

Reactieformulier

Consultatie NBA-handreiking 1153 - Frauderisicoanalyse

Consultatieperiode loopt tot en met 16 september 2024

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants



Instructies voor respondenten

We verzoeken u de consultatiereactie uiterlijk aan te leveren op **16 september 2024**.

Dit reactieformulier is bedoeld voor het geven van uw consultatiereactie op de concept NBA-handreiking 1153. Het gebruik van dit document zal de verzameling en analyse van consultatiereacties door de NBA vergemakkelijken.

U kunt reageren op alle vragen of alleen geselecteerde vragen. Om uw consultatiereactie zo goed mogelijk te kunnen behandelen, verzoeken we het volgende:

- Geef uw algemene reactie door middel van de 'drop-down' keuzemenu's.
- Geef de reden voor uw antwoorden bij de gedetailleerde reactie. Als u het niet eens bent met de voorstellen in de handreiking, geef dan uw specifieke redenen en specifieke suggesties aan voor het wijzigen van de handreiking.
- Benoem zo specifiek mogelijk waar uw consultatiereactie betrekking op heeft, bijvoorbeeld door te verwijzen naar specifieke paragrafen, voorbeelden of alinea's in de handreiking.
- Vermijd het invoegen van tabellen of tekstvakken in het formulier bij het geven van uw antwoorden op de consultatievragen, omdat dit de verzameling van de reacties zal bemoeilijken.
- **Dien uw opmerkingen in met behulp van dit formulier, zonder een begeleidende brief of een samenvatting van uw belangrijkste punten. Benoem in plaats daarvan eventuele belangrijke punten zoveel mogelijk in uw antwoorden op de vragen.**

Uw reactieformulier kunt u zenden naar: consultaties@nba.nl. De NBA vindt het belangrijk om transparant te zijn over de reacties die zij krijgt met betrekking tot voorgestelde regelgeving en toelichtingen daarop. Daarom vragen wij om bij indiening van uw reactie aan te geven of wij uw reactie wel of niet mogen publiceren op de website van de NBA.

Onderdeel A: Uw gegevens

Naam van uw organisatie (of uw naam als u een reactie indient in persoonlijke hoedanigheid)	BDO Audit & Assurance B.V.
Naam/namen van verantwoordelijke(n) voor deze indiening (of laat leeg als dit hetzelfde is als hierboven)	Karen Bastings (Partner Bureau Vaktechniek) en Pascal Belfroid (Lid MT Audit & Assurance)
Naam van contactpersoon voor deze reactie (of laat leeg als dit hetzelfde is als hierboven)	Karen Bastings
E-mailadres van contactpersoon	Karen.Bastings@bdo.nl

Onderdeel B: Antwoorden op de consultatievragen

Voor elke vraag, begint u met uw algemene antwoord op de vraag middels de keuzelijst. Geef uw gedetailleerde opmerkingen, indien van toepassing, daaronder bij de behorende sectie.

1. *Wat vindt u in het algemeen van de opzet en duidelijkheid van deze handreiking?*

Algemene reactie: Voldoende

Gedetailleerde reactie (indien van toepassing):

De handleiding is duidelijk qua tekst en de structuur voldoet. In zijn algemeenheid worden in de handreiking de relevante onderwerpen geraakt en zo herkennen wij deze binnen de controlepraktijk van BDO Audit & Assurance BV.

De leesbaarheid kan worden verbeterd. Het lijkt erop dat er soms later delen zijn toegevoegd, waardoor de handreiking niet altijd soepel leest en er veel verbindingswoorden zoals 'ook' gebruikt worden. Onze tekstsuggesties worden hierna in dit reactieformulier aangegeven.

2. *Wat vindt u van het samenvattende schema in afbeelding 2 op pagina 4?*

Algemene reactie: Voldoende

Gedetailleerde reactie (indien van toepassing):

Wij gaan er vanuit dat afbeelding 1 op pagina 4 wordt bedoeld ('fraud lens'). Wij hebben de volgende suggestie:

- Afbeelding 1 – pagina 4
Standaard 500 ontbreekt in de rechter benedenhoek. Op die plek staat 'evaluatie van controle-informatie'. Standaard 500 richt zich specifiek op de beoordeling van de betrouwbaarheid van ontvangen en gebruikte (controle) informatie die mede relevant is om daarmee onderkende frauderisico's voldoende te mitigeren.
- Bij Afbeelding 2 - pagina 6 hebben wij de volgende opmerking:
FRF wordt niet toegelicht, wij adviseren toe te lichten dat dit Fraude Risico Factoren betreft. Daarnaast worden 'orde van grootte' en impact in de handreiking door elkaar heen gebruikt. Gezien de Standaarden orde van grootte hanteren, adviseren wij deze term te gebruiken en consequent te hanteren.

3. *Is de toepassing van Standaard 240 en, meer specifiek, het door de accountant te volgen proces van de frauderisicoanalyse duidelijk uitgelegd?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

Het vertrekpunt van de frauderisicoanalyse betreft de weging van de inherente risico factoren (IRF's) en daarbij de relevante beweringen, kernmerken / gebeurtenissen, vatbaarheid voor manipulatie en de afweging kwalitatief / kwantitatief, dit zonder het meewegen van de relevante interne beheersingsmaatregelen (IB).

Paragraaf 2.1:

In paragraaf 2.1 wordt in de tweede alinea ingegaan op de interne beheersomgeving, onder andere door deze tekst: 'Ook verwerft de accountant inzicht in de interne beheersomgeving, het risico-

inschattingsproces van de entiteit en het proces van de entiteit om het interne beheersingssysteem te monitoren, het aanwezige informatiesysteem en communicatie en interne beheersingsactiviteiten., terwijl hieraan in 2.2 een paragraaf wordt gewijd. Wij adviseren een verwijzing naar paragraaf 2.2. op te nemen waar de IB nader wordt toegelicht of deze paragraaf te verplaatsen naar 2.2.

Paragraaf 2.2:

In paragraaf 2.2 missen wij een korte notitie omtrent soft controls, met daarbij verwijzing naar handreiking 1148 - soft controls. In de paragraaf staat reeds: *'Tekortkomingen in de interne beheersingsmaatregelen en -omgeving kunnen leiden tot frauderisicofactoren.'* Onze suggestie is om hieraan toe te voegen *'het ontbreken van het bestaan van soft-controls dient te worden meegewogen in de afweging van frauderisico's'*.

4. Verdiepende onderwerpen

a) *Is de uitwerking dat aanwezige maatregelen van interne beheersing binnen de entiteit geen positieve invloed hebben op de frauderisicoanalyse duidelijk (paragraaf 2.2)?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

Wij hebben de volgende suggestie voor een verduidelijking van paragraaf 2.2:

Opgenomen in de tekst staat: *'zo nee, dan speelt de interne beheersing in deze fase geen 'positieve' of 'compenserende' rol.'* Dit is naar onze mening verwarrend met het gevraagde van *'geen positieve invloed hebben op de frauderisicoanalyse'*. De tekst, door de dubbele ontkenning, kan nu worden geïnterpreteerd dat indien er wel een goede AO/IB is dat deze een positieve invloed kan hebben op de frauderisicoanalyse. Wij geven de suggestie om de tekst als volgt te formuleren (mede op basis van Standaard 315, A107): *Indien er sprake is van een in opzet adequate interne beheersing, heeft dit géén 'positieve' of compenserende invloed op de frauderisicoanalyse. Indien er sprake is van tekortkomingen in de opzet van de interne beheersing, kan dit wel een negatieve invloed hebben op de frauderisicoanalyse.*

b) *Is het onderscheid in frauduleuze financiële verslaggeving en oneigenlijke toe-eigening van activa duidelijk (paragraaf 2.3)?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

De tekst van de tweede en derde alinea van deze paragraaf geeft het onderscheid voldoende duidelijk aan. Dit onderscheid kan in brede kring ook als algemeen bekend worden verondersteld.

c) *Is de toelichting op de frauderisicofactoren duidelijk (hoofdstuk 3), inclusief de toelichting op de fraudedriehoek (paragraaf 3.3)?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

De uitleg over frauderisicofactoren is helder. Aanvullend hebben wij de volgende suggesties:

- In de uiteenzetting t.a.v. de gelegenheid wordt aandacht besteed aan de personen met specialisatie in bepaalde kennisgebieden. Er wordt hierover geschreven en afgesloten met de opmerking *'hoewel er geen actieve verplichting tot onderzoek is, is een professioneel-kritische*

houding geboden.' Graag zien wij hier verduidelijking wat (minimaal) wordt verwacht van ons als accountant en in het verlengde hiervan, welke vastleggingen hierbij verwacht worden. Dat zou kunnen gedaan worden middels een niet limitatieve uiteenzetting (suggesties – voorbeelden) bij voorkeur met verwijzing naar de van toepassing zijnde Standaarden. Een voorbeeld kan zijn: *'Standaard 240, bijlage 1 kan hierin een waardevol hulpmiddel zijn. Hier in staan voorbeelden van frauderisicofactoren genoemd per onderdeel van de fraudedriehoek. Hoewel deze voorbeelden uiteraard niet uitputtend zijn, kunnen deze waardevolle input leveren tijdens teamdiscussies. De gemaakte afwegingen worden vervolgens gedocumenteerd conform standaard 230. Een andere mogelijkheid is om de frauderisicofactoren in bijlage 1 in zijn geheel af te wegen en deze documentatie op te nemen in het controledossier.'*

- In dezelfde paragraaf worden social media berichten genoemd om aanvullende informatie te verkrijgen over de vaardigheden van medewerkers in sleutelposities. Hoewel wij het voorbeeld begrijpen, achten wij het toepassen hiervan sterk situationeel gebonden. Wij adviseren om 'social media berichten' te verwijderen en de volgende tekst op te nemen: *'Welke vaardigheden medewerkers op sleutelposities hebben kan blijken uit openbare bronnen waarin opleiding en ervaring vermeld staan'*. Wij hebben omtrent dit stuk eveneens nog een andere suggestie. Vanuit onder andere het verschenen rapport 'report to the nations 2024' van de ACFE blijkt dat 84% van de fraudeurs 'red flags' vertoonde in hun gedrag. We adviseren daarom om in de handreiking op te nemen dat er ook navraag wordt gedaan bij het management over hun maatregelen ten aanzien van het nagaan van de achtergrond en vaardigheden van medewerkers, zowel bij indiensttreding als gedurende hun dienstverband.

d) Is de evaluatie van frauderisicofactoren om te komen tot frauderisico's (hoofdstuk 4) duidelijk? En is de uitleg en het diagram in paragraaf 4.2 rondom het gebruik van het spectrum (waarschijnlijkheid x orde van grootte) duidelijk?

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

Paragraaf 4.1:

In de voorgenoemde paragraaf wordt gesteld *'De accountant moet de frauderisicofactoren evalueren en op basis van professionele oordeelsvorming nagaan of deze leiden tot een frauderisico. Hierbij kan één individuele frauderisicofactor (al) leiden tot een frauderisico.'* Vanuit de fraudedriehoek bezien (druk, gelegenheid, rationalisatie) is dit niet altijd juist. Er zijn altijd meerdere factoren die meespelen om tot een daadwerkelijke fraude te komen. Wij adviseren om een voorbeeld op te nemen om dit nader te verduidelijken. Hierbij hebben wij de volgende suggestie: *'De controller heeft de gelegenheid om te sturen met de cijfers. Echter is er geen sprake van een bonusstructuur of andere beloning in zijn voordeel, alsmede geen bankratio's waaraan moeten worden voldaan. In dit specifieke geval is er dus géén druk en/of rationalisatie om te sturen met cijfers. Vanuit de fraudedriehoek leidt deze mogelijkheid (FRF) dus ook niet tot een daadwerkelijk frauderisico.'*

Paragraaf 4.2:

In de handreiking staat: *'Het wordt aanbevolen om vast te leggen waarom een frauderisicofactor wel of niet resulteert in een frauderisico in het controledossier.'* Wij vinden dit vrijblijvend geformuleerd. Het vastleggen van overwegingen t.a.v. frauderisicofactoren en of deze vervolgens resulteren in een frauderisico is noodzakelijk (en in lijn met het rapport van de AFM – Scherper op frauderisico's). Wij begrijpen dat de handreiking niet verder kan gaan dan de Standaarden, maar we denken dat dit verduidelijkt kan worden. Dit maakt deel uit van de controledocumentatie (deze term is gedefinieerd in de HRA). Standaard 230.3 stelt dat controledocumentatie het opdrachtteam in staat stelt verantwoording af te leggen over zijn werkzaamheden. Verder staat in Standaard 230.8 dat een ervaren accountant die niet betrokken was bij de controle, inzicht moet kunnen krijgen in de uitkomsten van de

uitgevoerde controlewerkzaamheden. Dit kan alleen indien de overwegingen zijn vastgelegd. Wij bedoelen hier expliciet niet mee, dat je álle frauderisicofactoren moet afwegen, maar enkel deze die op de klant (specifiek) van toepassing zijn. Ons inziens is het logisch dat indien je frauderisicofactoren identificeert, je deze ook evalueert en dit documenteert in het controledossier.

e) *Wat vindt u van de toelichting op het veronderstelde frauderisico van doorbreking van de interne beheersing door het management (paragraaf 5.1)?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

De tekst is duidelijk geformuleerd, waarbij wij de volgende aanbeveling hebben:

De tabel onder 5.1 vermeldt verschillende factoren die óók relevant kunnen zijn voor de bepaling van materialiteit. In het kader van het proces is het van belang om opnieuw de materialiteitsoverwegingen nader te overwegen. Een toevoeging hieromtrent zien wij als een waardevolle aanvulling op deze richtlijn/paragraaf om het iteratieve proces van de (fraude)risico-inschatting te benadrukken. Wij hebben de suggestie om achter de laatste zin 'daarom is ... accountant vereist' het volgende toe te voegen: *In het kader van het iteratieve proces is het belangrijk om, indien er nieuwe frauderisicofactoren worden onderkend, te overwegen of de materialiteitsbepaling dient te worden herzien.*

f) *Wat vindt u van de toelichting op het veronderstelde frauderisico van de opbrengstverantwoording? Is de uiteenzetting van de hoofregel en de uitzondering (paragraaf 5.2) duidelijk?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

Niet van toepassing.

g) *Mist u nog andere onderwerpen waarop verdieping gewenst is? Zo ja, kunt u dit en de bijbehorende prioritering hiervan motiveren*

Algemene reactie: Ja

Gedetailleerde reactie (indien van toepassing):

In de handreiking wordt niet ingegaan op greenwashing wat zeker relevant gaat worden bij de werkzaamheden van de accountant bij de controle van ESG rapportages (en nu reeds het bestuursverslag). Het advies is om hieraan aandacht te besteden in de handreiking. Ons is bekend dat een brochure over ESG Fraude onderhanden is. Hiernaar kan wellicht worden verwezen.

5. Voorbeelden

a) *Zijn de voorbeelden (in de paragrafen 4.3, 4.4, 5.1 en 5.3) helder en illustratief?*

Algemene reactie: Duidelijk

Gedetailleerde reactie (indien van toepassing):

De gegeven voorbeelden zijn duidelijk en verhelderend. Hierbij hebben wij wel de navolgende suggesties:

Paragraaf 4.4 - Voorbeeld risico in betalingsorganisatie:

- Pagina 18 - De laatste alinea sluit af met 'rapporteert hierover in de management letter en/of het accountantsverslag'. In het begin van de handreiking wordt ook gesproken over de rapportering in de controleverklaring. Wij adviseren deze daarom ook hier toe te voegen, zeker omdat het voorbeeld benoemd dat op basis van de gegeven informatie een frauderisico is onderkend.

Paragraaf 5.1 – Tabel 1:

- Voorbeeld 6: het covenant in de frauderisicofactor wordt heel algemeen gehouden, terwijl de tendentie een duidelijk covenant beschrijft op bepaalde indicatoren van de jaarrekening. Wij adviseren het covenant in de gebeurtenis nader te duiden, zodat de tendentie een logisch gevolg hiervan is.

Paragraaf 5.3 – Voorbeeld 4:

- Hier staat opbrengst uit de verkoop van woningen (voorheen huurwoningen). Logisch is hier dat het voorheen huurwoningen zijn geweest. Aldus het voorstel dit tekstueel aanpassen naar: opbrengst uit de verkoop van huurwoningen.
- Gegeven is dat de corporatie 90% van haar opbrengsten genereert uit huuropbrengsten (waarschijnlijk inclusief opbrengst servicecontracten). Dat zou betekenen dat 10% uit verkoop komt, zoals beschreven zou dat regulier zijn. Wij onderkennen dat dit niet overeenkomstig is met de praktijk. De verkoopopbrengsten zijn over het algemeen regulier (heel) beperkt. Er kan sprake zijn van verkoop van (meerdere) complexen, bijv. bij taakoverdracht waarbij er dan sprake is van een incidenteel hoge verkoopopbrengst.
- Gegeven is: de corporatie kent een stabiel bestand aan huurwoningen. Met 100 aankopen en 500 verkopen betekent dit dat er sprake is van (relatief) zeer veel mutaties in het bezit. Dit kan, maar is niet zoals de algemene ervaring is in de praktijk.
- Gegeven is: verkoop van de 500 eenheden vindt plaats aan huurders en derden. Eerder in het voorbeeld is opgenomen dat er sprake was van voorheen huurwoningen. Dan verkoop aan huurders? Wie zijn derden, zijn dat andere corporaties (bijv. i.h.k.v. taakoverdracht) of commerciële vastgoed partijen? De partijen aan wie verkocht is, zijn relevant voor het afwegen van de frauderisicofactoren en daarmee de kwalificatie van het frauderisico.
- Gegeven is: Er zijn 1.000 woningen verduurzaamd, met als gevolg een tussentijdse huurverhoging. Dat kan, maar komt niet realistisch over. Wat is er dan verduurzaamd? In principe zal de corporatie de kosten van verduurzaming voor haar rekening nemen. Hierbij moet je denken aan isolatie maatregelen. Wanneer er sprake is van zonnepanelen, kan de corporatie besluiten om huurverhogingen door te voeren. Gangbaar is dit niet, omdat de woningcorporaties de energiebesparingen ten gunste laten komen van hun huurders (sociale huurwoningen).
- Gegeven is: Het verduurzamen van woningen doet inderdaad de score qua energielabel verbeteren. Het verkrijgen van een nieuw energie label is echter problematisch, omdat de bureaus die deze zouden moeten verstrekken een volle portefeuille hebben. Het uitvoeren van verduurzaming en het verkrijgen van nieuwe energie labels zal derhalve niet altijd samen op gaan. Veelal zie je in de praktijk dat corporaties daarom wachten met het aanvragen van een nieuw label totdat er een huurmutatie plaatsvindt en zij pas dan overgaan tot huurverhoging.

Paragraaf 5.3 – Voorbeeld 5:

- Het hanteren van een frauderisico bij de verkopen is logisch. Het is hierbij de vraag of er daadwerkelijk sprake zal zijn van een (materiële) stroom aan opbrengsten uit

projectontwikkeling. Veel meer zie je dat de projectontwikkeling gericht is op de realisatie van uitbreiding/vernieuwing van de portefeuille voor verhuur door de corporatie zelf. Daarbij kan, afgeleid, sprake zijn van een beperkte stroom aan verkopen; veelal nooit materieel in omvang. Wanneer, zoals in dit voorbeeld, de omvang ervan wel materieel is, dan kan inderdaad het frauderisico aanwezig zijn. Het is goed om daar in het voorbeeld een toevoeging over te maken. Wij adviseren om de volgende zin toe te voegen: *de verkoopstroom is materieel voor de woningcorporatie*. Dit kan worden toegevoegd onder 'evaluatie van de aard van de opbrengststromen/-transacties'

- Dit voorbeeld gaat specifiek in op woningcorporaties. Echter indien je het voorbeeld toepast op een profit organisatie met 'veel kleine, individuele transacties' waarbij sprake is van een homogene populatie, routinematig karakter en die voorspelbaar zijn, dient wel een risico inzake de opbrengstverantwoording te worden verondersteld. Om foutieve ontorechte toepassing te voorkomen, adviseren wij expliciet te verduidelijken hoe een woningcorporatie van een profit organisatie verschilt en daardoor dit voorbeeld niet kan worden toegepast.

Paragraaf 5.3 – Voorbeeld 6:

- Overall zouden wij eerder concluderen dat er rondom de opbrengsten verantwoording bij reguliere routinematige opbrengststromen uit rente en commissie geen sprake is van een verhoogd risico ten aanzien van opbrengstenverantwoording. Hoewel het voorbeeld aangeeft dat het om een complexe(re) berekening gaat, is dit in basis een regulier proces van de bank, en daarmee veelal niet complex. Dit mede gezien de deskundigheid van zowel de bank als de accountant. De frauderisico's verwachten wij alleen ten aanzien van de handmatige boekingen op deze routinematige opbrengsten stromen.
- Ten aanzien van stimulans/druk en dan de aspecten rondom bonussen en resultaat afhankelijke beloningen. Dat zijn veelal wel aspecten in onze praktijk die in overweging worden genomen. Suggestie is om deze incentive toe te voegen.
- In het voorbeeld ten aanzien van de renteopbrengsten staat vermeld dat er handmatige boekingen zijn betrokken bij de renteopbrengsten. Het is wat onwaarschijnlijk dat er bij een bank van enige omvang sprake is van handmatige boekingen op de renteopbrengsten. Het kan zijn dat het betrekking heeft op de overloop van renteopbrengsten maar dit staat wat ver af van de praktijk.
- Het proces van rente- en commissieopbrengsten is normaliter in praktijk een sterk geautomatiseerd proces, waarbij de interne beheersing met de automatiseringsomgeving de (minimale) basis is van de controle aanpak. Dit blijkt nu niet goed uit het beschreven risico, waardoor het onwaarschijnlijk is in de praktijk. Door het voorgaande t.a.v. voorbeeld 6 wordt de conclusie door ons niet gedeeld t.a.v. de kwalificatie ten aanzien van het risico van renteopbrengsten.
- Er wordt gesteld dat handmatige aanpassingen moeilijk te detecteren zijn. In het voorbeeld herkennen wij niet dat handmatige boekingen moeilijk te detecteren zijn (en waarom zou dat anders zijn bij commissieopbrengsten dan bij renteopbrengsten).
- Bij transactie fee is een link tussen de fee en de basis van de fee niet altijd goed te leggen in tegenstelling tot bij rente opbrengsten (namelijk op basis van de uitstaande lening en op basis van commissie opbrengsten op basis van uitstaand vermogen). De suggestie is om het ontbreken van dit verband toe te voegen.

- Bij het aspect druk zouden wij zeker bij overname fees de bonussen en resultaat afhankelijke beloningen terug laten komen. Zeker in deze tak is dat zeer gebruikelijk en daarmee een verhoogde stimulans / druk.

b) Kunt u aanvullende voorbeelden aanleveren die toezien op de verdiepende onderwerpen?

Algemene reactie: Nee

Gedetailleerde reactie (indien van toepassing):

De gegeven voorbeelden geven reeds diverse inzichten.

c) Kunt u voorbeelden aanleveren van hoe u uw cliënt heeft gestimuleerd een interne frauderisicoanalyse op te stellen, en hoe u deze analyse hebt gebruikt bij de uitvoering van uw eigen frauderisicoanalyse?

Algemene reactie: Ja

Gedetailleerde reactie (indien van toepassing):

BDO maakt gebruik van een compliance vragenlijst die bij alle controle opdrachten verplicht toegepast moet worden. Deze vragenlijst wordt besproken met cliënten op niveau van TCWG en andere functionarissen binnen de te controleren onderneming. Indien er sprake is van een interne frauderisicoanalyse wordt deze in de vragenlijst benoemd. Daarnaast is het inmiddels common practice dat gevraagd wordt om de intern uitgevoerde (fraude)risicoanalyse. Indien deze niet aanwezig is wordt dit gerapporteerd in de management letter en/of accountantsverslag en tevens (in de inleidende paragraaf) in de sectie 'controleaanpak frauderisico's' in de controleverklaring. Daardoor worden cliënten tevens gestimuleerd een eigen frauderisicoanalyse op te stellen.

6. Zijn de vereisten ten aanzien van het documenteren van de verschillende werkstappen in het proces van de frauderisicoanalyse voldoende duidelijk?

Algemene reactie: Onduidelijk

Gedetailleerde reactie (indien van toepassing):

Vanuit de handreiking en hierin het gevisualiseerde trechtermodel blijken de te volgen processtappen. Echter, niet nadrukkelijk blijkt uit deze handreiking hoe deze worden gedocumenteerd en wat de minimale verwachtingen daarbij zijn. Wij adviseren om nadrukkelijk in te gaan op de benodigde controledocumentatie zoals is opgenomen in Standaard 230. Zie hiervoor ook de beantwoording bij vraag D, paragraaf 4.2 alsmede vraag C.

7. Recent is de NBA-handreiking 1137 (corruptie, werkzaamheden van de accountant) geactualiseerd. Hierin wordt een link gelegd naar fraude en de frauderisicoanalyse. Is de uitwerking in deze NBA-handreiking 1153 volgens u voldoende duidelijk en consistent met de NBA-handreiking 1137?

Algemene reactie: Onduidelijk

Gedetailleerde reactie (indien van toepassing):

Corruptie wordt niet behandeld in deze handreiking. Wij vinden het belangrijk dat dit expliciet wordt benadrukt. Wij adviseren op pagina 5 onder 'opzet en afbakening' de volgende zin toe te voegen: *Deze*

handreiking gaat nadrukkelijk niet in op corruptie. Hiervoor is een aparte handreiking verschenen. Dit betreft handreiking 1137.

8. Heeft u nog andere adviezen en/of opmerkingen met betrekking tot de NBA-handreiking 1153?

Algemene reactie: Ja

Gedetailleerde reactie (indien van toepassing):

Wij hebben suggesties en opmerkingen die in de reactie op voorgaande vragen niet zijn genoemd. Deze hebben wij hieronder puntsgewijs opgenomen en zien vooral op tekstuele aanpassingen:

- Volledige handreiking: Graag aandacht voor consistente toepassing van 'dossier' versus 'controledossier'.
- Pagina 2 - Onderwerp: In deze NBA-handreiking wordt uitgelegd wat van de controlerende accountant verwacht wordt voor het doen van *een goede* frauderisicoanalyse. Suggestie om deze tekst aan te passen naar: *het doen van een frauderisicoanalyse zoals bedoeld in (onder andere) Standaard 240 en 315.*
- Pagina 4 & 5 - Introductie: in de notes wordt nog verwezen naar concept handreiking 1137, welke inmiddels definitief is, alsmede sommige notes die niet openbaar toegankelijk zijn. Wij adviseren deze na te lopen en up te daten.
- Pagina 4 - Introductie: *'Daarbij spelen diverse Standaarden uit de NV COS een rol.'* NV COS kan in deze zin weg, immers Standaarden zijn vermeld in de NV COS.
- Pagina 4 - Introductie: Fraudelens is naar onze mening geen algemeen bekend begrip en wordt in deze handreiking wel benoemd. Indien deze term gehanteerd blijft, adviseren wij om in het document een nadere uiteenzetting hieromtrent op te nemen (en niet alleen een verwijzing naar uitleg in een openbare bron).
- Pagina 6 - Introductie: in afbeelding 2 wordt aangegeven: Frauduleuze verslaggeving & oneigenlijke toe-eigening. Voorstel: Frauduleuze verslaggeving & oneigenlijke toe-eigening van activa.
- Pagina 6 - afbeelding 2: De term CBO staat nu genoemd, terwijl dit volgens de Standaarden 'initiële cijferanalyse' betreft. Wij adviseren de terminologie van de Standaarden te hanteren.
- Pagina 6 - afbeelding 2: IAD (Interne Accountants Dienst) staat in de Standaarden, maar is mogelijk geen algemeen bekende term. Wij adviseren deze afkorting toe te lichten.
- Pagina 6 – afbeelding 2: suggestie om te *'FR's niveau verantw. Als geheel'* te vervangen in *'FR's niveau van financiële overzichten'*, gezien deze term in de Standaard wordt gebruikt.
- Pagina 8 – Paragraaf 1.2: In deze paragraaf wordt ingegaan op mogelijke gedupeerden. Vanuit een (vrij recente) uitspraak van de accountantskamer wordt aangegeven dat individuele belangen niet onder de verantwoordelijkheid van de accountant vallen. In paragraaf 4.3 wordt dit nader toegelicht en verwezen naar deze uitspraak. Wij adviseren dit meteen in paragraaf 1.2 te verduidelijken.
- Pagina 8, paragraaf 2.1: In deze paragraaf is stellig opgenomen: *'Verder zal de accountant kennisnemen van de uitkomst van de door de entiteit zelf opgestelde frauderisicoanalyse'*.

Ervaring in de praktijk leert dat entiteiten nog niet altijd een eigen frauderisicoanalyse hebben gemaakt of dat de gemaakte frauderisicoanalyse nog niet aansluit op hetgeen daarvan verwacht kan worden. Dit hoeft niet alleen het geval te zijn bij kleinere entiteiten, maar kan ook het geval zijn bij grotere entiteiten, zeker met een DGA structuur en / of beperkingen t.a.v. toezichthouders, zoals geen RvC (TCWG). De accountant dient dan aanvullende werkzaamheden uit te voeren, zoals ook benoemd, zoals het (onder andere) inwinnen van inlichtingen. Daarom adviseren wij om dit te specificeren en aan te geven '*indien er sprake is van een zelf opgestelde frauderisicoanalyse*'. Het is evident dat er een goede fraudediscussie dient plaats te vinden met de cliënt op verschillende niveaus binnen de organisatie. Een specifieke toevoeging daarvan zouden we toejuichen. In dat kader kunnen bij de bespreking van de AO/IB (opzet) de volgende vragen worden gesteld bij medewerkers die bij de verschillende processen zijn betrokken:

- Wat zijn volgens jullie frauderisico indicatoren binnen het proces (druk, gelegenheid en rechtvaardiging uitwerken)?
- Is er fraude geweest, of zijn er vermoedens van fraude?
- Waar ziet de entiteit zelf mogelijkheden binnen het proces om fraude te kunnen plegen?

Voorgaande vragen staan los van de fraudebespreking met het management / TCWG.

- Pagina 11 - Paragraaf 2.3: De tekst onder het voorbeeld behandelt het ontvreemden van '*intellectueel eigendom, persoonsgegevens en bouwtekeningen*'. Wij adviseren om 'bouwtekeningen' niet op te nemen in de tekst. Deze kan namelijk ons inziens verwarring opleveren. Hoewel wij snappen dat dit bedoeld is voor bouwtekeningen bijvoorbeeld bij ASML, kan dit door iemand ook worden geïnterpreteerd als een simpele, niet materiele bouwtekening waardoor het doel van de tekst mogelijk niet wordt bereikt.
- Pagina 13 - paragraaf 2.5: de term *brainstormsessie* is geen term zoals die voorkomt in de Standaarden. Wij adviseren de terminologie gelijk te houden aan de Standaarden, zijnde '*bespreking opdrachtteam*'.
- Pagina 14 - Paragraaf 3.3: De term frauderisicofactoren wordt pas in de eerste alinea van hoofdstuk 3 uitgelegd, terwijl deze al meerdere keren in hoofdstuk 1 en 2 wordt genoemd. Het zou logischer zijn om deze eerder in de handleiding te definiëren.
- Pagina 14 - Paragraaf 3.3: De afbeelding van de fraudedriehoek kan qua lay-out verbeterd worden. Tevens adviseren wij de term '*vaardigheid*' onder gelegenheid aan te passen naar '*bekwaamheid*'.
- Pagina 15 - paragraaf 2.5: suggestie om toe te voegen: '*ondersteun de fraudediscussie met data-analyse in de planningsfase*'. Vermeld daarbij duidelijk dat deze data-analyse uitsluitend bedoeld is voor risico-inschattingswerkzaamheden en niet als vervanging dient voor werkzaamheden in de uitvoeringsfase, om te voorkomen dat frauderisico's ten onrechte worden afgeschaald in de planningsfase. Uit controlewerkzaamheden dient vervolgens te blijken of deze werkzaamheden hebben geresulteerd in voldoende en geschikte controle informatie t.a.v. het onderkende frauderisico. Relevant daarbij is dat de frauderisico's ook worden opgenomen in de controleverklaring.
- Pagina 17 - Paragraaf 4.3: in de laatste alinea van pagina 17 wordt gesproken over een '*omissie of zwakte*'. Volgens de Standaarden verwijst dit naar (significante) tekortkomingen. We adviseren de terminologie van de Standaarden te gebruiken en dit aan te passen.

- Pagina 18 - Paragraaf 4.4: Het *'touch and stay'* risico is een risico wat ons inziens niet een algemeen bekende term is. Graag een korte uiteenzetting toevoegen.
- Pagina 18 - Paragraaf 4.4: Wij kunnen zowel het *'touch and stay'* alsmede het *'hit-and-run'* risico plaatsen en dit is ons inziens ook terecht ingeschat. Wij adviseren de tekst na het antwoord iets te herzien en te verduidelijken dat er door dit risico altijd sprake is van zowel het *'touch and stay'* risico als het *'hit-and-run'* risico.
- Pagina 18 - Paragraaf 4.4: In het voorbeeld staat vermeld: 'Op basis van het inzicht in het betalingsproces blijkt dat de controller in staat is de bankrekeningnummers van crediteuren aan te passen op de betaaladvieslijst nádat de DGA de betalingen heeft geautoriseerd.' Wij adviseren om dit voorbeeld te verduidelijken met *'nadat de DGA de betaaladvieslijst heeft geautoriseerd.'*
- Pagina 20 - Paragraaf 5.1 - Voorbeeld 8: hier wordt in de kolom *'mogelijk frauderisico'* terugverwezen naar voorbeeld 2. Dit sluit echter niet geheel aan op voorbeeld 8. *'Het doorvoeren van afwaarderingen door een te negatieve inschatting van de waardering van activa'* heeft ons inziens niks te maken met *'het niet besteden van een subsidie in het boekjaar.'* Wij adviseren niet terug te verwijzen, maar per frauderisicofactor de 'hoe en waar managementfraude' toe te lichten.
- Pagina 24 – Paragraaf 5.2, voorbeeld 2 retailer: er is onterecht een ')' toegevoegd na 'additionele' in de eerste paragraaf van het voorbeeld.
- Pagina 27 & 28 - Voorbeeld 6: In het voorbeeld ten aanzien van de renteopbrengsten staat vermeld dat *'vooraf kan niet geen rekening worden gehouden met de effectieve werking'*. Het woordje *'niet'* zal hier moeten vervallen.