verder worden onderzocht.

**Verscherpte Customer Due Diligence (CDD)**
De instelling voert naar aanleiding van gegenereerde alerts diepgaand onderzoek uit naar de achtergrond van cliënten die betrokken zijn bij transacties met leningovereenkomsten met overboekingen van buitenlandse entiteiten. In het bijzonder besteedt de instelling aandacht aan:
- Ongebruikelijke bedrijfsstructuren, zoals cliënten met slapende bedrijven of bedrijven met weinig activiteiten, de reden voor deze structuren moet duidelijk en rationeel zijn.

26 Zie Good practice – Gebruik scenario's – Witwassen via loanback in hoofdstuk 4.
27 Zie voor een nadere toelichting op transactiemonitoring en het gebruik van business rules: DNB Q&As en Good Practices Wwft, § 4.1

- De herkomst van de middelen die onder de noemer 'lening' bij de cliënt komen. Hiertoe wordt ook de leningdocumentatie geanalyseerd, eventueel met inzet van bijzondere analyses en hulpmiddelen (zie hieronder).
- Wanneer er sprake is van leningen wordt nagegaan of er ook sprake is van een periodieke betaling van rente en aflossing.

**Geautomatiseerde analyse van leningovereenkomsten**
De instelling maakt gebruik van analysesoftware om leningovereenkomsten van cliënten te scannen op verdachte patronen of inconsistente informatie. De instelling:

- Identificeert leningovereenkomsten waarbij de voorwaarden en bedragen onrealistisch lijken in verhouding tot de normale bedrijfsactiviteiten van de betrokken partijen.
- Controleert op mogelijk valse documentatie. Bijvoorbeeld documentatie met een lay-out die wijst op gekopieerde elementen of inconsistente handtekeningen – deze factoren kunnen wijzen op frauduleuze leningovereenkomsten.
- Controleert het aflossingsschema in de leningovereenkomsten en controleert of geen sprake is van voortdurende opschorting van aflossingstermijnen.

## Good practice – Vaststellen beheersmaatregelen naar aanleiding van data-analyse van transacties naar hoogrisicolanden

Een bank heeft geanalyseerd dat de exposure op hoogrisicolanden een materieel risico inhoudt. Zij heeft een diepgaande analyse gedaan naar de transactiestromen in haar portefeuille naar hoogrisicolanden.

- De bank gebruikt deze analyse om een groep klanten te identificeren die een outlier vormen ten opzichte van hun peers. Deze klanten worden onderworpen aan een Event Driven Review (EDR).
- Ook beoordeelt de bank of het transactiegedrag van de klanten past binnen de risicobereidheid van de instelling, en zo niet, welke mitigerende maatregelen in dit kader nodig zijn.
- Tevens gebruikt de bank de inzichten uit de analyse om haar mitigerende maatregelen beter in te richten. Waar nodig worden business rules of modellen ten behoeve van transactiemonitoring aangescherpt.

## Good practice – Vermijden risico

Een instelling die actief is in de EU onderzoekt de mogelijkheden om haar activiteiten uit te breiden. Een van de mogelijkheden betreft het aanbieden van producten en diensten via lokale agenten in Zuid-Amerikaanse landen. Na het uitvoeren van een SIRA ziet de instelling dat het corruptierisico hoog is. De instelling wil niet betrokken raken bij corruptie. Tegelijkertijd vraagt de beheersing van dit risico in dit geval om intensievere maatregelen en een hoge mate van professionaliteit. De gevraagde capaciteit en expertise overstijgen de mogelijkheden van de instelling. De instelling besluit om het risico te vermijden en af te zien van deze mogelijkheid.

## Good practice – Monitoren op betaalverzoeken

Een instelling stelt in haar risicoanalyse vast dat een grote hoeveelheid ontvangen en verstuurde betaalverzoeken van of naar één cliënt een indicator zou kunnen zijn voor fraude of witwassen. Op basis van deze analyse en van haar risicotolerantie heeft de instelling *Key Risk Indicators* (KRI's) vastgesteld per peer groep, op het aantal ontvangen en verstuurde betaalverzoeken en de omvang van de bedragen die daarmee zijn gemoeid. Bij het doorbreken van de grens zoals gesteld in de KRI volgt een Event Driven Review (EDR).

### Good practice – Betalingsautorisatieprocedure

Een bestuurder van een instelling is zelfstandig bevoegd om tot 10 miljoen euro de instelling te binden. Om te voorkomen dat bestuurders hier misbruik van maken heeft de instelling procedures in werking die onder meer borgen dat bij besluitvorming over verbintenissen het vier-ogenprincipe wordt toegepast en ook dat ten minste twee personen toestemming moeten geven voor het vrijgeven van betalingen. Dit laatste wordt door het betalingssysteem van de instelling afgedwongen.

### Good practice – Leningen aan bestuurders

Een instelling verstrekt leningen aan bestuurders. Uit de risicoanalyse volgt dat hier een materieel risico bestaat op belangenverstrengeling. Om dit risico te beheersen heeft de instelling in beleid en procedures vastgelegd dat dergelijke leningen uitsluitend worden verstrekt in de normale uitoefening van het bedrijf en slechts worden afgesloten na instemming door de raad van commissarissen. Bij het voorstel aan de raad van commissarissen is een opinie van de compliance officer gevoegd.

### Good practice – Data-analyse voor cashgebruik: KRI's en transactiemonitoring

Een instelling heeft op basis van een data-analyse op het cashgebruik van haar cliënten inzicht verkregen in het gemiddelde cashgebruik en in outliers waar het gaat om cashgebruik van haar retailcliënten en de verschillende referentiegroepen binnen deze populatie. Op basis van deze verkregen inzichten worden KRI's opgesteld per referentiegroep, alsook transactiemonitoring rules. Van cliënten die vervolgens afwijken van de KRI's wordt bepaald of een EDR nodig is. Hierbij wordt de cliënt enkel bevraagd indien sprake is van opvallend en mogelijk niet legitiem gebruik van contant geld.

### Good practice – Landenrisico en beheersing

Een instelling heeft voor zichzelf een aantal landen gedefinieerd die zij als hoog risico beschouwt, gebruikmakend van verschillende externe bronnen. Op basis hiervan heeft de instelling voor enkele landen bepaald dat zij daar geen activiteiten kan uitvoeren gezien haar beheersingskader. Voor andere landen zijn limieten gezet op het aantal (zakelijke) klanten dat zij wil accepteren uit deze landen. Tegelijkertijd heeft de instelling KRI's gezet op de transactiestromen van en naar deze landen en deze omgezet in concrete business rules voor het transactiemonitoringsysteem, zodat het goed in staat is de geld-stromen van en naar deze landen te monitoren.

### Good practice – Risicobeoordeling van betaaldienstverleners met sub-merchants

Een betaalinstelling heeft vastgesteld dat er betaaldiensten worden verleend aan cliënten met sub-merchants. Om de beheersmaatregelen goed toe te kunnen spitsen besluit de betaalinstelling om bij het vaststellen van een risicoprofiel voor de cliënten met sub-merchants rekening te houden met de risico's van de onderliggende sub-merchants. De risico's van de sub-merchants zouden immers ook het risicoprofiel van de cliënt kunnen beïnvloeden – bijvoorbeeld in een situatie waarin de cliënt met sub-merchants op zichzelf een 'laag risico' zou krijgen, terwijl de sub-merchants van de cliënt 'hoog risico' activiteiten verrichten zoals gokactiviteiten.

## Good practice – Risicobeoordeling van trustkantoor leidt tot afscheid van cliënten

Een trustkantoor heeft vastgesteld dat er in de cliëntenportefeuille doelvennootschappen aanwezig zijn waarbij sprake is van een zelfstandig bevoegde buitendirecteur én geen inzagebevoegdheid van het trustkantoor op de bankrekening van de doelvennootschap.

Het trustkantoor stelt vast dat adequate transactiemonitoring hierdoor niet mogelijk is en er een verhoogde kans bestaat op verschillende integriteitsrisico's zoals witwassen, sanctieontwijking en belastingontduiking – die niet nader te analyseren en dus ook niet te beheersen zijn. Het trustkantoor besluit afscheid te nemen van deze cliënten indien de bevoegdheid tot inzage op de rekening niet binnen een maand is verkregen – de risico's zijn onvoldoende beheersbaar en vallen daarmee buiten de risicotolerantie.

## Good practice – Niet aannemen kandidaat

Een instelling heeft een vacature voor een compliance officer. Een van de sollicitanten voldoet volgens haar CV aan de criteria en wordt uitgenodigd voor een gesprek. Het gesprek verloopt goed en de instelling wil haar aannemen.

De instelling ziet de functie van compliance officer als integriteitsgevoelig. Voor integriteitsgevoelige functies heeft de instelling een procedure vastgesteld, waarbij er eerst een screening plaatsvindt en een beoordeling van de betrouwbaarheid van de kandidaat. Onderdeel van de screening is een diplomacheck.

Uit de diplomacheck komt naar voren dat de sollicitant niet beschikt over het universitaire diploma dat zij had aangegeven op haar CV. De instelling legt dit voor aan de kandidaat, en zij geeft toe dat zij niet beschikt over het diploma. De instelling gaat niet verder met de kandidaat.

# 6 Risicomonitoring en herziening

## Ratio

Door het monitoren van de risico's en van de werking van de beheersmaatregelen stelt een instelling vast of het beheersingskader nog voldoet. Er zijn meerdere redenen voor een instelling om op continue basis de organisatie door te lichten om te bezien bij welke bedrijfsonderdelen er gevaar op integriteitrisico's bestaat, en om waar nodig haar SIRA en haar beheersmaatregelen bij te stellen:

- Een instelling en haar omgeving blijven zich ontwikkelen. Zo kunnen bijvoorbeeld incidenten die zich voordoen, geopolitieke ontwikkelingen, de introductie van een nieuw product of een overname aanleiding zijn om de integriteitsrisicoanalyse te herzien. Dit kan dan uiteraard ook gevolgen hebben voor de beheersmaatregelen.
- Van de geïmplementeerde beheersmaatregelen kan duidelijk worden dat die niet voldoen. Uit bijvoorbeeld incidentmeldingen, klachten of audits kan blijken dat de beheersing op sommige plekken te zwak is, of dat bepaalde lage risico's worden beheerst met meer middelen dan nodig. Ook kan blijken dat er beheersmaatregelen in werking zijn waarvan het bijbehorende risico niet meer actueel is – de instelling kan dan overwegen om deze beheersmaatregelen af te schaffen.

Door risicomonitoring en herziening beschikt de instelling over een actuele en goed toegespitste SIRA, met de daarbij passende beheersmaatregelen. De instelling borgt hiermee de integere uitoefening van het bedrijf en doet daarmee het redelijkerwijs mogelijke om te voorkomen dat zij betrokken raakt bij gebeurtenissen, activiteiten of partijen die de integriteit van de instelling en/of van haar medewerkers aan kunnen tasten.

## Good practices

### Good practice – Gebruik van *feedbackloops*

Een instelling heeft in het kader van de risicomonitoring *feedbackloops* geïmplementeerd. De instelling gebruikt deze *feedbackloops* om na te gaan of integriteitsrisico's wijzigen dan wel of er sprake is van nieuwe integriteitsrisico's of van verschijningsvormen daarvan.

De instelling maakt hierbij onder meer gebruik van inzichten uit:

- rapportages van relevante autoriteiten en organisaties zoals DNB, FATF, AMLC, OESO etc.
- onderzoeken van toezichthouders
- exitgesprekken
- event-driven en periodieke reviews
- FIU-meldingen en feedback vanuit de FIU
- uitkomsten van sectoranalyses van brancheorganisaties
- uitkomsten van compliance monitoring en uitgevoerde audits
- *lessons learned* uit klachten en incidenten.

De instelling voert een analyse uit aan de hand van vragen als: Is hier sprake van een nieuw of gewijzigd risico? Hoe heeft dit kunnen gebeuren? Waarom waren de beheersmaatregelen niet effectief? Hoe voorkomen we een eventueel falen in de toekomst? Op deze wijze vergroot de instelling haar inzicht in hoe risico's zich kunnen manifesteren en in de werking van de beheersmaatregelen.

## Good practice – *Feedbackloop* naar aanleiding van de uitkomst periodieke review

Een accountmanager van een trustkantoor constateert tijdens de periodieke review van een doelvennootschap dat de omzet uit operationele activiteiten van een deelneming van de doelvennootschap fors is gestegen. De deelneming is geografisch gelegen naast een land waarop sancties van kracht zijn.

De accountmanager doet nader onderzoek en vraagt documentatie op bij de doelvennootschap. Op basis van de uitkomsten van dit onderzoek wordt overgegaan tot een procedure van her-acceptatie. Tevens stelt de accountmanager de compliance officer op de hoogte.

De compliance officer voert een bredere analyse uit op de portefeuille om na te gaan of dit scenario ook bij andere doelvennootschappen in de portefeuille voorkomt. Het scenario wordt opgenomen in de SIRA.

## Good practice – *Feedbackloop* naar aanleiding van datalek of schandaal

Een instelling monitort voortdurend externe nieuwsbronnen en media-uitingen voor informatie die relevant kan zijn voor haar risicoanalyse. Wanneer een nieuw groot datalek of financieel schandaal aan het licht komt, analyseert de instelling onmiddellijk de beschikbare gegevens en identificeert potentiële risico's en blootstellingen binnen haar klantenbestand en transactiestromen. Vervolgens worden deze bevindingen gebruikt om bestaande risicomodellen te verfijnen en aan te passen, waardoor de instelling haar preventie- en detectiecapaciteiten voor financiële misdrijven versterkt. Deze benadering stelt de instelling in staat om proactief te reageren op nieuwe informatie en haar risicobeheersingsproces voortdurend te verbeteren.

## Good practice – *Feedbackloop* op basis van een analyse van recente exits

Een betaalinstelling voert regelmatig een diepgaande analyse uit van recente exits, waarbij de redenen voor vertrek van cliënten worden geanalyseerd en geëvalueerd. Door deze analyse kan de betaalinstelling trends en patronen identificeren met betrekking tot risicovolle cliënten en activiteiten.

Op basis van deze inzichten past de instelling haar risicoanalyse aan door nieuwe risicofactoren toe te voegen, herziet zij bestaande risico-modellen en brengt zij verbeteringen aan in haar cliëntmonitoring en due diligence procedures.

Door op deze wijze lessen te trekken uit recente exits die de instelling om Wwft-redenen heeft geïnitieerd, kan de betaalinstelling haar risicobeheersingsprocessen versterken en proactief risico's identificeren en beheersen.

## Good practice – Monitoren geopolitieke ontwikkelingen

Een internationaal opererende verzekeraar houdt nauwlettend zicht op geopolitieke ontwikkelingen en internationale conflicten die van invloed kunnen zijn op haar zakelijke activiteiten. Wanneer een internationaal conflict escaleert en leidt tot het opleggen van sancties, voert de verzekeraar onmiddellijk een risicoanalyse uit om de mogelijke impact op haar activiteiten te evalueren. Dit omvat een grondige beoordeling van haar blootstelling aan risico's die voortvloeien uit de sancties, zoals het zakendoen (of het faciliteren daarvan) met gesanctioneerde personen of entiteiten, en de aantasting van haar reputatie.

Op basis van deze analyse ontwikkelt de verzekeraar een bijgewerkt risicobeheersingsplan dat gericht is op het identificeren, beoordelen en beheersen van nieuwe en opkomende risico's die voortvloeien uit het conflict en de daaropvolgende sancties.

## Good practice – Gebruik van meldingen aan en feedback van de FIU

Een bank gebruikt haar FIU-meldingen en de feedback ten aanzien van deze meldingen vanuit de FIU als input voor haar risicoanalyseproces. Ze analyseert deze informatie om trends, patronen en risicovolle gedragingen te identificeren die mogelijk niet eerder waren opgemerkt in haar eigen monitoringprocessen.

Op basis van deze analyse past de bank haar risicomodellen en transactiemonitoringregels aan om beter in staat te zijn ongebruikelijke en mogelijk verdachte activiteiten te detecteren en te rapporteren aan de FIU. Daarnaast gebruikt de bank de ontvangen feedback om haar medewerkers te trainen en bewust te maken van de nieuwste ontwikkelingen en trends in financiële criminaliteit.

## Good practice – Analyse transacties naar hoogrisicolanden

Een bank constateert een significante toename van transacties vanuit een buurland van een 'sanctieland'. De bank voert een verdiepende analyse uit naar de transacties en betrekt daarbij indicatoren zoals:

- frequentie, omvang en bestemming van de transacties
- relatie tussen de opdrachtgever en de begunstigde
- aard van de transacties
- reguliere activiteiten van de betrokken partijen in relatie tot de waargenomen transacties.

De bank constateert een sterk verhoogde kans op betrokkenheid bij omzeiling van sanctiemaatregelen. Dit valt ver buiten de risico-tolerantie van de bank, en zij neemt dan ook aanvullende, verscherpte beheersmaatregelen.

## Good practice – Rol van Compliance en Audit

Om de effectiviteit van het gehele SIRA-proces en de samenhang met procedures en maatregelen te borgen, beoordelen de compliance- en de auditfunctie van een instelling periodiek de opzet en werking van het beheersingsraamwerk ten aanzien van de integriteitsrisico's. Hierover wordt gerapporteerd aan het bestuur. Op basis hiervan stelt de instelling waar nodig beheersmaatregelen bij.

## Good practice – Betrokkenheid Raad van Bestuur

Een instelling behandelt de resultaten van de recente SIRA met regelmaat in vergaderingen van haar Raad van Bestuur (RvB). Tijdens deze vergaderingen worden de belangrijkste risico's besproken en geëvalueerd, inclusief de potentiële impact ervan op de organisatie. Op basis van deze analyse stelt de RvB prioriteiten vast voor risico-beheersing en bepaalt zij welke gebieden speciale aandacht nodig hebben.

De RvB neemt vervolgens de leiding in het aanscherpen van de mitigerende maatregelen om de geïdentificeerde risico's effectief aan te pakken. Dit kan onder meer inhouden dat er extra middelen worden toegewezen aan risicovolle gebieden, het implementeren van nieuwe controles en procedures, het bijwerken van bestaande richtlijnen en beleid, of het afschaffen van beheersmaatregelen omdat het betreffende risico zich niet meer voordoet.

Daarnaast zorgt de RvB er voor dat er regelmatig opvolging wordt gegeven aan de genomen maatregelen om te evalueren of ze effectief zijn geweest in het verminderen van de risico's. Indien nodig worden aanpassingen gemaakt om de doeltreffendheid van de maatregelen te verbeteren.

# Bijlage  Belangrijkste wijzigingen ten opzichte van de SIRA Good Practices uit 2015

De belangrijkste wijzigingen ten opzichte van de SIRA Good Practices uit 2015 zijn de volgende.

| Onderwerp | Wijziging |
|---|---|
| Weergave cyclus risicomanagement | De cyclus van integriteitsrisicomanagement is minder gedetailleerd weergegeven door deze te beperken tot de 4 hoofdstappen. Dit vloeit voort uit de wens om minder voorschrijvend te formuleren. |
| Ratio | Per onderdeel van de cyclus van integriteitsrisicomanagement wordt aangegeven wat de ratio is van het nemen van de betreffende stap. Dit maakt tegelijkertijd duidelijk dat het niet primair gaat om het uitvoeren van bepaalde stappen in een bepaalde volgorde, maar veel meer om de uitkomst van het proces: een goede SIRA als basis voor passende beheersmaatregelen. |
| Voorbeelden van integriteitsrisico's | De lijst met voorbeelden van integriteitsrisico's is niet meer opgenomen. Deze lijst was bedoeld om voorbeelden te bieden die instellingen konden helpen om zich te oriënteren op voor hen mogelijk relevante risico's. In de praktijk zien we dat instellingen in veel gevallen de lijst als voorschrift hanteren. In veel SIRA's wordt dan de lijst met voorbeelden tot uitgangspunt van de analyse genomen. |
| Poster integriteitrisicoanalyse | De poster is vervallen. In de praktijk wordt deze door veel instellingen als de door DNB voorgeschreven methode van analyse beschouwd. De poster was echter bedoeld als een overzicht om richting te geven. |

| Onderwerp | Wijziging |
| --- | --- |
| Risico-identificatie en risicoanalyse | De stap 'risico-identificatie' omvatte het ontwikkelen van een organisatieschets, het bepalen van scenario's en van de scoresystematiek voor kans en impact.<br><br>In deze nieuwe uiting wordt bij de stap van risico-identificatie de nadruk gelegd op het organisatierisicoprofiel en op identificatie van factoren die relevant kunnen zijn in het kader van integriteitrisico's.<br><br>In de stap risicoanalyse ligt de nadruk op het concretiseren van de risico's. De benadering uit de uiting van 2015, waarbij het bepalen van kans en impact bij het optreden van scenario's belangrijk was, is genuanceerd. Onder de SIRA Good Practices uit 2015 zagen we dat instellingen het bepalen van kans en impact als een verplichte stap beschouwden, en daarbij een mathematische precisie toepasten die minder goed past bij de kwalitatieve aard van veel integriteitsrisico's. Het nadenken over kans en impact kan een goed hulpmiddel zijn in de analysefase, maar er zijn meer goede manieren denkbaar die de analyse kunnen ondersteunen.<br><br>Het is goed om te realiseren dat risico-identificatie en risicoanalyse wel te onderscheiden zijn, maar niet goed te scheiden. De fasen kunnen volgtijdelijk maar vaak ook tegelijkertijd worden doorlopen. Daarbij kan een instelling bijvoorbeeld het standpunt innemen dat het concretiseren van risico's beter bij risico-identificatie dan bij risicoanalyse past. Voor DNB is die kwalificatie van ondergeschikt belang. |
| Gebruik scenario's | Bij het gebruik van scenario's is meer de nadruk gelegd op het belang van de concrete uitwerking van scenario's toegespitst op de instelling. Dit stelt de instelling beter in staat om specifiek op haar toegespitste, effectieve beheersmaatregelen te definiëren. |
| Gebruik van data-analyse | Het gebruik van data-analyse kan van toegevoegde waarde zijn bij het opstellen van een SIRA. Hier wordt meer aandacht aan besteed. |

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

**Volg ons op:**
LinkedIn
Twitter
Instagram

DeNederlandscheBank
EUROSYSTEEM