De integriteit-risicoanalyse

Meer waar dat moet, minder waar dat kan

DeNederlandscheBank
EUROSYSTEEM

De integriteitrisicoanalyse

Meer waar dat moet, minder waar dat kan

Een gebruikersgids en een poster

Samenvatting

In dit document kunt u lezen welke stappen uw instelling[1] moet nemen om een gedegen integriteitrisicoanalyse op te stellen. Een integriteitrisicoanalyse is niet alleen een wettelijke verplichting. Zonder deze risicoanalyse kan een instelling de integriteitwetgeving niet risicogebaseerd naleven. Daarnaast is de integriteitrisicoanalyse een voorwaarde voor een toereikende inrichting van de integere bedrijfsvoering. Het is niet duidelijk waarop de risicobeheersing is gericht als een instelling onvoldoende kennis heeft van de mogelijke integriteitrisico's, dan wel ongegronde aannames op dat gebied maakt.

In dit document staat beschreven waarom uw instelling een integriteitrisicoanalyse moet maken, hoe u dat kunt doen en welke gevolgen u aan de risicoanalyse moet verbinden. In het midden van dit document zit ook een poster waarop een overzicht staat van de afzonderlijke stappen en de vragen die u uzelf stelt bij het opstellen van de analyse.

Allereerst dient u goed in beeld te krijgen waar uw instelling integriteitrisico's kan lopen. Bekijk hiervoor uw gehele organisatie. U identificeert per integriteitrisico de factoren die een rol spelen en de mogelijke scenario's en scoort deze op kans en impact. Nadat u de aard en omvang van deze brutorisico's heeft bepaald, bekijkt u of deze binnen uw risk appetite vallen.

Vervolgens beoordeelt u per brutorisico welke beheersingsmaatregelen u heeft getroffen en of deze maatregelen effectief zijn. Aan de hand van de brutorisico's en de beoordeling van de beheersing, komt u tot een overzicht van nettorisico's. Ook hier bepaalt u of de nettorisico's binnen uw risk appetite vallen. Indien risico's hier niet binnen vallen, beslist u hoe u deze risico's kunt vermijden of verminderen. Als uit de risicoanalyse blijkt dat verbetering in de beheersing nodig is, geeft u dat ook aan in een overzicht. Samen met een planning van voorgestelde acties.

Uiteindelijk dient de integriteitrisicoanalyse voor het bestuur als sturingsdocument en voor de business als duidelijk overzicht van risico's.

1 Met instelling bedoelen we een bank, verzekeraar, betaalinstelling, wisselinstelling, trustkantoor of pensioenfonds.

Inhoudsopgave

Inleiding

Weet u waar u integriteitrisico's loopt?

De krantenkoppen laten steeds vaker zien welke grote impact integriteitincidenten hebben op ondernemingen. Integriteitrisico's zijn groter dan vroeger. Ze hebben niet alleen grote gevolgen voor uw reputatie, maar steeds vaker zijn ook de financiële gevolgen zeer ingrijpend. U kunt slachtoffer worden van financieel-economische criminaliteit, maar u kunt er (onbedoeld) ook aan meewerken. Ook u kunt dus ter verantwoording worden geroepen door DNB, andere toezichthouders of opsporingsautoriteiten: steeds vaker zien we bestuurders of medewerkers van financiële ondernemingen in het beklaagdenbankje.

Financiële ondernemingen en pensioenfondsen hebben een belangrijke maatschappelijke verantwoordelijkheid als poortwachter van een integere en schone financiële sector. Zij bestrijden criminaliteit door de systemen en dienstverlening voor criminelen zo ontoegankelijk mogelijk te maken en samen te werken met opsporingsinstanties.

Maar wat weet u eigenlijk van integriteitrisico's? Waar kunnen deze ontstaan binnen uw bank, verzekeraar, betaalinstelling, wisselinstelling, trustkantoor of pensioenfonds en hoe dan? En als u de oorzaak kent, kent u dan de aard en de omvang van de risico's? En heeft u er voldoende aan gedaan om deze risico's te beheersen of (beter nog) te voorkomen? Kortom, een integere bedrijfsvoering begint bij een permanent goed beeld van – de aard en omvang van – de risico's die u loopt als u (onbedoeld) financieel-economische criminaliteit begaat of faciliteert. Uit de beoordeling van ruim 170 integriteitrisicoanalyses heeft DNB vastgesteld dat meer dan 80% van de analyses niet voldoet en dat er vele instellingen zijn die niet over een integriteitrisicoanalyse beschikken. DNB vindt het zeer zorgelijk dat dit cruciale onderdeel bij zo veel instellingen niet op orde is en heeft daarom besloten deze good practices te publiceren.

Om te borgen dat instellingen een integere bedrijfsvoering hebben, heeft de wetgever in financiële wetgeving allerlei verplichtingen opgenomen waaraan uw instelling moet voldoen. Daarin speelt een systematische inventarisatie en analyse van integriteitrisico's, een systematische integriteitrisicoanalyse, een centrale rol.

Wettelijk kader

Een bank, verzekeraar, betaalinstelling, elektronischgeldinstelling, wisselinstelling of bijkantoor draagt op grond van artikel 10 Besluit prudentiële regels Wft zorg voor een systematische analyse van integriteitrisico's. Integriteitrisico's zijn daarbij gedefinieerd als het 'gevaar voor aantasting van de reputatie of bestaande of toekomstige bedreiging van vermogen of resultaat van een financiële onderneming als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is voorgeschreven'.

Een trustkantoor maakt op grond van artikel 4 Regeling integere bedrijfsvoering Wtt 2014 periodiek een analyse van de risico's ten aanzien van de integere bedrijfsvoering. De integere bedrijfsvoering is een sturing van de organisatie en de inrichting van de processen die integriteitrisico's beheersen. Integriteitrisico's zijn het risico van ontoereikende naleving van dat wat bij wettelijk voorschrift is bepaald als ook het risico van betrokkenheid van het trustkantoor of haar medewerkers bij handelingen die zo ingaan tegen dat wat 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.

Een pensioenfonds draagt op grond van artikel 19 Besluit financieel toetsingskader pensioenfondsen zorg voor een systematische analyse van integriteitrisico's. Op grond van artikel 14 Besluit uitvoering Pensioenwet maakt een fonds een systematische analyse van de risico's die samenhangen met de uitbesteding van werkzaamheden op het niveau van de gehele organisatie en op het niveau van de bedrijfsonderdelen.

Een onterecht vertrouwen in procedures en maatregelen

Veel instellingen hebben vuistdikke procedureboeken en maatregelen in stelling gebracht om integer handelen door en binnen de instelling te waarborgen. De wet eist ook tal van procedures en maatregelen, waarmee de illusie van beheersing kan ontstaan. Procedures geven u namelijk alleen de schijn van risicobeheersing, vooral als u ze niet baseert op en richt tegen daadwerkelijke risico's. Alleen door de risico's naar hun aard en verschijningsvorm goed te begrijpen, kunt u procedures en maatregelen effectief in stelling brengen. Zonder goed begrip van de aard en omvang van het risico bestaat bij het naleven van de procedures het gevaar op 'afvinkgedrag'. Naleving zonder overtuiging of begrip is een risico op zich. Mede daarom is veel van de regelgeving risk based: de wettelijk voorgeschreven procedures moeten worden opgevolgd, maar de wijze en intensiteit ervan is afhankelijk van de omvang van het risico. In sommige gevallen biedt u dat dus ook de mogelijkheid om procedures te beperken en kostenvoordeel te halen. In andere gevallen moeten echter verscherpte maatregelen worden getroffen.

Voorbeelden waar minder kan en waar meer moet

Soorten klanten of diensten met een potentieel lager risico

- Beursgenoteerde vennootschappen die onderworpen zijn aan bepaalde transparantievereisten
- Overheden of overheidsbedrijven
- Levensverzekeringspolissen met een lage premie
- Pensioenverzekeringsovereenkomsten die geen afkoopclausule bevatten en niet als zekerheidstelling kunnen dienen
- Financiële producten of diensten om financiële inclusie te vergroten
- Producten met lage bestedingslimieten (bijvoorbeeld bepaalde soorten elektronisch geld)

Soorten klanten of diensten met een potentieel hoger risico

- Bedrijven waar veel geldverkeer in contanten plaatsvindt
- Rechtspersonen of juridische constructies die vehikels zijn voor het aanhouden van persoonlijke activa
- Private banking
- Producten of transacties die anonimiteit bevorderen
- Zakelijke relaties op afstand of transacties op afstand
- Betalingen die worden ontvangen van onbekende of niet-verbonden derden
- Nieuwe producten en nieuwe zakelijke praktijken, zoals nieuwe leverings-mechanismen
- Het gebruik van nieuwe of in ontwikkeling zijnde technologieën voor zowel nieuwe als bestaande producten

Wat bedoelen we eigenlijk met een systematische inventarisatie en analyse?

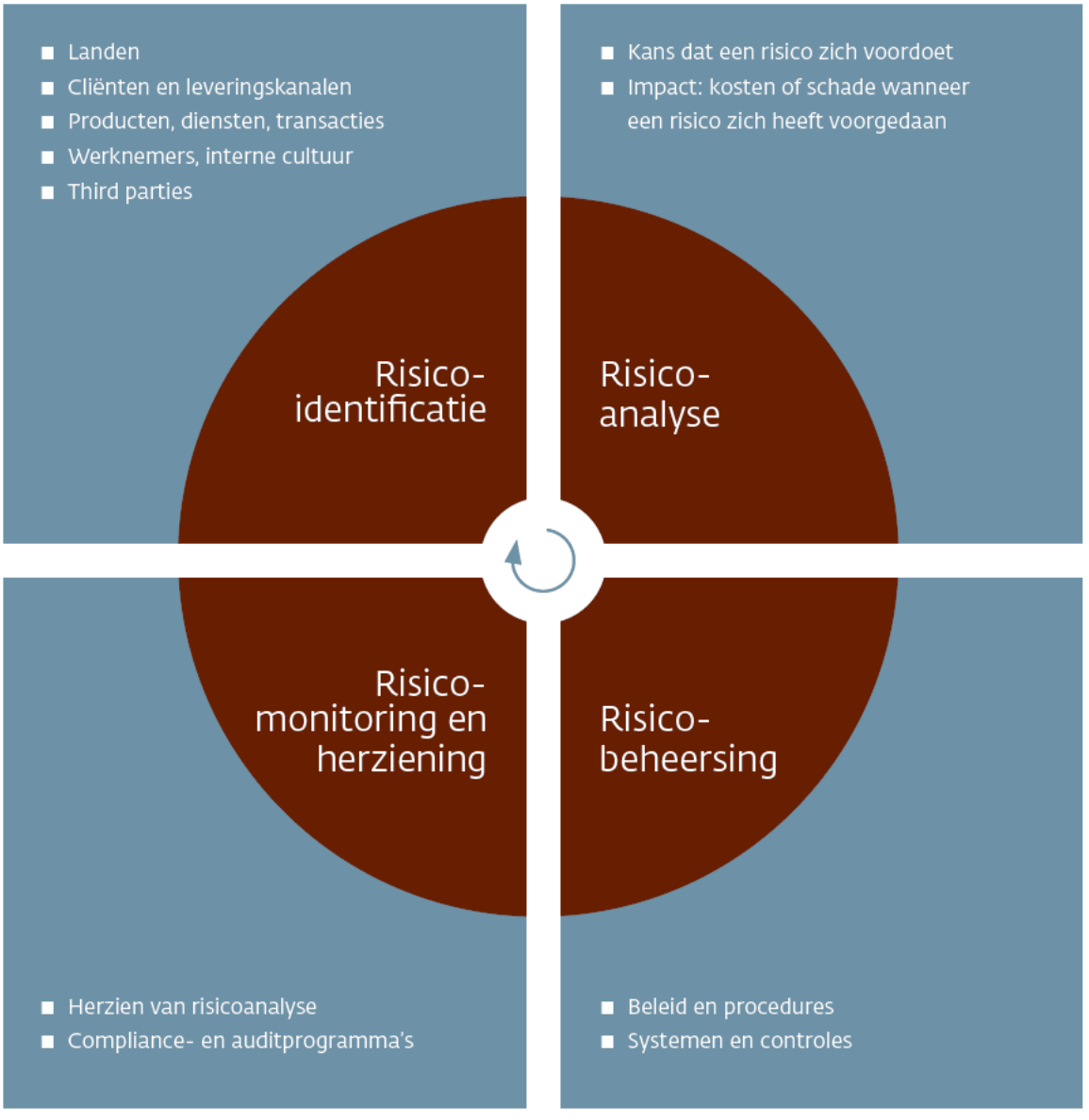
'Bezint eer ge begint' is het credo. Voordat u maatregelen en procedures invoert of herziet, moet u eerst gedegen onderzoek doen naar de aard (verschijningsvormen, scenario's van financieel-economische criminaliteit) en omvang van de risico's. Dit proces kent twee fasen:

1. Identificeer de mogelijke risico's
2. Analyseer en bepaal de aard en omvang van de risico's

Daarna komt het op maat inrichten van het beheersingskader: het beleid, de maatregelen en de procedures.

De wet en de toezichthouder verlangen een systematische benadering van deze manier van risicobeheersing. En systematisch houdt ook in dat het een cyclisch proces is: dat betekent dat u de inventarisatie, analyse en de (toetsing van de effectiviteit van de) beheersing periodiek moet 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 uw instelling uitgebreid of veranderd worden, kunnen zich bepaalde trends voordoen binnen het financieel-economische verkeer, of kan wet- en regelgeving aangepast worden. In dit document vindt u voorbeelden en handvatten voor de risico-identificatie- en risicoanalysefase: van de voorbereidingen tot aan het beslissen over te nemen beheersingsmaatregelen.

Identificatie en analyse zijn systematisch, doordat u ze enerzijds periodiek uitvoert (en bij tussentijdse triggerevents) en anderzijds doordat het een cyclisch geheel is van identificatie gevolgd door analyse en beheersing. De uitkomst van dit proces is het nettorisico; de omvang van het risico dat overblijft als alle procedures en maatregelen adequaat hun werk doen. De vraag is in hoeverre dit nettorisico voor u acceptabel is en past binnen uw risk appetite.


Landen
Cliënten en leveringskanalen
Producten, diensten, transacties
Werknemers, interne cultuur
Third parties
Risico-identificatie
Kans dat een risico zich voordoet
Impact: kosten of schade wanneer een risico zich heeft voorgedaan
Risico-analyse
Risico-beheersing
Beleid en procedures
Systemen en controles
Risico-monitoring en herziening
Herzien van risicoanalyse
Compliance- en auditprogramma's

De integriteitrisicoanalyse: verplicht maar vooral nuttig

De systematische integriteitrisicoanalyse levert u belangrijke rapportages op voor diverse afdelingen binnen uw organisatie. Allereerst leggen deze rapportages de basis voor uw (periodiek te herziene) integriteitbeleid. De output van de risicoanalyse is in de eerste plaats een sturingsdocument voor het management. De organisatie wordt in actie gezet om passende maatregelen te nemen om de risico's daadwerkelijk te gaan beheersen. Voor Compliance en Audit speelt de output ook een belangrijke rol. Zij zetten de analyses in bij hun gapanalyses en bij het opstellen van jaarplannen en controleonderzoeken. Compliance en andere tweedelijnsfuncties spelen verder een belangrijke adviserende rol bij het formuleren van het integriteitbeleid. Aangezien communicatie en opleiding sleutelprocessen zijn bij risicobeheersing, zullen de afdelingen die hier verantwoordelijk voor zijn op zijn minst ook kennis moeten nemen van de uitkomsten van de risicoanalyses. De rapportages zijn ten slotte van dusdanig wezenlijk belang dat ook toezichthoudende organen (Raad van Commissarissen, Raad van Toezicht) binnen de instelling dienen te worden geïnformeerd.

De EU anti-witwasrichtlijn

Ook de EU anti-witwasrichtlijn geeft aan dat een risicoanalyse essentieel is. In Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering heeft de EU bepaald dat een integrale op risicogebaseerde benadering moet worden gebruikt. Dit omdat witwasrisico's en risico's van terrorismefinanciering van geval tot geval kunnen variëren. Deze op risicogebaseerde benadering is geen vrijblijvende optie, maar moet gepaard gaan met het gebruik van empirisch onderbouwde besluitvorming. Het witwasrisico en het risico van terrorismefinanciering waarmee instellingen geconfronteerd worden, wordt zo efficiënter aangepakt.

Artikel 8 van de Richtlijn stelt dat instellingen verschillende stappen moeten ondernemen om hun witwasrisico en risico van terrorismefinanciering te identificeren en te beoordelen. Hierbij moeten ze rekening houden met risicofactoren die verband houden met hun cliënten, landen of geografische gebieden, producten, diensten, transacties en leveringskanalen. Deze stappen zijn evenredig met de aard en omvang van de instelling. De risicobeoordelingen worden gedocumenteerd, actueel gehouden en beschikbaar gesteld aan de toezichthouders.

In de bijlagen bij deze Richtlijn staan niet-limitatieve lijsten van factoren en soorten bewijs van potentieel hoger en lager risico.

Handvatten bij een integriteitrisicoanalyse

Wie maakt een integriteitrisicoanalyse?

Het is een misvatting dat de systematische integriteitrisicoanalyse vooral een onderwerp van Compliance is. Management, Compliance, Risk Management en de business werken samen aan de uitvoering van de integriteitrisicoanalyse. De verantwoordelijkheid voor de kwaliteit en de uitvoering hoort in eerste instantie bij de eerste lijn te liggen, de business. Daar manifesteren de risico's zich als eerste. De rol van Compliance is er een van procesbewaking, faciliteren en toetsen. Ook andere afdelingen, zoals Veiligheidszaken of Audit, kunnen de nodige input leveren. De uiteindelijke verantwoordelijkheid voor de integriteitrisicoanalyse ligt bij de bestuurders.

Veel instellingen laten zich bijstaan door externe deskundigen op het gebied van integriteit, fraude, financieel-economische criminaliteit of risicobeheersing. Maar uiteindelijk moet de inventarisatie en analyse volledig eigenaarschap, inclusief besluitvorming, hebben van de eerst-verantwoordelijke voor de analyse. Deze verantwoordelijkheid is meestal belegd bij de business of Risk Management. Pensioenfondsen laten hun risicoanalyse vaak uitvoeren door het bedrijfsbureau of zelfs de pensioenuitvoerder. De verantwoordelijkheid ligt bij het bestuur en dus zal dit zeker een initiërende en actieve rol moeten spelen. Dat dit ook het meest logisch is, volgt uit het feit dat de procedures en maatregelen vooral door de eerste lijn moeten worden uitgevoerd.

Good practice van een proces bij een instelling

Een instelling vormt per bedrijfsonderdeel werkgroepen. In deze werkgroepen bespreken medewerkers de kans dat integriteitrisico's omtrent bijvoorbeeld witwassen of corruptie zich kunnen voordoen. De werkgroepen beoordelen onder andere de kans dat een klant door middel van bepaalde witwas-scenario's geld via de instelling kan witwassen, de kans dat door relaties tussen medewerkers en klanten belangenverstrengeling kan ontstaan, of door het gebruik van bepaalde producten of activiteiten in bepaalde landen internationale sancties kunnen worden omzeild. Deze sessies worden begeleid door Compliance.

Aan de hand van een vooraf opgesteld scoremodel beoordeelt Compliance vervolgens samen met Risk Management wat de impact zou zijn op de instelling als een scenario zich zou voordoen. De sessies leiden tot een matrix van kans en impact van brutorisico's. Vervolgens beoordeelt Compliance samen met Audit wat het niveau van beheersing is omtrent de verschillende scenario's. De matrix van de brutorisico's en de beheersingsmaatregelen levert vervolgens een overzicht op van nettorisico's en hiaten in de beheersing.

Met het bestuur wordt dit alles uitgebreid besproken en bekeken of de bruto- en nettorisico's binnen de risk appetite vallen. Het bestuur beslist vervolgens of risico's moeten worden afgebouwd of vermeden en welke verdere maatregelen worden getroffen.

Om welke integriteitrisico's gaat het?

Het gaat om niet-integer gedrag van (medewerkers en/of bestuurders van) de instelling en om niet-integer gedrag van derden (klanten, leveranciers, adviseurs) dat aan de instelling kan worden toegerekend of waarbij de instelling een strafbare rol speelt. Het meest in het oog springend zijn de gedragingen die vallen binnen de grenzen van delictsomschrijvingen in het Wetboek van Strafrecht of de economische ordeningswetten: witwassen is een van de bekendere integriteitrisico's. Minder bekend zijn de witwasvarianten, zoals schuldwitwassen. Maar ook handel met voorkennis, terrorismefinanciering, het omzeilen van economische en financiële sancties, fraude, oplichting, verduistering, valsheid in geschrifte, ambtelijke of niet-ambtelijke omkoping en schijn van belangenverstrengeling. Het zijn slechts enkele voorbeelden. Integriteitrisico's kunnen ook betrekking hebben op het overtreden van of handelen in strijd met interne regels van de organisatie.

Ook het overtreden van internationale regelgeving behoort tot de integriteitrisico's. Bekend zijn bijvoorbeeld de extraterritoriale werking van de Amerikaanse sanctie- en anti-corruptiewetgeving en de Engelse anti-corruptiewetgeving.

Voorbeelden van integriteitrisico's

- Witwassen
- Terrorismefinanciering
- Omzeiling sanctieregelgeving
- Corruptie (omkoping)
- Belangenverstrengeling
- Interne en externe fraude
- Ontduiking of ontwijking van fiscale regelgeving
- Marktmanipulatie
- Cybercrime
- Maatschappelijk onbetamelijk gedrag

Poster integriteitrisicoanalyse

Deze poster geeft in een oogopslag een overzicht van de afzonderlijke stappen die uw instelling neemt om een integriteitrisicoanalyse te maken. Het geeft de stappen weer om de brutorisico's per integriteitrisico in kaart te brengen en te analyseren op kans en impact, om de effectiviteit van de beheersing te beoordelen, en om nettorisico's en hiaten in de beheersingsmaatregelen te bepalen. Bij deze stappen staan de vragen die u uzelf stelt bij het opstellen van de integriteitrisicoanalyse. Deze poster is een overzicht om richting te geven; het is niet de bedoeling dit als standaardformat te gebruiken.

Integriteitrisicoanalyse

Stap 1:
de voorbereiding en risico-identificatie

- Organisatieschets: maak per bedrijfsonderdeel/ bijkantoor/dochter een inventarisatie van de organisatie voor wat betreft producten, klanten, landen, werknemers, derde partijen, et cetera.
- Scenario's: bekijk welke integriteitrisico's zich kunnen voordoen en op welke wijze deze zich kunnen voordoen.
- Scoringssystematiek: bepaal op welke manier kans en impact beoordeeld zullen worden.

Stap 2:
de analyse

- Brutorisico's: bepaal per scenario wat de kans en impact is dat het betreffende scenario zich voordoet.
- Risk appetite: beoordeel wat het brutorisico is en of dat binnen de risk appetite valt.
- Beheersing: benoem en beoordeel per scenario de beheersingsmaatregelen die er tegenover staan.

Identificatie			Analyse			
Risico	Factor	Scenario	Kans	Impact	Brutorisico	Risk app
(Met welke integriteitrisico's kan de instelling te maken krijgen?)	(Welke factoren, zoals klanten, landen, werknemers, spelen een rol per risico?)	(Op welke manieren kan het risico zich materialiseren?)	(Wat is de mogelijkheid dat een scenario zich voordoet?)	(Wat zijn de gevolgen als een scenario zich voordoet?)	(Door de beoordeling van kans en impact wordt het inherente risico vastgesteld.)	(Past het inherent risico bin risk appe
Witwassen						
Fiscale fraude						
Corruptie (omkoping)						
Omzeiling sancties						
Terrorisme-financiering						
Belangen-verstrengeling						
Interne fraude						
Externe fraude						
Cybercrime						
Maatschappelijk onbetamelijk gedrag						

Stap 3:
beslissing over te nemen maatregelen

- Nettorisico's: bepaal het nettorisico per scenario door brutorisico en beheersing te vergelijken.
- Risk appetite: beoordeel of het nettorisico binnen de risk appetite valt.
- Maatregelen: bepaal wat de actie moet zijn, meer beheersing of risico verminderen.

			Beoordeling			
etite	Beheersings-maatregelen	Beoordeling beheersing	Nettorisico	Risk appetite	Gap	Te nemen maatregel
e, bruto-nen de tite?)	(Wat zijn de beheersings-maatregelen die tegenover een scenario staan?)	(Wat is de effectiviteit van de beheersings-maatregelen?)	(Door de beoordeling van brutorisico en beheersing wordt het nettorisico vastgesteld.)	(Past het nettorisico binnen de risk appetite?)	(Wat zijn tekort-komingen in de maatregelen?)	(Welke maatregelen moeten genomen worden om het risico te beheersen of te vermijden?)

Hoe maakt u een integriteitrisicoanalyse?

Stap 1: de voorbereiding en de risico-identificatie

Om een integriteitrisicoanalyse voor te bereiden, neemt u eerst een aantal voorbereidende stappen. Zo stelt u een organisatieschets op, maakt u een overzicht van mogelijke scenario's per integriteitrisico en bepaalt u hoe kans en impact worden beoordeeld. De voorbeelden die DNB hier geeft, zijn algemeen en vertaalt u zelf naar de context van uw eigen organisatie.

Organisatieschets – inventarisatie

Om de integriteitrisicoanalyse te maken, moet u een goed beeld hebben van uw organisatie. Dit betekent dat u een analyse maakt van verschillende aspecten van uw instelling waar integriteitrisico's zich kunnen voordoen. Deze inventarisatie bevat een actuele beschrijving van de aard en omvang van het bedrijf en op welke markten de instelling zich begeeft. Grotere instellingen maken een dergelijke organisatieschets voor de diverse bedrijfsonderdelen en business lines. Ook de dochters en bijkantoren stellen een schets op van hun onderdeel.

Per integriteitrisico zijn verschillende factoren belangrijk. Zo maakt u voor het risico witwassen een analyse van aantal en soort klanten, producten die de klanten afnemen, landen waar de klanten zaken doen of transacties uit ontvangen of naar betalen. Voor de risicoanalyse met betrekking tot het niet naleven van sancties is het naast een analyse van klanten en landen ook relevant om een goed beeld te hebben van het soort goederen waarin de klanten handelen. Voor een risico als corruptie of belangenverstrengeling zult u kennis moeten hebben van bijvoorbeeld het aantal werknemers dat betrokken is bij de inhuur van derde partijen en het aantal en soort sponsoringcontracten.

Door de organisatieschets heeft uw instelling een goed beeld van alle factoren waardoor uw instelling blootgesteld wordt aan risico's.

Good practice

Een instelling maakt voor bijvoorbeeld de witwasrisicoanalyse per bedrijfsonderdeel een cijfermatig overzicht van klanten, producten en leveringskanalen.

- Bij klanten wordt een analyse gemaakt van de maturiteit van het klantenbestand, de complexiteit van klantenstructuren, aantallen politically-exposed persons (PEP's), overzicht van vermogen en de verdeling van klanten over de risicocategorieën.
- Bij landen bepaalt de instelling het aantal transacties naar en vanuit hoogrisicolanden, het aantal klanten in hoogrisicolanden en de landen waar klanten activiteiten ondernemen.
- Bij producten en transacties brengt de instelling per afdeling de productgroepen en soorten producten in kaart. Daarbij wordt aangegeven of het een laag-, medium- of hoogrisico product is. Verder wordt een overzicht gemaakt van het aantal klanten met hoogrisicoproducten en het aantal contante transacties.
- Bij leveringskanalen worden aantallen of percentages in kaart gebracht van klanten die via het directe kanaal, via een accountmanager worden bediend en die voornamelijk via online kanalen zakendoen met de instelling.

Scenario's – verschijningsvormen

Elke instelling moet weten hoe een integriteitrisico zich kan manifesteren. Oftewel verschillende verschijningsvormen van financieel-economische criminaliteit. U blijft hiervoor voortdurend op de hoogte van nieuwe vormen van witwassen, manieren om sancties te omzeilen, nieuwe fraudevormen en corruptiemogelijkheden.

Het gaat om inherente risico's of brutorisico's. Ofwel de risico's die bestaan als er geen enkele beheersingsmaatregel tegenover zou zijn gesteld. Het is een inventarisatie van de dreigingen die op de organisatie afkomen.

Het is hierbij belangrijk dat u als instelling op de hoogte blijft van publicaties van onder andere de Financial Action Task Force, de Europese Unie, het Internationaal Monetair Fonds, de Wereldbank, Transparency International, nationale en internationale toezichthouders, de Financial Intelligence Unit, en consultancy-organisaties.

Good practice

Per integriteitrisico beschrijft een instelling meerdere relevante scenario's. Daarin geeft de instelling aan op welke wijze zich risico's kunnen voordoen via factoren als klanten, medewerkers, derden, producten, diensten of landen.

Fiscale risico's	■ Klanten maken gebruik van complexe, ondoorzichtige constructies ■ Medewerker adviseert over mogelijkheden tot fiscale ontduiking ■ Klanten zijn gevestigd in intransparante jurisdicties
Witwassen	■ De herkomst van vermogen van klanten is onduidelijk ■ Klanten zitten in een cash-intensieve sector ■ Prepaidkaarten kunnen opgeladen worden met een hoog bedrag ■ Het beloningsbeleid werkt ongewenst klantacceptatie in de hand ■ Gelden van/naar een politically-exposed person (PEP) uit een hoogrisicoland ■ Uitkering van verzekeringen bij afkoop gaan naar ander dan verzekeringnemer ■ Uitkering van verzekeringen gaan naar sanctie- of hoogrisicolanden
Corruptie / belangen-verstrengeling	■ Medewerkers en klanten/derde partijen/inhuur hebben persoonlijke relaties ■ Een kleine groep medewerkers werkt op een specialistisch gebied ■ De interne cultuur van de instelling laat niet toe dat men elkaar aanspreekt ■ De cultuur van buitenlandse kantoren versterkt mogelijkheden tot belangenverstrengeling ■ Klanten zijn actief in vastgoed/infrastructuur/grondstoffen/energie sectoren ■ Klanten of instelling zijn actief in politiek instabiele gebieden
Sanctie omzeiling	■ Klanten doen veel zaken met sanctielanden ■ Klanten zijn actief in handel in goederen die onder embargo's vallen ■ Instelling faciliteert handelsfinanciering met partijen in sanctielanden ■ De instelling is zelf actief in sanctielanden
Interne fraude	■ Er is geen periodieke interne screening ■ Er is geen vierogencontrole ■ Procedures zijn niet duidelijk

Scoringssystematiek

De scenario's die u per integriteitrisico heeft benoemd, scoort u vervolgens op kans en impact. Kans en impact drukt u het beste uit in een waarde, bijvoorbeeld een getal. U beoordeelt hoe groot de kans is dat een specifiek scenario zich bij uw organisatie zal voordoen en welke gevolgen dat dan zal hebben. Een kwantificatie of kwalificatie van risico's maakt onderling vergelijk mogelijk. Ook kunt u hiermee een toe- of afname van het risico door de tijd heen zichtbaar maken.

Bij het scoren van kans moet u denken aan het aantal keer per jaar dat iets voorkomt, de frequentie. Voor de beoordeling van de kans dat een bepaald risico optreedt, kijkt u of het risico zich al eens eerder heeft voorgedaan en of er zich relevante incidenten hebben voorgedaan. Of u maakt een inschatting hoe vaak het scenario kan voorkomen.

Bij impact gaat het om een negatieve beïnvloeding van het voortbestaan van de onderneming. Maar bijvoorbeeld ook om de omvang, als het risico zich al eens eerder heeft voorgedaan. De impact kan worden beschreven in termen van 'verlies van vertrouwen', 'verlies van omzet' en 'beschadiging van de reputatie'. Maar ook in ruimere zin als 'verlies van vertrouwen in het financiële stelsel', de 'reputatie van de financiële sector', de 'reputatie van Nederland', de 'internationale reputatie' en 'schade aan het vestigingsklimaat'. Uw instelling zal een waarde aan dit soort factoren moeten toekennen. Bij het scoren van impact moet u ook denken aan het kwantificeren van schade aan de reputatie van de instelling of aan kosten die de instelling zal maken vanwege maatregelen van de toezichthouder.

Verschillende voorbeelden van beoordeling kans en impact

Kans	Niet waarschijnlijk: het scenario komt minder dan 1 keer per jaar voor Mogelijk: het scenario kan 1 keer per jaar voorkomen Waarschijnlijk: het scenario komt mogelijk een aantal keren in een jaar voor	1 het scenario komt 1 keer per 5 jaar voor 2 het scenario komt 1 keer per jaar voor 3 het scenario komt 2-3 keer per jaar voor 4 het scenario komt meer dan 4 keer per jaar voor	Laag: het is onwaarschijnlijk dat het scenario voorkomt Medium: er is enige kans dat het scenario zich voordoet Hoog: er is een redelijke kans dat het scenario voorkomt
Impact	Laag: nauwelijks financiële of reputatieschade; geen maatregel van toezichthouder Medium: beperkte financiële of reputatieschade; enkelvoudige maatregel van toezichthouder Hoog: hoge financiële of reputatieschade; zware of meerdere maatregelen van toezichthouder	Financieel verlies (boete, rechtszaak, et cetera) en indirect verlies (kosten, et cetera) 1 < EUR 9.999 2 > EUR 10.000 en < EUR 100.000 3 > EUR 100.000 en < EUR 1.000.000 4 ≥ EUR 1.000.000	Reputatieverlies 1 nauwelijks verlies van vertrouwen, geen impact op bedrijfsvoering 2 verlies van vertrouwen of klachten van klanten, kortetermijnimpact op bedrijfsvoering 3 mediumtermijnimpact op klanten en bedrijfsvoering 4 langetermijnimpact op klanten en bedrijfsvoering

Stap 2: de risicoanalyse

In de analysestap beoordeelt u de brutorisico's en de beheersingsmaatregelen die daar tegenover staan. De output is een overzicht van de nettorisico's: de risico's die 'overblijven'.

Analyse van brutorisico's per scenario

Nadat u voor uw instelling mogelijke scenario's heeft opgesteld en heeft bepaald hoe de kans en impact van die scenario's worden gescoord, worden de scenario's daadwerkelijk geanalyseerd. U kunt hiervoor bijvoorbeeld via een self assessment de eerste lijn de verschillende scenario's laten scoren door aan te geven hoe groot de kans is dat de beschreven situatie zich voordoet. Ook kan dit worden gedaan via interviews of in werkgroepen binnen de instelling of afdeling.

Een goede analyse laat medewerkers nadenken of er ook andere scenario's denkbaar zijn, en of er zich in het verleden andere situaties hebben voorgedaan. Het is de taak van Compliance om de antwoorden van de eerstelijnsmedewerkers te challengen. Compliance bepaalt ook wat de impact kan zijn.

De kans en impact vormen samen het brutorisico. Per scenario moet u bekijken of deze brutorisico's binnen de risk appetite vallen. In de risk appetite geven het senior management en het bestuur de instelling een kader van het type en niveau van het risico dat ze bereid zijn te accepteren. In de risk appetite bepaalt het bestuur expliciet de grenzen waarbinnen de medewerkers worden verwacht te werken bij het nastreven van de strategie van de instelling. Zo geeft de risk appetite bijvoorbeeld aan bij welke tekortkomingen of overtredingen een instelling wel of niet betrokken wil zijn.

Bij brutorisico's die buiten de risk appetite vallen, moet een instelling ook overwegen om de betreffende dienstverlening niet meer te verlenen of het soort klanten niet meer te bedienen.


kans
X
impact
=
bruto-
risico

Voorbeelden van kans- en impactanalyse

Brutorisico's		Impact 4	3	2	1
Kans	4	Extreem	Extreem	Hoog	Hoog
	3	Extreem	Hoog	Hoog	Matig
	2	Extreem	Hoog	Matig	Laag
	1	Extreem	Matig	Laag	Laag

Brutorisico	Omschrijving	Actie/risk appetite
laag	Onwaarschijnlijk dat het voorkomt met zeer lage impact	Risico kan geaccepteerd worden
matig	Kan wellicht voorkomen met geringe impact	Risico kan met enige beheersing genomen worden
hoog	Kans is groot dat het voorkomt met grote impact	Risico moet beheerst worden
extreem	Risico zal zeer zeker voorkomen met grote gevolgen	Risico mag niet genomen worden

Good practice van een analyse van brutorisico's

Scenario	Kans	Impact	Bruto-risico	Actie/Risk appetite
Klanten maken gebruik van complexe, ondoorzichtige constructies	4	4	extreem	niet acceptabel, vermijden
Medewerker adviseert over mogelijkheden tot ontwijking van fiscale regelgeving	1	3	hoog	acceptabel, beheersen
Klanten zitten in offshoregebieden	3	3	hoog	acceptabel, beheersen
Medewerker is privé betrokken bij klant	2	2	matig	acceptabel, enige beheersing

Wat is dit onderdeel van de risicoanalyse niet?
Dit gaat **niet** om een risicobeoordeling van individuele klanten.

Analyse van beheersing

Per scenario/brutorisico bekijkt u welke beheersingsmaatregelen er tegenover staan. Dit betekent dat u bijvoorbeeld alle werkinstructies benoemt en beoordeelt op effectiviteit.

Het ligt voor de hand dat Compliance dit doet in overleg met Audit en met de diverse afdelingen waar de beheersingsmaatregelen uitgevoerd worden. Compliance heeft een monitorende rol en zal derhalve een goed beeld hebben van het niveau van de beheersing. Kennis en inzicht vanuit de business is echter essentieel.

Bij de beoordeling van de beheersing van integriteitrisico's is het van groot belang om ook mee te nemen de mate waarin de organisatiecultuur integer handelen bevordert of daaraan afbreuk doet. Beloningen, outsourcing, en in diverse landen activiteiten hebben, zijn factoren die een rol spelen bij de mate waarin de beheersing effectief is.

Het is hierbij wel zaak dat u de beheersing realistisch beoordeelt. Als u namelijk een goed beeld wilt hebben van mogelijke grote risico's waar beperkte beheersing tegenover staat, heeft het geen zin om de beheersing te rooskleurig in te schatten. Ook voegt het weinig toe om alleen op te sommen dat men bepaalde procedures heeft of controles doet. Het gaat primair om de vaststelling dat de beheersingsmaatregel bestaat en daadwerkelijk toegepast wordt. Ook hiervoor gebruikt uw instelling een methodiek om de beheersing te analyseren. Dit kan kwalitatief of kwantitatief zijn.

Naast een overzicht en waardering van beheersingsmaatregelen, geeft elke instelling ook een beschrijving van incidenten die zich het afgelopen jaar hebben voorgedaan en van tekortkomingen die aan het licht zijn gekomen.

Als er zich nieuwe risico's voordoen waar nog geen beheersingsmaatregelen tegenover staan, moet de instelling beoordelen of men het risico wil accepteren, beperken of vermijden. Afhankelijk van de keuze zal daarvoor vervolgens een beheersingsmaatregel moeten worden ingericht.

Voorbeelden van beoordeling van werking beheersingsmaatregelen

Criteria om huidige beheersing te waarderen (opzet en werking)		
	1 werkt volledig en optimaal	Sterk: er zijn sterke maatregelen om het risico te beheersen
	2 kan op onderdelen verbeterd worden, maar werkt adequaat en heeft effect	Effectief: het risico wordt adequaat beheerst
	3 substantiële verbetering nodig, maar er is enig effect	Ineffectief: het risico wordt niet adequaat beheerst
	4 geen beheersing, of beheersing heeft geen effect.	

Wat is geen good practice?

Een instelling hecht doorgaans veel belang aan de mate van naleving van de regelgeving. Daardoor wordt veelal hoofdzakelijk gedacht aan het risico dat overblijft na het nemen van maatregelen (het nettorisico). Voor de integriteitrisicoanalyse is het juist relevant om niet uit te gaan van de mate van beheersing om vervolgens te bekijken of er nog nettorisico's zijn. Zonder de voorafgaande analyse van brutorisico's zal een instelling nooit goed kunnen beoordelen waar de integriteitrisico's zich voordoen.

Stap 3: de bepaling van nettorisico's en beslissing over te nemen beheersingsmaatregelen

Uw instelling bepaalt het nettorisico door het niveau van de beheersing 'af te trekken' van het brutorisico. Het nettorisico is het restrisico dat overblijft van een brutorisico bij een optimaal functionerende beheersing.

Bij de bepaling van het nettorisico beoordeelt u of dit nettorisico binnen de risk appetite valt. Dus een beoordeling van de mate waarin uw instelling het nettorisico uiteindelijk wil accepteren, beperken of vermijden. Als dit resterende risico niet binnen uw risicotolerantie zit, dan moet u extra beheersingsmaatregelen treffen of zult u het risico verminderen. In die gevallen dat vermindering vanwege het inherente karakter van het risico niet mogelijk is (bijvoorbeeld landen waar klanten betalingen uit ontvangen), kiest u vanzelfsprekend voor aanvullende beheersing. Niet alle risico's zullen tot nul teruggedrongen kunnen worden. Na aanvullende maatregelen kan er dus een restrisico overblijven. U moet zich hier wel van bewust blijven.

Juist dit deel van de analyse, waar hiaten in beheersing of risico's die buiten de risk appetite vallen zijn vastgesteld, is belangrijk voor management om kennis van te nemen. Management zal aan de hand daarvan moeten beslissen over de te nemen acties. Management zal de integriteitrisicoanalyse immers als sturingsdocument gebruiken. Uiteindelijk levert de integriteitrisicoanalyse een goed beeld van risico's waar meer beheersing nodig is en risico's die met minder beheersing gemitigeerd kunnen worden.

Ook is het belangrijk dat u alle medewerkers een exemplaar van de integriteitrisicoanalyse met een duidelijke toelichting verstrekt. Dit kan bijvoorbeeld in een schematisch overzicht waarin in één oogopslag is te zien waar zich de hoogste risico's voordoen en hoe deze gemitigeerd moeten worden. Op deze manier zijn medewerkers ook goed op de hoogte van de belangrijkste risico's en kunnen zij de regelgeving risicogebaseerd naleven.

Voorbeelden van beoordeling nettorisico en vervolgacties

Nettorisico	Omschrijving	Acties waartoe management kan beslissen
	Laag risico: het is onwaarschijnlijk dat het risico schade veroorzaakt Medium risico: er is enige mogelijkheid dat het risico schade veroorzaakt Hoog risico: er is redelijke kans dat het risico schade veroorzaakt	Accepteren: nettorisico is laag en mitigerende maatregelen werken goed Verminderen: verminderen van risico of verbeteren beheersing Overdragen: risico eventueel verzekeren (niet outsourcen) Vermijden: stoppen met de activiteit

Good practice

Een instelling biedt het bestuur een duidelijk overzicht van geïdentificeerde tekortkomingen en bruto- en nettorisico's die buiten de risk appetite vallen. Inclusief voorgestelde acties en een planning. Dit overzicht laat zichtbaar de prioriteiten zien. Daarnaast worden meer algemene verbeterpunten benoemd die bij het maken van de risicoanalyse aan het licht zijn gekomen.

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