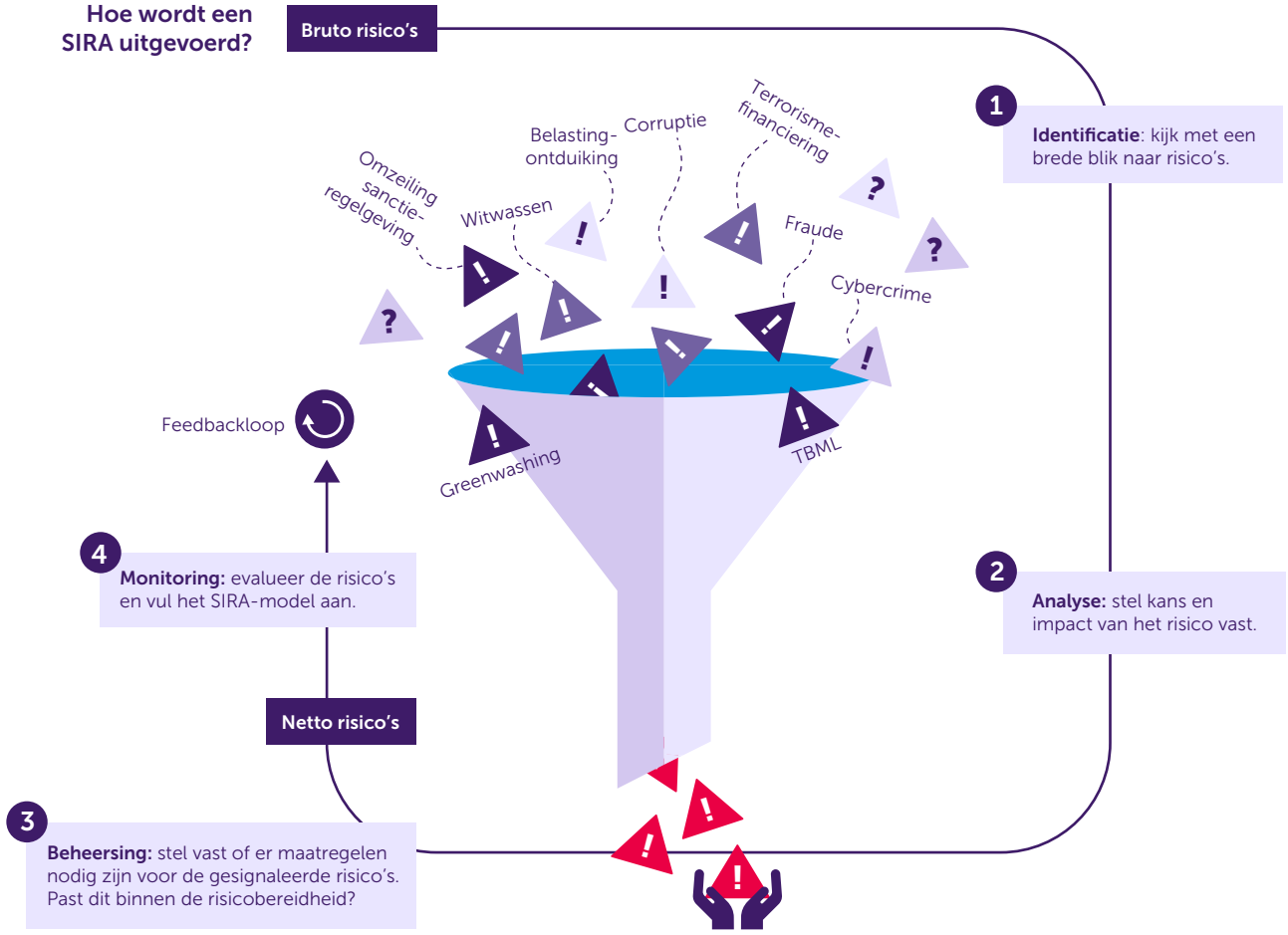
TOEZICHT VISUELE SAMENVATTING

SIRA: van analyse naar beheersing

In het kort De AFM en het BFT hebben gezamenlijk een themaonderzoek uitgevoerd naar de systematische integriteits-risicoanalyse (SIRA) bij accountantsorganisaties. Wij hebben hierbij onderzocht of accountantsorganisaties het SIRA-beleid goed hebben opgezet en adequaat naleven, zodat integriteitsrisico's beter worden beheerst. We concluderen dat het beleid om een goede systematische risicoanalyse op integriteit uit te kunnen voeren steeds beter op orde is bij middelgrote accountantsorganisaties. Wel kan de invulling van dit beleid specifieker en vraagt de toepassing ervan om verbetering.

Hoe wordt een SIRA uitgevoerd?



BUREAU FINANCIEEL TOEZICHT

AFM

TOEZICHT RAPPORT

Inhoud

BUREAU FINANCIEEL TOEZICHT

AFM

1. Inleiding

1.1 Scherpe poortwachtersrol accountantsorganisaties belangrijk voor vertrouwen

Accountantsorganisaties hebben een belangrijke poortwachtersrol. Het is van belang om te voorkomen dat het financieel-economisch stelsel wordt misbruikt voor maatschappelijk schadelijk gedrag en te verzekeren dat het vertrouwen in de integriteit van het stelsel gehandhaafd blijft.

Als accountantsorganisaties die rol niet goed uitvoeren, kan dat negatieve gevolgen hebben voor het vertrouwen in dit stelsel én de beroepsgroep. Het dienen van het publiek belang is een belangrijke legitimiteit voor de wettelijke status van het accountantsberoep.

Accountantsorganisaties moeten daarom onder andere integriteitsrisico's beheersen. Dit gaat zowel om de integriteitsrisico's bij (controle)cliënten als die in de eigen organisatie en vraagt van de accountantsorganisaties dat zij zich bewust zijn van integriteitsrisico's die zich kúnnen voordoen. Door externe ontwikkelingen, zoals digitalisering en internationale gebeurtenissen, neemt ook nog eens de diversiteit en complexiteit van deze risico's toe. Voor accountantsorganisaties is de juiste toepassing van de systematische integriteitsrisicoanalyse (SIRA) daarmee extra relevant geworden.

De Autoriteit Financiële Markten (AFM) en het Bureau Financieel Toezicht (BFT) vinden het belangrijk dat accountantsorganisaties de integriteitsrisico's op een goede manier analyseren en beheersen. Dat stelt hen beter in staat incidenten en betrokkenheid bij strafbare feiten, zoals onder meer witwassen, terrorismefinanciering en corruptie te voorkomen. De SIRA is een effectief instrument om inzicht te verkrijgen in integriteitsrisico's en deze te beheersen en geeft handvatten om invulling te geven aan de poortwachtersrol.

Daarom hebben de AFM en het BFT een gezamenlijk themaonderzoek uitgevoerd naar het gebruik van de SIRA bij accountantsorganisaties met een reguliere Wta-vergunning (AO's-RV). Dit onderwerp bevindt zich op een snijvlak van de toezichtvelden van de AFM en het BFT, respectievelijk de integere en beheerste bedrijfsvoering en de naleving van de verplichtingen van de Wwft[1]. De AFM en het BFT beogen met een gezamenlijk onderzoek naar de SIRA de toezichtsdruk te verminderen.

1.2 Vervolg op eerder onderzoek naar SIRA

De AFM heeft in 2017/2018 een verkennend onderzoek gedaan naar de opzet van het SIRA-beleid van AO's-RV. Uit dit onderzoek bleek dat bij de onderzochte AO's-RV ruimte was voor verbetering in de manier waarop integriteitsrisico's werden geanalyseerd en beheerst.

Ook het BFT heeft de afgelopen jaren bij zijn toezichtonderzoeken vastgesteld dat de invulling en het actueel houden van het risicobeleid en -management een blijvend aandachtspunt is voor instellingen, waaronder AO's-RV. Onderdeel van dit risicobeleid is het beoordelen van de integriteitsrisico's rondom witwassen en terrorismefinanciering.

1 Wwft: Wet ter voorkoming van witwassen en financieren van terrorisme.

Verder hebben de AFM en het BFT signalen ontvangen waaruit bleek dat accountantsorganisaties, waaronder AO's-RV, onvoldoende oog hebben voor de beoordeling en beheersing van integriteitsrisico's die de accountantsorganisaties kunnen raken.[2] Dit beeld wordt bevestigd door een aantal recente publicaties:

- Uit het themaonderzoek cliënt- en opdrachtaanvaarding en -continuering (CEAC) 2022 van de AFM bleek dat accountantsorganisaties meer diepgang moeten geven aan de beoordeling van de integriteit van hun controlecliënten. Bij meer dan de helft van de onderzochte accountantsorganisaties was het CEAC-beleid niet op orde en bij het merendeel van de onderzochte wettelijke controles waren de CEACs onvoldoende uitgevoerd.[3] Een goede SIRA kan helpen bij het verbeteren van dit proces.
- Het rapport 'Fraude vraagt een meer kritische grondhouding' van de NBA.[4]
- Uit 'Sector in Beeld 2023'[5] en onderliggende data kwam een aantal ontwikkelingen naar voren waaruit blijkt dat de toepassing van de SIRA door accountantsorganisaties aandacht verdient:
  - Het aantal AO's-RV is in de afgelopen jaren gedaald. Dit terwijl over de jaren heen het aantal wettelijke controles ongeveer gelijk is gebleven. Het marktaandeel van AO's-RV in de wettelijke controles is de afgelopen jaren gestegen.
  - Er is al enige jaren sprake van een tekort aan accountants. Personeelstekorten leiden ertoe dat accountantsorganisaties kritischer (moeten) kijken naar hun cliëntenportefeuilles en kritischer zijn in het aannemen van nieuwe cliënten.
  - Cliënten die bijvoorbeeld actief zijn in meer risicovolle branches of landen laten vaker dan voorheen de jaarrekeningcontrole uitvoeren door kleine(re) AO's-RV.
- Uit het themaonderzoek frauderisicoanalyse 2023 van de AFM bleek dat de frauderisicoanalyse op meerdere onderdelen tekortschiet en deze scherper uitgevoerd dient te worden.[6]

1.3 Vijf belangrijkste uitkomsten uit het onderzoek

Het doel van ons onderzoek is om te toetsen of AO's-RV de SIRA structureel en doorlopend beoordelen en waar nodig aanscherpen, zodat integriteitsrisico's adequaat worden beheerst. In het onderzoek hebben integriteitsrisico's die verband houden met de Wwft (-verplichtingen) extra aandacht gekregen. De AFM en het BFT willen met dit rapport de sector *good practices* aanreiken en valkuilen delen die we in de praktijk hebben gezien. De AFM en het BFT roepen de AO's-RV op om de SIRA, waar nodig, verder aan te scherpen en dit beleid na te leven.

De belangrijkste uitkomsten van het onderzoek naar de opzet en naleving van de SIRA zijn:

A. Ten opzichte van de uitkomsten van het eerdere AFM-onderzoek naar de SIRA zijn AO's-RV aan de slag gegaan met het opstellen en verbeteren van het SIRA-beleid en het inzichtelijk maken van integriteitsrisico's in een SIRA-model:
   1. **Elk onderzocht kantoor beschikt over een SIRA-beleid**, waar dit in 2017/2018 alleen uit een plan van aanpak bestond met het voornemen om een SIRA-beleid op te (gaan) stellen.
   2. **Het SIRA-beleid en -model moeten wel meer kantoorspecifiek gemaakt worden**.

B. Bij de toetsing of het SIRA-beleid wordt nageleefd door de AO's-RV in de opdrachten die zij uitvoeren, is gebleken dat zij integriteitsrisico's onvoldoende identificeren en beheersen door:
   3. **te beperkte scope**: integriteitsrisico's zijn breder dan enkel risico's ten aanzien van de Wwft, fraude en corruptie. Er ligt onvoldoende focus op andere integriteitsrisico's zoals branchespecifieke integriteitsrisico's, sanctiewetgeving, *trade based money laundering* (TBML) of *greenwashing*. Deze maken te weinig onderdeel uit van de integriteitsrisico's in de risicoanalyse (paragraaf 3.1).

2 Onder meer kan worden gedacht aan recente witwascasussen bij entiteiten die worden gecontroleerd door AO's-RV en signalen over overtreding van de sanctiewetgeving door gecontroleerde entiteiten.

3 Onderzoek naar CEAC (afm.nl) (december 2022)

4 Fraude vraagt een meer kritische grondhouding (nba.nl) in juni 2022.

5 Bron: AFM, Sector in beeld 2023 - Ontwikkelingen in de markt van accountantsorganisaties

6 Scherper op frauderisico's! (afm.nl) (medio 2023)

4. **onvoldoende expliciete overweging integriteitrisico's:** in de dossiers wordt onvoldoende vastgelegd waarom de geïdentificeerde integriteitsrisico's wel of niet meegenomen moeten worden in de controleaanpak. De AO's-RV kunnen blinde vlekken hebben ten aanzien van hun klant, bijvoorbeeld door de vaak langdurige relatie. Risico's worden mogelijk impliciet overwogen en niet voldoende vastgelegd (paragraaf 3.2).
5. **ontoereikende waarborgen:** op geïdentificeerde risico's worden onvoldoende (specifieke) werkzaamheden verricht en worden niet specifiek op integriteitsrisico's gerichte waarborgen getroffen (paragraaf 3.3).

1.4 Leeswijzer

In hoofdstuk 2 worden de uitkomsten van het onderzoek ten aanzien van het SIRA-beleid gedeeld en in hoofdstuk 3 de naleving van het SIRA-beleid. In hoofdstuk 2 en 3 staan we ook stil bij valkuilen en *good practices*. In hoofdstuk 4 gaan we in op de onderzoeksaanpak. In hoofdstuk 5 schenken we aandacht aan hoe nu verder?

2. SIRA-beleid duidelijk verbeterd, maar pas op voor papieren tijger

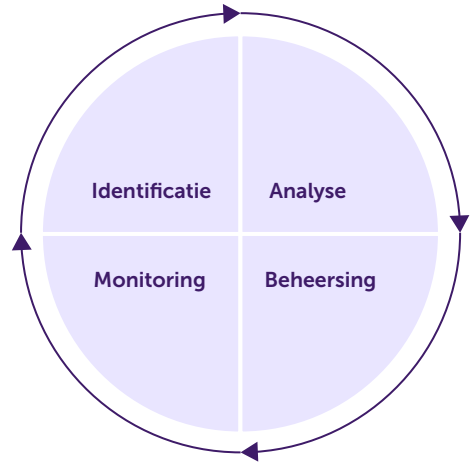
In 2019 hebben de AFM, NBA en SRA uitgesproken dat zij verwachten dat alle AO's-RV uiterlijk eind 2020 aantoonbaar integriteitsrisico's inzichtelijk maken, beheersen en monitoren.[7]

Uit ons onderzoek blijkt dat de geselecteerde AO's-RV een SIRA-beleid hebben en integriteitsrisico's inzichtelijk maken in een SIRA-model. Hier is sprake van een verbetering ten opzichte van het onderzoek uit 2017/2018. Ons onderzoek laat echter ook zien dat bij nagenoeg alle onderzochte AO's-RV sprake is van een theoretische benadering van de SIRA. Er moet worden voorkomen dat de SIRA een papieren tijger wordt. AO's-RV hebben voor standaardrisico's beoordeeld of deze zich zouden kunnen voordoen. We zien dat (integriteits)risico's in het beleid algemeen geformuleerd zijn en niet voldoende zijn afgestemd op de cliëntenportefeuille van de accountantsorganisaties (aard en omvang van de cliënten). Daarnaast worden risico's als gevolg van ontwikkelingen (bijvoorbeeld *cybercrime* en *greenwashing)* onvoldoende in de analyse betrokken.

"Je gaat het pas zien als je het door hebt", zei Johan Cruijff. Dit geldt ook voor (integriteits)risico's. Het is belangrijk dat accountantsorganisaties deze risico's op cliëntniveau beheersen. En om *in control* te zijn, moeten zij het geheel van integriteitsrisico's daarnaast óók op kantoorniveau beheersen. Uit diverse gesprekken met AO's-RV komt naar voren dat zij in de komende periode die volgende stap gaan zetten. Dit is noodzakelijk voor de beheersing.

Wij hebben bij de geselecteerde AO's-RV het meest recent uitgewerkte SIRA-beleid/risicobeleid en SIRA-model opgevraagd. In het onderzoek naar de opzet van het beleid zijn verschillende onderdelen betrokken, zoals de algemene opzet, *risk appetite,* risico-identificatie, risicoanalyse, risicobeheersing en risicomonitoring. In dit hoofdstuk staan we stil bij valkuilen en *good practices* ten aanzien van deze onderdelen.

Cyclus risicobeheersing integriteitsrisico's



2.1 Maak beleid meer kantoorspecifiek

De AO's-RV beschikken alle over een risicobeleid in de vorm van een (kwaliteits)handboek en een SIRA-model. De SIRA vindt bij de meeste onderzochte AO's-RV óf op kantoorniveau óf op cliëntniveau plaats en in een enkel geval op beide niveaus. De diepgang van de verstrekte documentatie verschilt. De verschillen zijn deels te verklaren door de omvang en de volwassenheid van de AO-RV en door de aard en risicoclassificatie van hun cliëntenportefeuille. Daarnaast bestaan tussen de AO's-RV aanzienlijke verschillen in de frequentie en de intensiteit waarmee aandacht wordt besteed aan vooral het actualiseren en het aanvullen van het SIRA-model.

AO's-RV die zijn aangesloten bij een brancheorganisatie maken veelal gebruik van kwaliteitshandboeken van de brancheorganisatie. Wij constateren dat de (kwaliteits)handboeken van bijna alle AO's-RV weinig

7 AFM biedt handvatten beheersing integriteitsrisico's accountantsorganisaties

kantoorspecifiek zijn gemaakt. Procedures zijn vaak op hoofdlijnen beschreven en risico's uit het SIRA-model komen niet terug in het beleid en zijn niet afgestemd op de specifieke kenmerken van de AO-RV of de aard en risicoclassificatie van haar cliëntenportefeuille.
Voor wat betreft het SIRA-model maakt het merendeel van de AO's-RV gebruik van een (voorbeeld)*template.* Veelgebruikte voorbeelden zijn modellen van DNB en brancheorganisaties.

Het SIRA-beleid/risicobeleid en het SIRA-model zijn naar onze mening het meest effectief als zij kantoorspecifiek zijn gemaakt voor de accountantsorganisatie en de cliënten die worden bediend. Het gaat hierbij om onder meer (actuele) cliëntspecifieke en kantoorspecifieke risico's en aanvaardbare en onaanvaardbare risico's (inclusief beheersmaatregelen).

Wij hebben gezien dat door AO's-RV het opstellen van het SIRA-model op verschillende manieren is vormgegeven. Sommige AO's-RV kozen voor een organisatiebrede werkgroep. Bij andere AO's-RV zijn de risico's door de compliance officer in kaart gebracht.

Wij vinden het belangrijk dat de SIRA binnen de gehele organisatie bekend is en wordt gedragen. Medewerkers zijn beter in staat integriteitsrisico's te herkennen als ze vaker en diepgaander worden besproken binnen de organisatie en de teams. Dit kan in de vorm van praktijkcasussen en/of het formuleren van scenario's. Daardoor is de feedbackloop ingebed; dat maakt onderdeel uit van een goede risicomonitoring.

2.2 Bepaal risk appetite op kantoorniveau

Risk appetite is de risicobereidheid van de organisatie bij het nastreven van haar doelstellingen. Het vaststellen en vastleggen van de *risk appetite* is een belangrijk startpunt bij de risicobeheersing. De *risk appetite* geeft aan welke (integriteits)risico's een accountantsorganisatie wel of niet bereid is te lopen, al dan niet na het treffen van beheersmaatregelen. Hierbij kan worden gedacht aan het uitsluiten van branches, geografische gebieden en maximum aandeel van hoog risico cliënten in de portefeuille. Deze risicobereidheid is kantoorspecifiek. Het vaststellen van de *risk appetite* is een iteratief proces, waarbij interne en externe ontwikkelingen kunnen leiden tot het bijstellen van de *risk appetite.*

Wij constateren dat het merendeel van de onderzochte AO's-RV op organisatieniveau geen *risk appetite* heeft geformuleerd. In de (kwaliteits) handboeken staat vaak wel een opsomming welke branches of type ondernemingen een AO-RV niet wil accepteren. In de SIRA-modellen is in de meeste gevallen bij de scenario's aangegeven of deze wel of niet vallen binnen de *risk appetite* van de AO-RV, maar is niet specifiek gemaakt hoe de *risk appetite* moet worden bepaald.

Uit de interviews met de AO's-RV is naar voren gekomen dat de *risk appetite* vaak is ingegeven door kennis die in huis is, de beschikbare capaciteit, aantrekkelijk werkgeverschap en in mindere mate door (integriteits)risico's.

Wij hebben bij een aantal AO's-RV een *risk appetite* op kantoorniveau gezien. AO's-RV streven bijvoorbeeld naar een maximaal percentage cliënten met een verhoogd risicoprofiel. Er wordt een cliëntenstop ingesteld voor dit soort cliënten als de maximale capaciteit is bereikt. Wij vinden dat dit voorbeeld als startpunt kan worden gebruikt, maar verdere specificering nodig heeft. Daarbij kan bijvoorbeeld worden gedacht aan het specificeren of het percentage moet worden gezien in het licht van cliënt- of opdrachtniveau, of juist in het licht van het aantal cliënten, de omzet of het totaal aantal uren. Daarbij is ook belangrijk dat naar alle integriteitsrisico's wordt gekeken en niet slechts naar de Wwft-risico's.

2.3 Zie de échte integriteitsrisico's

De risico-identificatie verloopt bij voorkeur via een vaste, gestandaardiseerde en – waar mogelijk – geautomatiseerde werkwijze. Voor ons onderzoek hebben wij de risico-identificatie, de in het beleid opgenomen integriteitsrisico's en de scenario's in het SIRA-model beoordeeld. In de meeste gevallen zijn in het beleid (integriteits)risico's opgenomen. We zien dat (integriteits)risico's in het beleid vaak algemeen geformuleerd zijn en niet in overeenstemming zijn met de aard van de cliëntenportefeuille van de accountantsorganisaties. De risico's in het beleid zien daarnaast voornamelijk op witwassen en financieren van terrorisme.

In de SIRA-modellen is in bijna alle gevallen een aantal standaardrisico's opgenomen, waaronder: witwassen, (fiscale) fraude, corruptie/omkoping, omzeiling sancties, terrorismefinanciering, belangenverstrengeling, *cybercrime* en maatschappelijk onbetamelijk gedrag. Deze risico's vormen de basis voor de scenario's die de AO's-RV hebben geformuleerd. In de scenario's zien wij grote verschillen in de aantallen en de kwaliteit. Zo kan het SIRA-model actueel worden gehouden door het toevoegen van scenario's als deze zich voordoen in de praktijk.

Voor een goede risico-identificatie is ten minste het volgende nodig:

- Benader integriteitsrisico's vanuit verschillende invalshoeken. Voorbeeld: corruptierisico's worden gekoppeld aan een land en de daarbij behorende CPI-score[8]. Dit terwijl ook corruptierisico's kunnen bestaan door de branche waarin de cliënt actief is;
- Identificeer cliëntspecifieke risico's;
- Identificeer kantoorspecifieke risico's. Denk hierbij aan leveranciers, werknemers en eigen dienstverlening;
- Benoem aanvaardbare en onaanvaardbare risico's;
- Neem risico's uit praktijkvoorbeelden op in het SIRA-model;
- Werk bijbehorende scenario's uit; **concreter = beter!**

GOOD PRACTICES: (technische) ondersteuning helpt!
Een AO-RV heeft een applicatie die wordt gebruikt om risico's te inventariseren en vast te leggen. Deze applicatie wordt intern en door cliënten (*self-assessment)* gebruikt om risico's te inventariseren en vast te leggen. In de applicatie zijn taken, risico's en acties opgenomen. De SIRA is onderdeel van deze taken en wordt periodiek besproken en geëvalueerd. Dit zorgt ervoor dat de SIRA leeft binnen de organisatie, regelmatig wordt geactualiseerd en dat acties worden gemonitord. De applicatie zorgt bovendien voor tijdige registratie en opvolging van incidenten.

Andere AO's-RV hebben een registratiesysteem waarin - naast de risicoclassificatie van de gehele cliëntenportefeuille- is vastgelegd wat bijzondere gevallen zijn, welke cliënten/*proposals* zijn afgewezen en wat de reden hiervoor is.

VALKUIL: is het een match?
Diverse accountantsorganisaties maken gebruik van externe KYC-dienstverleners[9] voor het uitvoeren van (delen van) het cliëntenonderzoek. Wij zien dat een aantal AO's-RV volledig steunt op de uitkomsten die zij ontvangen van deze externe partijen.

Voordat een externe partij wordt gecontracteerd, is het belangrijk om na te gaan of deze past bij de eigen cliëntenportefeuille. Als een accountantsorganisatie bijvoorbeeld een internationale cliëntenportefeuille heeft, is het van belang dat niet alleen de Kamer van Koophandel wordt geraadpleegd, maar ook registers in landen waar de cliënten actief zijn. De accountantsorganisatie moet achteraf ook toetsen of het cliëntenonderzoek dat is uitgevoerd, voldoet aan de Wwft-verplichtingen. Indien noodzakelijk moet de accountantsorganisatie aanvullende werkzaamheden uitvoeren.

8 CPI staat voor Corruption Perceptions Index, een overzicht van Transparency International. De lijst is een indicator die aangeeft in hoeverre de publieke sector van verschillende landen wordt ervaren als vrij van corruptie.

9 KYC staat voor Know your customer.

3. Naleving van het opgestelde SIRA-beleid vraagt om verbetering

Hoewel alle onderzochte AO's-RV een SIRA-beleid en een SIRA-model hebben, blijkt dat de naleving onvoldoende is en beter moet. Uit ons onderzoek blijkt dat in nagenoeg alle gevallen nog sprake is van een theoretische exercitie. Eén van de belangrijkste conclusies is dat integriteitsrisico's onvoldoende worden onderkend, waardoor de (controle)werkzaamheden om de integriteitsrisico's te beheersen veelal tekortschieten dan wel kwaliteitswaarborgen onvoldoende zijn ingezet.

Hierbij merken we op dat in het onderzoek alleen afgeronde dossiers zijn betrokken. Dit terwijl het SIRA-beleid bij veel onderzochte AO's-RV afgelopen jaar is geactualiseerd. Wij verwachten dat op korte termijn de stijgende lijn die in het vorige hoofdstuk aan de orde is gekomen in de naleving bij lopende en de toekomstige opdrachten terug te zien.

3.1 Kijk breder naar integriteitsrisico's in de identificatiefase

Let op de volgende integriteitsrisico's:
- belangenverstrengeling
- corruptie en omkoping
- *cybercrime*
- *greenwashing*
- interne/externe fraude
- maatschappelijk onbetamelijk gedrag
- marktmanipulatie
- omzeiling sanctieregelgeving
- ontduiking van fiscale regelgeving
- terrorismefinanciering
- *trade-based money laundering* (TBML)
- witwassen

Voorafgaand aan een opdracht is het identificeren van de integriteitsrisico's een belangrijke stap. In het merendeel van de onderzochte dossiers is deze niet voldoende gebleken. Bij de *non-assurance*-opdrachten bleek er veelal geen aparte vastlegging te zijn van (geïdentificeerde) integriteitsrisico's. Daarvoor werd vaak verwezen naar het cliëntacceptatieproces van het wettelijke-controledossier, waarvan het identificeren van integriteitsrisico's onderdeel uitmaakt.
Het merendeel van de bevindingen[10] in het onderzoek ziet op het *niet* dan wel onvoldoende identificeren van integriteitsrisico's in de opdrachtacceptatie- en -continuatiefase. Dit werkt door in het vervolg van de (controle)werkzaamheden.

Waar de integriteitsrisico's *wel* zijn geïdentificeerd, beperken deze zich bij meer dan de helft van de onderzochte dossiers tot witwasrisico's, waarbij vooral wordt ingegaan op de meldingsplicht van ongebruikelijke transacties. Bij minder dan de helft van de onderzochte dossiers is een corruptierisico geïdentificeerd. Andere relevante integriteitsrisico's blijven merendeels buiten ogenschouw, waaronder landenrisico's en branchespecifieke integriteitsrisico's. Een open blik en een professioneel-kritische instelling zijn vereist om tot een volledige identificatie van de integriteitsrisico's te komen.

Een andere observatie is dat accountants beredeneren waarom integriteitsrisico's zich *niet* voordoen in plaats van dat zij onderzoeken hoe integriteitsrisico's zich *wel* kunnen voordoen. Het is essentieel kennis van de branche te hebben waarin de betreffende cliënt actief is. Een voorbeeld is het gebruik van een branchespecifieke template om integriteitsrisico's in kaart te brengen.

We hebben bij een aantal AO's-RV gezien dat zij bij negatieve mediaaandacht ten aanzien van de cliënt dit in het managementteam en met de compliance officer bespreken. Vervolgens bekijken zij of met beheersingsmaatregelen het integriteitsrisico naar een aanvaardbaar niveau teruggebracht kan worden of dat aanvullende beheersings-

10 Er is sprake van een bevinding als niet wordt voldaan aan een Wwft-norm, een Wta/Bta-norm of een NV COS-norm.

maatregelen of zelfs het afscheid nemen van de cliënt nodig zijn. Een ander voorbeeld is dat periodiek wordt gemonitord of sprake is van nieuwe media-aandacht. Als dat zo is, worden de integriteitsrisico's opnieuw geëvalueerd.

Nog een manier om vroegtijdig integriteitsrisico's te identificeren, is dat voorafgaand aan het intake-gesprek met de cliënt een *'pre-client due diligence*-toets' wordt uitgevoerd. Daarbij worden de Wwft-vereisten nagelopen.

Van accountantsorganisaties wordt een professioneel-kritische houding verwacht. In het merendeel van de dossiers bleek dat integriteitsrisico's met onvoldoende diepgang worden besproken. Sommige integriteitsrisico's worden wel geïdentificeerd, maar vervolgens weggeredeneerd: *'we kennen de cliënt', 'dit speelt hier niet'* en *'de branche wordt zwaar gereguleerd'*. De integriteitsrisico's worden vervolgens niet opgenomen in de risicoanalyse.

VALKUIL: wat is vaak?
Wij hebben gezien dat voor de indeling van integriteitsrisico's gebruik wordt gemaakt van subjectieve schalen, zoals 'komt vaak voor' tegenover 'komt niet zo vaak voor'. Daarbij is niet gekwantificeerd wat 'vaak' inhoudt. De valkuil hierbij is dat het identificeren van het integriteitsrisico afhankelijk is van wat de accountant zelf onder 'vaak' verstaat.

GOOD PRACTICE: standaard puntensysteem
Als good practice - om de subjectiviteit uit bovengenoemde valkuil zo veel mogelijk op te lossen - hebben wij bij een AO-RV gezien dat wordt gewerkt met een standaard puntensysteem. Hierbij wordt gewerkt met geobjectiveerde en gesloten vragen. Het totaal aantal punten kan vervolgens worden afgezet tegen de *risk appetite* van de accountantsorganisatie. Met dit geobjectiveerde systeem wordt zoveel mogelijk voorkomen dat het al dan niet identificeren van integriteitsrisico's afhankelijk is van de persoon die de beoordeling doet.

GOOD PRACTICE: betrek de keten
Een AO-RV betrekt de keten bij het identificeren van integriteitsrisico's. Zij laat de cliënt een *self-assessment* uitvoeren, waarbij deze zelf nadenkt over de mogelijke integriteitsrisico's in zijn branche en onderneming. Dit heeft als voordeel dat de externe accountant met een bredere blik de risico-identificatie kan uitvoeren en biedt een opening voor een open gesprek met de cliënt over integriteitsrisico's.

GOOD PRACTICE: inzicht in brancherisico's
Een AO-RV zoekt op internet naar voorbeelden van fraude en rechterlijke uitspraken in de branche waarin de cliënt werkzaam is, om voorafgaand aan de opdracht een breder beeld te hebben van de branchespecifieke integriteitsrisico's.

3.2 Overweeg integriteitsrisico zorgvuldig en leg vast

Een jaarrekeningencontrole vindt risicogestuurd plaats. Dit betekent dat op basis van de risicoschatting specifieke controlewerkzaamheden worden uitgevoerd. Alleen door geïdentificeerde integriteitsrisico's in de risicoanalyse te onderkennen, kunnen daar passende beheersingsmaatregelen en werkzaamheden op worden ingezet. Uit ons onderzoek is gebleken dat in het merendeel van de onderzochte dossiers onvoldoende wordt overwogen waarom bepaalde geïdentificeerde risico's niet worden onderkend in de risicoanalyse, waardoor beperkt gebruik wordt gemaakt van kwaliteitswaarborgen en waarbij geen specifieke werkzaamheden worden uitgevoerd.

Integriteitsrisico's kunnen gedurende de opdracht wijzigen. Daarom moeten de integriteitsrisico's gedurende de opdracht op meerdere momenten worden geëvalueerd. Dit kan er bijvoorbeeld toe leiden dat in de afrondingsfase van een opdracht een integriteitsrisico wordt geïdentificeerd en dat aanvullende werkzaamheden worden uitgevoerd. Op die manier worden ook de meest actuele integriteitsrisico's meegenomen in de opdracht. Dit is bijvoorbeeld in het bijzonder relevant bij de naleving van de Sanctiewet, omdat sanctiemaatregelen gedurende de opdracht kunnen wijzigen. Dit voorbeeld geeft aan dat het SIRA-proces doorlopend wordt uitgevoerd (plan, do, check, act) tijdens de opdracht.

3.3 Zet de risicobeheersing meer specifiek in

In het SIRA-beleid moet worden nagedacht of specifieke beheersingsmaatregelen passend zijn bij de onderkende integriteitsrisico's. In meer dan de helft van de onderzochte dossiers is aangetroffen dat de beheersingsmaatregelen niet specifiek op het integriteitsrisico zien of ontoereikend zijn om het risico naar een aanvaardbaar niveau terug te brengen. In de dossiers waarbij opdrachtgerichte kwaliteitsbeoordeling (OKB) is toegepast, is in het merendeel van de gevallen vastgesteld dat de OKB niet specifiek de onderkende integriteitsrisico's meeneemt in de beoordeling.

Het specifiek maken van de beheersingsmaatregelen en werkzaamheden voor de onderkende integriteitsrisico's moet beter. Juist in dossiers waarbij een langdurige cliëntrelatie bestaat, is het belangrijk om specifieke beheersingsmaatregelen toe te passen.

Tijdens het onderzoek hebben wij geobserveerd dat accountants bedenken waarom integriteitsrisico's er niet zijn, terwijl zij juist moeten onderzoeken en onderbouwen hoe integriteitsrisico's zich *wel* kunnen voordoen. Als ervan wordt uitgegaan dat een integriteitsrisico zich bij de cliënt niet zal manifesteren, moet dit wel worden vastgesteld. Vervolgens moeten accountants hierop specifieke werkzaamheden verrichten met een professioneel-kritische instelling en gerichte kwaliteitswaarborgen inzetten.

GOOD PRACTICE: gebruik data-analyse
AO's-RV voerden gedurende de (controle)werkzaamheden een data-analyse uit op cliënt- en dossierniveau. Zo wordt bijvoorbeeld vanuit de betaalbestanden en auditfile van de cliënt een query gedraaid en vertaald naar een landkaart waaruit blijkt waar het geldverkeer plaatsvindt. Vervolgens wordt op afwijkende patronen ingezoomd.

GOOD PRACTICE: uitgebreide risicomatrix
In het softwareprogramma voor de (controle)opdracht van een AO-RV zijn werkprogramma's opgenomen met daarbij een uitgebreide risicomatrix met aandacht voor specifiek de integriteitsrisico's en de Wwft. Zo wordt de beheersing van integriteitsrisico's ingebed in de werkzaamheden.

4. Onderzoeksaanpak

Ons onderzoek omvat de toetsing van de opzet van het beleid omtrent de beheersing van (integriteits)risico's van AO's-RV en de naleving van dat beleid. Hierbij hebben wij een gedifferentieerde onderzoeksaanpak gehanteerd, waarbij enige verschillen zijn in de manier waarop de geselecteerde AO's-RV zijn onderzocht. Voor ons onderzoek zijn 18 kantoren geselecteerd, voornamelijk middelgrote AO's-RV.

Voor het onderzoek naar de opzet van de SIRA en het beleid hebben wij bij de geselecteerde AO's-RV (beleids)documentatie opgevraagd en beoordeeld. Vervolgens is het beleid besproken met de beleidsbepalers.

Voor het onderzoek naar de naleving van het SIRA-beleid en de relevante wet- en regelgeving ten aanzien van integriteitsrisico's hebben wij in het onderzoek, bij 13 van 18 AO's-RV, in totaal 34 dossiers getoetst. Dit ging om *non-assurance*-dossiers (bijvoorbeeld samenstel-, fiscaal advies- en NOW[11]-dossiers) en om wettelijke-controledossiers. De naleving van het SIRA-beleid en de daarbij horende integriteitsrisico's in deze dossiers zijn met de beleidsbepalers en opdrachtverantwoordelijke externe accountants besproken. Dit onderdeel is nieuw ten opzichte van het eerdere SIRA-onderzoek.

Wij hebben voor zover mogelijk dossiers geselecteerd die door de betreffende AO-RV als 'hoog cliënt- en of opdrachtrisico' zijn geclassificeerd. Als deze niet aanwezig waren, hebben we 'midden cliënt- en of opdrachtrisico' geselecteerd. Op deze manier hebben wij geprobeerd inzicht te verkrijgen in de verrichte werkzaamheden omtrent de door de betreffende accountantsorganisatie geïdentificeerde integriteitsrisico's.

11 NOW: tijdelijke Noodmaatregel Overbrugging voor Werkgelegenheid. Dit is een subsidie die is bedoeld voor werkgevers die kampen met substantieel omzetverlies als gevolg van Covid-19.

5. Hoe nu verder?

De AFM en het BFT blijven aandacht houden voor de SIRA.

Zoals eerder opgemerkt laten cliënten die bijvoorbeeld actief zijn in meer risicovolle branches of landen vaker dan voorheen de jaarrekeningcontrole uitvoeren door AO's-RV. Dit leidt ertoe dat ook deze AO's-RV te maken krijgen met meer en andere (integriteits)risico's. De AFM en het BFT willen benadrukken dat de integriteitsrisico's meer omvatten dan alleen witwassen en corruptie. Daarbij merken wij op dat integriteitsrisico's niet statisch zijn. Denk bijvoorbeeld aan de veranderende sanctiemaatregelen na de inval van Rusland in Oekraïne in 2022.

Het onderkennen en beheersen van integriteitsrisico's is van essentieel belang voor de beheersing van de eigen organisatie. Bij het merendeel van de onderzochte AO's-RV is nog sprake van een theoretische exercitie. Accountantsorganisaties moeten voorkomen dat de SIRA een papieren tijger wordt.

Hoewel de AFM en het BFT gematigd positief zijn over de uitkomsten ten aanzien van het beleid, stellen wij vast dat de naleving in de dossiers bij het merendeel onvoldoende is en verbetering behoeft. Wij verwachten dat op korte termijn de volgende stap wordt gezet: van SIR-A (analyse) naar SIR-B (beheersing).

Met deze publicatie beogen wij de sector handvatten te geven en moedigen wij alle accountantsorganisaties en hun brancheorganisaties aan de SIRA naar een hoger niveau te tillen.