Handvatten bij toepassing Systematische Integriteitsrisico Analyse (SIRA)

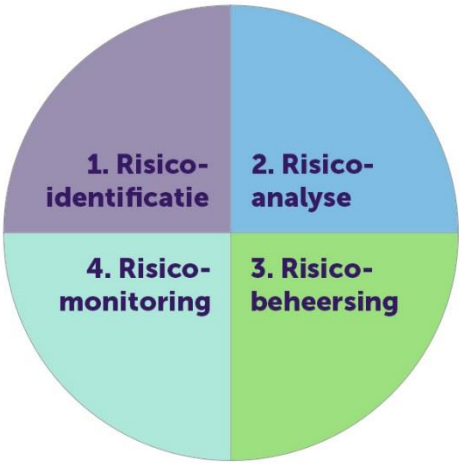
Hulpmiddel bij de beheersing van integriteitsrisico's door niet-OOB accountantsorganisaties

Inzicht in en de beheersing van integriteitsrisico's zijn noodzakelijke voorwaarden voor een integere en beheerste bedrijfsvoering. Het stelt een accountantsorganisatie immers beter in staat incidenten en betrokkenheid bij strafbare feiten te voorkomen, zoals witwassen, terrorismefinanciering, corruptie etc.

Handvatten op basis van inzichten uit de praktijk
In dit document staan handvatten voor het opstellen van een SIRA, op basis van de inzichten uit een verkenning van de Autoriteit Financiële Markten (AFM) naar de risicoanalyse en -beheersing van niet-OOB accountantsorganisaties in 2017 en 2018. Een goede SIRA is maatwerk en het vergt tijd en aandacht om deze toe te spitsen op de specifieke kenmerken (en risico's) van de organisatie. Het doel van deze handvatten is dat accountantsorganisaties kritisch en doorlopend hun eigen beheersing van integriteitsrisico's beoordelen en deze waar nodig aanscherpen.

Wat is de SIRA?
De SIRA is een effectief instrument om inzicht te verkrijgen in integriteitsrisico's en deze te beheersen. De SIRA vormt zo een goede basis voor een adequate inrichting van een beheerste en integere bedrijfsvoering. Meer informatie vindt u in brochures van De Nederlandsche Bank (DNB)[1].

SIRA in vier processtappen
De SIRA bestaat uit vier processtappen.



1. Risico-identificatie
Het maken van een organisatieschets en het identificeren van integriteitrisico's en risicoscenario's.

Vaak is een risico breed gedefinieerd, zoals: het risico op witwassen. Een risicoscenario is de concrete verschijningsvorm van dat risico, zoals bijvoorbeeld: een controleopdracht accepteren bij een klant met grote contante ongebruikelijke geldstromen.

2. Risicoanalyse
Het bepalen van de kans dat een bepaald risicoscenario zich voordoet en welke impact dit, zonder risicobeheersing, heeft: het zogeheten bruto-risico.

3. Risicobeheersing
Het in kaart brengen van beleid, systemen en maatregelen die het bruto-risico beheersen. Daarna bepalen welk risico resteert: het zogeheten netto-risico. Dan beoordelen wat de risicobereidheid is voor dit netto-risico en of (aanvullende) maatregelen nodig zijn.

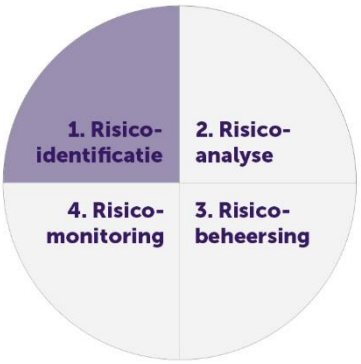
4. Risicomonitoring en -herziening
De periodieke evaluatie en mogelijke aanpassing van de integriteitsrisico's, -scenario's en de beheersing daarvan.

---

[1] - De integriteitrisicoanalyse: https://www.toezicht.dnb.nl/binaries/50-234068.pdf
- Good practice Integrity Risk Appetite: https://www.toezicht.dnb.nl/binaries/50-236706.pdf

Stap 1. Risico-identificatie

Risico-identificatie begint met het maken van een brede beschrijving van de accountantsorganisatie: de organisatieschets. Aan de hand van de organisatieschets wordt een overzicht gemaakt van alle mogelijk integriteitsrisico's en haar verschijningsvormen (de risicoscenario's). Ook wordt bepaald hoe de kans en impact van een risico gewogen gaan worden in stap 2.



Inzichten uit de AFM-verkenning voor het identificeren van integriteitsrisico's

- Het toewijzen van een functionaris die het hele proces van opstellen en implementeren van de SIRA begeleidt, verkort de doorlooptijd van het proces en draagt bij aan de kwaliteit van de geïdentificeerde risico's en risicoscenario's.

- Een gedetailleerde organisatieschets helpt bij het specifiek maken van de SIRA op de context van de eigen organisatie en bevordert daardoor de volledigheid van de risico-identificatie. Een gedetailleerde organisatieschets beschrijft - onder meer - de verschillende rechtspersonen en juridische structuur, de landen waarin de organisatie actief is, de (soorten) dienstverlening, de governance, de deskundigheid en het opleidingsniveau van de medewerkers, de samenwerking met of uitbesteding aan derde partijen, de klanten en de sectoren en landen waarin deze klanten actief zijn.

- De toepasbaarheid van de SIRA wordt vergroot wanneer medewerkers vanuit de verschillende lagen en afdelingen binnen de accountantsorganisatie worden betrokken bij de risico-identificatie. De bekendheid met en het inzicht in de verschillende risico's verschillen immers per organisatieonderdeel. Het betrekken van medewerkers heeft als bijkomend voordeel dat de kennis en bewustwording van de verschillende risico's en het draagvlak voor beheersmaatregelen binnen de organisatie worden vergroot.

- De risico-identificatie kan op verschillende manieren worden gestimuleerd. Een aantal accountantsorganisaties liet bijvoorbeeld (groepen) medewerkers in open discussies brainstormen over risico(scenario)'s of lieten hen in dilemmabesprekingen discussiëren over integriteitsschendingen waarbij hun organisatie betrokken was of kon zijn.

- De Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft) kent een verplichte risicobeoordeling voor accountantsorganisaties. De risico's die betrekking hebben op witwassen en terrorismefinanciering zijn integriteitsrisico's en kunnen in de SIRA worden betrokken.

Good practices geobserveerd bij kleinere[2] accountantsorganisaties

'Wij hebben gemerkt dat het faciliteren van open discussies en dilemmabesprekingen door een aparte functionaris het proces van risico-identificatie sterk bevordert.'
'Wij gebruiken voorbeelden uit de praktijk van de sector om het denkproces te stimuleren.'

Good practices geobserveerd bij middelgrote accountantsorganisaties

'Wij laten ook de eerstelijnsmedewerkers de risico's identificeren, want daar zit veel operationele kennis van de risico's. Daarna combineren wij de input van alle organisatieonderdelen.'
'Wij laten de verschillende vestigingen onafhankelijk van elkaar de risico's identificeren.'

[2] Indicatief moet gedacht worden aan accountantsorganisaties met 1 tot 5 externe accountants.

Stap 2. Risicoanalyse

Na de identificatie en inventarisatie van alle risicoscenario's worden deze geanalyseerd. Er wordt dan een inschatting gemaakt van de kans dat een bepaald scenario zich voordoet en de impact zodra het scenario zich manifesteert.[3]

De geschatte kans en impact bepalen samen het bruto-risico van een risicoscenario. Dit is het bruto-risico dat een accountantsorganisatie loopt zonder rekening te houden met beheersmaatregelen.

Inzichten uit de AFM-verkenning voor het analyseren van integriteitsrisico's

- Bij het beoordelen van de kans op een risicoscenario, is het nuttig om rekening te houden met integriteitsincidenten die in het (recente) verleden plaatsvonden. Een kanttekening hierbij is dat risicoscenario's die hebben plaats gevonden, mogelijk al zijn voorkomen door bestaande beheersmaatregelen. Om te voorkomen dat die risicoscenario's buiten beeld blijven, worden in deze stap beheersmaatregelen buiten beschouwing gelaten.

- Impact kan financieel en niet-financieel zijn. De niet-financiële impact van risicoscenario's, zoals reputatieschade of afbreuk aan de kwaliteit van dienstverlening, is moeilijk vergelijkbaar. Sommige accountantsorganisaties hanteren daarom categorieën die wel onderling vergelijkbaar zijn. Deze categorieën hebben bijvoorbeeld aanduidingen als 'hoog', 'midden', 'laag' of scores van 1 tot 5.

- Consequent gebruikmaken van een eenduidige scoringsmethodiek bij het bepalen van de bruto-risico's, helpt om risico's onderling te kunnen vergelijken en de ontwikkeling van risico's gedurende een periode te kunnen monitoren.

- Sommige accountantsorganisaties vergelijken per risicoscenario eerst het bruto-risico met de risicobereidheid, voordat zij kijken naar beheersmaatregelen. Het voordeel daarvan is dat de kans en impact realistischer kan worden geschat. Bovendien biedt dit meer inzicht in het risico-(scenario) dat de organisatie loopt als een of meer beheersmaatregelen onverwachts (deels) wegvallen.

Good practices geobserveerd bij kleinere accountantsorganisaties

'Wij hebben iedereen via een vragenlijst de verschillende risicoscenario's laten scoren en alle medewerkers gevraagd hoe groot zij de kans inschatten dat een beschreven situatie zich voordoet.'

Good practices geobserveerd bij middelgrote accountantsorganisaties

'Zowel risicoscenario's die een (potentiële) grote financiële schade omvatten als een ernstige reputatieschade vallen bij ons in de categorie "impact: zeer groot".'

'Wij hebben meerdere teams onafhankelijk van elkaar de verschillende risicoscenario's op bepaalde deelgebieden laten inventariseren en elkaar vervolgens laten tegenlezen en uitdagen.'

[3] In stap 1 zijn de (soorten) kans en impact bepaald, het wegen van de risicoscenario's vindt in deze stap plaats

Stap 3. Risicobeheersing

Om risico's te beheersen wordt bij elk bruto-risico vastgesteld welke beheersmaatregelen daar tegenover (moeten) staan. Een beheersmaatregel moet in opzet, bestaan en werking effectief zijn.

Het risico dat resteert na effectieve beheersmaatregelen, is het netto-risico. Is er een verschil tussen het netto-risico en de risicobereidheid van de accountantsorganisatie? Dan worden extra (beheers)maatregelen getroffen.

Inzichten uit de AFM-verkenning voor het beheersen van integriteitsrisico's

- Bij de meeste accountantsorganisaties is aandacht voor de beheersing van integriteitsrisico's. Deze aandacht is echter niet voldoende structureel en bevat niet alle integriteitsrisico's. Het is belangrijk om dit goed in te bedden in de organisatie.

- Door na het vaststellen van het netto-risico een vergelijking te maken met de risicobereidheid, worden mogelijke hiaten inzichtelijk. Ook wordt duidelijk welke risico's buiten de risicobereidheid vallen. Zo kan een organisatie beslissen over aanvullende beheersmaatregelen.

- Organisaties die de uitkomsten van de SIRA actief delen binnen de organisatie, stellen dat dit het bewustzijn van medewerkers vergroot omtrent de integriteitsrisico's en de beheersing daarvan. Dit draagt bij aan de effectiviteit van de beheersmaatregelen.

- Enkele accountantsorganisaties betrekken de uitkomsten van onderzoeken naar gedrag en cultuur in hun organisatie bij het toepassen van de SIRA.

- De accountantsorganisaties benadrukken het belang van een open cultuur en voorbeeldgedrag van leidinggevenden als belangrijke pijlers voor een integere en risicobewuste organisatie.

Good practices geobserveerd bij kleinere accountantsorganisaties

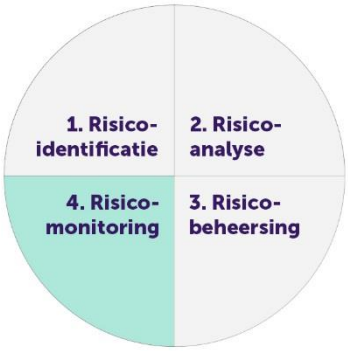
'Wij gebruiken de SIRA jaarlijks ook als aanknopingspunt om het gesprek over integriteitsrisico's met elkaar te voeren.'

'Wij accepteren uitsluitend opdrachten van klanten als het mogelijk is toereikende kwaliteitsmaatregelen (zoals een opdracht gerichte kwaliteitsbeoordeling) te nemen om de risico's te mitigeren.'

Good practices geobserveerd bij middelgrote accountantsorganisaties

'Voor het herkennen van integriteitsrisico's in de praktijk is de bewustwording van de verschijningsvormen van deze risico's belangrijk. Wij delen de SIRA intern en besteden hier jaarlijks aandacht aan in onze trainingen.'

Stap 4. Risicomonitoring en -herziening



De integriteitsrisico's en beheersmaatregelen worden periodiek beoordeeld. Waar nodig worden deze aangepast.

Door de SIRA continu te actualiseren, kunnen wijzigingen in en nieuwe integriteitsrisico's tijdig worden herkend en beheersmaatregelen zo nodig worden genomen of aangescherpt. Hierdoor ontstaat een cyclisch proces van monitoring en herziening van integriteitsrisico's.

Inzichten uit de AFM-verkenning voor de monitoring en herziening van integriteitsrisico's

- De uitkomsten van de risico-identificatie, -analyse en -beheersing zijn door accountantsorganisaties niet altijd aantoonbaar vastgelegd. Dit bemoeilijkt de monitoring, herziening en daarmee ook de beheersing van integriteitrisico's. Daarom is dit een punt van aandacht voor accountantsorganisaties.

- Organisaties onderkennen dat het evalueren en periodiek toetsen van beheersmaatregelen hen in staat stelt om problemen in de beheersing tijdig te identificeren en te verbeteren. De AFM ziet dat in de praktijk weinig terug bij de geselecteerde accountantsorganisaties[4].

- Sommige accountantsorganisaties vinden het nuttig om in de SIRA een beschrijving op te nemen van (bijna) voorgedane incidenten en de impact hiervan. Dit vergroot de bewustwording en zorgt ervoor dat er beter van incidenten geleerd kan worden.

- Bij enkele accountantsorganisaties is de informatie uit de SIRA een onderdeel van de rapportage aan beleidsbepalers over mogelijke (integriteit)risico's die de organisatie loopt. Zij vinden dat de SIRA een goed hulpmiddel is bij het inventariseren, analyseren, beheersen en monitoren van integriteitsrisico's en waardevolle informatie oplevert voor de organisatie.

[4] De AFM heeft daarom geen 'good practices' geïdentificeerd voor deze stap.

Verantwoording

De good practices in dit document zijn praktijkvoorbeelden van specifieke niet-OOB accountantsorganisaties die uit de verkenning van de AFM zijn gebleken. Waar nodig zijn deze geanonimiseerd en herschreven. De good practices kunnen andere accountantsorganisaties helpen voor verdere verbetering en implementatie van de SIRA en de invulling van een aantoonbare integere en beheerste bedrijfsvoering. Alternatieve invullingen, passend bij de specifieke kenmerken van de desbetreffende accountantsorganisatie, zijn uiteraard ook mogelijk.

De tekst in dit document is met zorg samengesteld en is informatief van aard. U kunt er geen rechten aan ontlenen. Door besluiten op nationaal en internationaal niveau is het mogelijk dat de tekst niet langer actueel is wanneer u deze leest. De Autoriteit Financiële Markten (AFM) is niet aansprakelijk voor de eventuele gevolgen – zoals bijvoorbeeld geleden verlies of gederfde winst – ontstaan door acties ondernomen naar aanleiding van deze tekst.