Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

NBA Notitie

Best practices frauderisicobeheersing voor bestuurders en toezichthouders

1 juli 2021

Ter afstemming met:
- Stakeholders
- NBA bestuur
- Stuurgroep Publiek belang
- NBA ledengroepen
- NBA Sectorcommissies

Opgesteld door NBA Werkgroep Fraude
fraude@nba.nl

Inhoud

Samenvatting

Hoe geeft u als bestuurder van een organisatie concreet invulling aan frauderisicobeheersing? Hoe zorgt u ervoor dat fraude tijdig wordt ontdekt en in de kiem wordt gesmoord? Met deze best practices kunnen bestuurders en commissarissen van organisaties invulling geven aan risicobeheersing, preventie en detectie van fraude en corruptie. De best practices zijn opgesteld door de Werkgroep Fraude van de NBA, waarbij input is verkregen van een groot aantal belangenorganisaties van bestuurders, toezichthouders, aandeelhouders, grote en kleine ondernemingen en non-profitorganisaties. De best practices zijn als volgt:

1. Het bestuur heeft **integriteit van ondernemen** en **eerlijk zaken doen** als basis, vervult hierin een voorbeeldrol voor haar werknemers en draagt dit uit (**'tone-at-the-top'**). Het bestuur bevordert een **open cultuur**, waarin ruimte is voor het melden van misstanden. Het bestuur draagt zorg voor een **interne gedragscode**, draagt dit actief uit en bespreekt dit met de werknemers en hanteert een **zerotolerance beleid ten aanzien van bewuste niet-naleving van wet- en regelgeving**.

2. Het bestuur ontwikkelt normen en waarden ten aanzien van het **mitigeren van corruptierisico's** in zakelijke relaties met klanten, leveranciers en tussenpersonen, **inclusief richtlijnen voor het accepteren en geven van geschenken**, nevenactiviteiten, **belangenverstrengeling**, representatie en sponsoring. Daarbij is voorts beleid en meldplicht bij nauwe of langdurige relaties tussen bestuursleden en/of werknemers met klanten, leveranciers of tussenpersonen. **Bij het aangaan van een zakelijke relatie vindt een screening plaats.**

3. Het bestuur draagt zorg voor een **adequaat systeem van inschatting van fraude- en corruptierisico's**, alsmede **interne beheersingsmaatregelen** die deze risico's mitigeren. Voorts stelt het bestuur periodiek **de effectieve werking** van deze beheersingsmaatregelen vast en evalueert het periodiek de **fraude risico inschatting** met gebruikmaking van de **fraudedriehoek.**

4. Het bestuur faciliteert **voldoende tegenspraak** binnen het bestuur en vanuit de organisatie door zorg te dragen voor voldoende **diversiteit** binnen bestuur, management en toezichthoudend orgaan, **laat zich gevraagd en ongevraagd adviseren** en zorgt voor **voldoende gelegenheid tot inspraak van werknemers.**

5. Het bestuur bevordert een cultuur waarin **aandacht is voor het functioneren, de prestaties en gelijke behandeling van werknemers** en een marktconform beloningsbeleid wordt gehanteerd. **Medewerkerstevredenheid** wordt periodiek en anoniem gemeten en de uitkomsten worden opgevolgd.

6. Het bestuur waarborgt een veilige omgeving waarin **werknemers, klanten, leveranciers en andere stakeholders worden gestimuleerd problemen of misstanden te melden** of bespreekbaar te maken bij een (fraude)meldpunt, met bescherming van (de anonimiteit van) melders of klokkenluiders, communiceert haar klokkenluidersregeling aan alle relevante partijen en draagt zorg voor **adequate opvolging van meldingen.**

7. Het bestuur verleent haar **volledige medewerking aan** de uitvoering van werkzaamheden door **de accountant**, verschaft proactief alle informatie en **laat de accountant jaarlijks één of meerdere door het bestuur onderkende frauderisico's nader onderzoeken.** Voorts meldt het bestuur zo vroeg mogelijk eventuele misstanden aan de accountant en faciliteert een directe lijn tussen ondernemingsraad, toezichthoudend orgaan en de accountant.

8. Het bestuur draagt periodiek zorg voor **trainingen fraudebewustzijn** voor alle medewerkers inclusief bestuurders, afgestemd op de aard, omvang en complexiteit van de organisatie en onderstreept en communiceert het **belang van fraudebewustzijn, inclusief** de risico's van **cyberfraude.**

9. Het bestuur draagt zorg voor een **zorgvuldig proces van schattingen in de jaarrekening**, laat het schattingsproces en de uitkomsten toetsen door zowel de accountant als het toezichthoudend orgaan en draagt zorg voor een **adequate administratie** en adequaat proces van het opmaken van de jaarrekening.

10. Het bestuur hanteert een **realistisch en passend beloningsbeleid, waarin prikkels die leiden tot ongewenst gedrag worden voorkomen** en waarbij het beloningsbeleid wordt betrokken in de fraude risico inschatting.

11. Het bestuur **handelt adequaat en voortvarend bij een vermoeden van fraude of niet-naleving van wet- en regelgeving en stelt vooraf een fraude respons plan op**, om voorbereid te zijn op de vraag hoe te handelen bij voorbereid te zijn op de vraag hoe te handelen bij een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues. **Aanbevelingen voor een door de organisatie op te stellen fraude respons plan hiervoor zijn in bijlage 1 van deze best practices opgenomen.**

Het toezichthoudend orgaan van de organisatie ziet actief toe op de daadwerkelijk uitvoering van de hiervoor genoemde best practices en levert waar nodig en waar mogelijk hiertoe zelf ook een inhoudelijke bijdrage. In de nadere uitwerking van de best practices in dit document worden puntsgewijs de actiepunten voor zowel het bestuur als het toezichthoudend orgaan concreet benoemd.

Inleiding

Hoe geeft u als bestuurder van een organisatie concreet invulling aan frauderisicobeheersing? Hoe zorgt u ervoor dat fraude of corruptie tijdig wordt ontdekt en in de kiem wordt gesmoord? Welke acties neemt u als bestuurder, als u wordt geconfronteerd met ernstige vermoeden van fraude of corruptie die serieuze impact heeft op de organisatie?

Welke rol speelt u als commissaris als het gaat om frauderisicobeheersing? Hoe weet u dat het bestuur de fraude- en corruptierisico's beheerst? Hoe stelt u vast dat het bestuur zelf niet fraudeert? En als het bestuur zich daaraan schuldig maakt, welk stappenplan volgt u dan, als (lid van) het toezichthoudend orgaan van de organisatie?

Het zijn relevante vragen voor elke bestuurder en commissaris. Uiteraard in het belang van de organisatie, maar ook omdat het voortvloeit uit de wettelijke verplichting in brede zin van bestuurders die tegenover de organisatie gehouden zijn tot een behoorlijke vervulling van hun taken. En uit de wettelijke verplichting van commissarissen, om in het belang van de organisatie toezicht te houden op het beleid van het bestuur. Verder is het opmaken van een getrouwe jaarrekening een wettelijke verplichting van het bestuur.

Het beheersen van risico's is één van de pijlers van goed bestuur en toezicht, en dit geldt uiteraard ook voor frauderisico's. Maar hoe dan?

De in deze notitie opgenomen concrete en brede set aan ‘best practices’ is behulpzaam voor (bestuurders en commissarissen van) organisaties in het kader van het voorkomen van fraude en corruptie en het beheersen van fraude- en corruptierisico’s. Organisaties kunnen deze ‘best practices’ toepassen op een wijze die het best past bij de desbetreffende organisatie en haar omgeving.

Voorts bevatten deze ‘best practices’ concrete aanbevelingen voor een door ondernemingen en organisaties op te stellen fraude response plan (bijlage 1). Een dergelijk plan beoogt in feite een leidraad of spoorboekje te zijn voor hoe het bestuur en het toezichthoudend orgaan dient te handelen bij vermoeden van fraude. Een fraude response plan stelt een organisatie in staat om adequaat en voortvarend te handelen om schade voor de organisatie, in welke vorm dan ook, zoveel mogelijk te beperken.

Deze best practices, die zijn uitgewerkt door de werkgroep fraude van de Nederlandse Beroepsorganisatie van Accountants, zijn met input van vele belangenorganisaties en (oud) bestuurders en commissarissen tot stand gekomen. Het document kent een ‘top down’ structuur, met een samenvatting, een verdiepende uitwerking per ‘best practice’ en bijlagen, waaronder de aanwijzingen voor een door de organisatie op te stellen fraude response plan. Benadrukt wordt dat de ‘best practices’ voor elke organisatie(grootte) relevant zijn, maar wel specifiek dienen te worden toegepast, rekening houdend met de complexiteit en omvang van de desbetreffende organisatie. Als concreet voorbeeld geldt dat best practices voor het toezichthoudend orgaan niet van toepassing zullen zijn voor organisaties die geen raad van commissarissen of soortgelijk toezichthoudend orgaan kennen. Het kan daarbij wel relevant zijn om voor dergelijke organisaties te bezien of de in de ‘best practices’ uitgewerkte aspecten voor commissarissen op een andere wijze of door een ander orgaan kunnen worden ingevuld.

Best practices frauderisicobeheersing voor bestuurders en toezichthouders

1. Tone at the top, cultuur en gedrag, inclusief interne gedragscode

Het bestuur:	Het toezichthoudend orgaan:
• toont een voorbeeldrol richting haar werknemers, handelt hiernaar en bevordert een open cultuur; • bevordert openheid, tegenspraak, acceptatie van fouten, eerlijk handelen en integere bedrijfsvoering; • draagt zorg voor voldoende diversiteit binnen het bestuur en toezichthoudend orgaan en een evenwichtige verdeling van taken, bevoegdheden en besluitvorming; • draagt zorg voor een interne gedragscode, die wordt gecommuniceerd aan werknemers, met frequente herhaling van communicatie, waarin duidelijk wordt gemaakt dat frauduleus en/of bewust onwettig handelen, financieel economische criminaliteit en (bewuste) overtredingen van wet- en regelgeving niet wordt getolereerd en zal leiden tot sancties; • bewaakt de naleving van de interne gedragscode; • bewaakt dat werknemers zich blijven herkennen in de 'tone at the top', en gaat daarover in gesprek met werknemers en met de leidinggevenden; • neemt haar beslissingen op basis van normen en waarden, vanuit haar interne gedragscode en richtlijnen vanuit de sector/branche; • maakt publiek op welke wijze zij haar bestuur van de organisatie heeft ingericht; • agendeert frequent (en tenminste eenmaal per jaar) de evaluatie van de integere bedrijfsvoering, naleving wet- en regelgeving en ethisch handelen; • creëert in haar benaderingswijze een dusdanige open sfeer dat werknemers zich gesteund en gestimuleerd voelen in vrijheid en zonder (nadelige) consequenties hun ervaringen te delen en (vermoedens van) onregelmatigheden of misstanden te melden.	• toont een voorbeeldrol richting het bestuur, handelt hiernaar en bevordert een open cultuur; • ziet toe op openheid, tegenspraak, acceptatie van fouten, eerlijk handelen en integere bedrijfsvoering; • monitort het bestaan van voldoende diversiteit binnen het bestuur en toezichthoudend orgaan en een evenwichtige verdeling van taken, bevoegdheden en besluitvorming; • houdt toezicht op de naleving van de interne gedragscode en adviseert aan het bestuur over de inhoud; • stelt voorts vast dat bestuurders en toezichthouders, zich houden aan de interne gedragscode en richtlijnen vanuit de sector/branche; • is alert op dominantie van individuele bestuurders en toezichthouders en neemt maatregelen in dat kader indien nodig; • onderhoudt contact met de bestuurders én met de leidinggevenden én bijvoorbeeld ook met de ondernemingsraad; • bespreekt met het bestuur de uitkomsten van gesprekken met werknemers en met de leidinggevenden over de heersende cultuur en naleving van de interne gedragscode en richtlijnen vanuit de sector/branche, met waarborg van anonimiteit; • bespreekt met de accountant de cultuur, het anti-corruptiebeleid en de interne beheersingsmaatregelen.

2. Anti-corruptie maatregelen en afspraken met klanten en leveranciers

Het bestuur:	Het toezichthoudend orgaan:
• ontwikkelt als onderdeel van haar interne gedragscode, waarden en normen en eisen gericht op het mitigeren van corruptierisico's in haar contracten met klanten, leveranciers en tussenpersonen/agenten; • ontwikkelt als onderdeel van de interne gedragscode, beleid en meldplichten ten aanzien van nauwe/langdurige relaties tussen werknemers/bestuursleden met klanten, leveranciers en tussenpersonen/agenten; • stelt voorafgaand aan het aangaan van een klant- of leveranciersrelatie een screening of “due diligence” onderzoek in; Bijvoorbeeld is de persoon met wie ik een overeenkomst afsluit de persoon, die hij zegt dat hij is en komen de bankrekeningen en de factuurgegevens overeen met wat ik over deze persoon kan vinden op bijvoorbeeld internet, KvK etc.; • ontwikkelt als onderdeel van de interne gedragscode, richtlijnen voor de organisatie ten aanzien van accepteren/geven van relatiegeschenken, nevenactiviteiten, belangenverstrengeling, representatie en sponsoring; • draagt zorg voor de naleving van de interne gedragscode en richtlijnen vanuit de sector/branche en rapporteert hierover aan het toezichthoudend orgaan.	• houdt toezicht op de naleving van de interne gedragscode met waarden en normen en eisen gericht op het mitigeren van corruptierisico's in de contracten van de organisatie met klanten, leveranciers en tussenpersonen/agenten; • houdt toezicht op de naleving van het beleid en de meldplichten ten aanzien van nauwe/langdurige relaties tussen werknemers/bestuursleden met klanten, leveranciers en tussenpersonen/agenten; • houdt toezicht op de naleving van de richtlijnen voor de organisatie ten aanzien van accepteren/geven van relatiegeschenken, nevenactiviteiten, belangenverstrengeling, representatie en sponsoring; • houdt toezicht op de naleving van de interne gedragscode en richtlijnen vanuit de sector/branche en neemt kennis van de rapportage hierover door het bestuur.

3. Interne beheersing

Het bestuur:	Het toezichthoudend orgaan:
• draagt zorg voor een adequaat systeem van inschatting van fraude- en corruptierisico's (fraude risicomanagement systeem); • draagt zorg voor interne beheersingsmaatregelen gericht op het wegnemen dan wel tot een aanvaardbaar niveau mitigeren van frauderisico's (ter voorkoming en detectie van fraude en corruptie); • stelt periodiek de effectieve werking van de interne beheersingsmaatregelen vast en laat zich hierover door de accountant informeren en adviseren; • rapporteert periodiek over de effectieve werking van de interne beheersingsmaatregelen (en incidenten) en geeft opvolging aan de actiepunten uit de rapportage; • voert periodiek een frauderisico-inschatting uit, waarbij nadrukkelijk de fraudedriehoek wordt betrokken bij het inschatten van frauderisico's. **Voorbeelden hiervan zijn in bijlage 2 beschreven;** • informeert het toezichthoudend orgaan over de inschatting van de algemene frauderisico's en de specifieke frauderisico's die samenhangen met doorbreking van de interne beheersings-maatregelen door bestuurders en betrekt het toezichthoudend orgaan bij de maatregelen, die de hiermee samenhangende frauderisico's wegnemen dan wel tot een aanvaardbaar niveau mitigeren; • informeert de accountant jaarlijks over de uitkomsten van de inschatting door het bestuur van frauderisico's en de geïmplementeerde interne beheersingsmaatregelen.	• ziet toe op het door het bestuur ontwikkelde systeem van inschatting van fraude- en corruptierisico's (fraude risicomanagement systeem; • betrekt in haar toezicht informatie vanuit andere afdelingen van de organisatie, bijvoorbeeld informatie van de afdeling P&O en HR over werknemersverloop, ziekteverzuim en ontslagen, , alsmede informatie over langdurige inkoop- en verkooprelaties; • stelt op basis van de periodieke rapportage door het bestuur, de effectieve werking van de interne beheersingsmaatregelen (en incidenten) vast en laat zich hierover door de accountant inlichten en adviseren. En ziet erop toe dat er opvolging wordt gegeven aan de actiepunten uit de rapportages; • neemt middels een vertegenwoordiger vanuit het toezichthoudend orgaan (of audit commissie) deel aan de periodieke frauderisico-inschattingen; • houdt toezicht op de interne beheersingsmaatregelen gericht op het wegnemen dan wel tot een aanvaardbaar niveau mitigeren van frauderisico's (ter voorkoming en op de detectie van fraude en corruptie), waarbij in het bijzonder aandacht uitgaat naar de frauderisico's die samenhangen met doorbreking van de interne beheersingsmaatregelen door bestuurders; • neemt kennis van bevindingen met betrekking tot fraude en frauderisico's gerapporteerd door belangrijke organisatie onderdelen, zoals risk management, legal, compliance en internal auditor. In het bijzonder gaat daarbij de aandacht uit naar de frauderisico's, die samenhangen met doorbreking van de interne beheersingsmaatregelen door bestuurders.

4. Voldoende tegenspraak binnen bestuur en vanuit organisatie

Het bestuur:	Het toezichthoudend orgaan:
• draagt zorg voor voldoende diversiteit binnen het bestuur, management en toezichthoudend orgaan en een evenwichtige verdeling van taken, bevoegdheden en besluitvorming, waarbij ingrijpende besluiten goedkeuring behoeven van alle bestuursleden (unanimiteit) en/of het toezichthoudend orgaan; • stelt vast dat belangrijke organisatie onderdelen, zoals risk management, legal, compliance en de internal auditor in staat zijn (onafhankelijke) assessments uit te voeren en advies te geven bij ingrijpende besluiten; • neemt kennis van de adviezen van werknemers in belangrijke posities, en geeft aan wat zij hiermee heeft gedaan in haar besluitvorming; • zorgt voor voldoende inspraakmogelijkheden vanuit de werknemers, zoals door het instellen van een ondernemingsraad of personeelsvereniging.	• houdt toezicht op het bestaan van voldoende diversiteit binnen het bestuur, management en toezichthoudend orgaan en een evenwichtige verdeling van taken, bevoegdheden en besluitvorming, waarbij ingrijpende besluiten goedkeuring behoeven van alle bestuursleden (unanimiteit) en/of het toezichthoudend orgaan; • ziet erop toe dat belangrijke organisatie onderdelen, zoals risk management, legal, compliance en internal auditor (indien aanwezig) door het bestuur in staat worden gesteld (onafhankelijke) assessments uit te voeren en advies te geven bij ingrijpende besluiten; • ziet erop toe dat belangrijke organisatie onderdelen, zoals risk management, legal, compliance en de internal auditor (indien aanwezig) het toezichthoudend orgaan kunnen informeren zonder tussenkomst van bestuur; • neemt kennis van de adviezen van werknemers in belangrijke posities en de besluitvorming van het bestuur, en geeft aan wat zij hiermee heeft gedaan in haar toezicht.

5. Aandacht voor werknemers en bestuursleden

Het bestuur:	Het toezichthoudend orgaan:
• toont een voorbeeldrol richting haar werknemers en handelt hiernaar en bevordert een open cultuur; • draagt zorg voor een open cultuur, waarin aandacht is voor het functioneren en de prestaties van alle werknemers; • draagt zorg voor een zichtbare en benaderbare vertrouwenspersoon, die onder meer werknemers kan opvangen, begeleiden en ondersteunen, voorvallen analyseert en werknemers hierover adviseert en ook kan verwijzen naar professionele hulpverleners; • behandelt werknemers gelijk en draagt zorg voor een marktconform beloningsbeleid; • voert een achtergrondonderzoek van werknemers, bestuurders en toezichthouders uit, voordat er een relatie met de organisatie wordt aangegaan; • stelt zich (rekening houdend met de privacywetgeving) op de hoogte van persoonlijke omstandigheden van werknemers; • verkrijgt (rekening houdend met de privacywetgeving) inzicht in persoonlijke omstandigheden van werknemers die tot druk zouden kunnen leiden om fraude te plegen, (zoals onder meer verslavingen of financiële problemen) en betrekt dit in de frauderisico-inschatting; • biedt waar mogelijk en/of gewenst, hulp aan werknemers bij moeilijke persoonlijke omstandigheden; • waarborgt altijd een veilige omgeving, door het bieden en realiseren van de bescherming en anonimiteit aan de fraudemelders en klokkenluiders. • faciliteert periodiek een (extern gefaciliteerd) anoniem medewerkers tevredenheidsonderzoek (MTO), waarbij het de vergelijkbaarheid met de uitkomsten van eerder MTO's worden meegewogen; • besteedt in het MTO aandacht aan aanknopingspunten voor frauderisicobeheersing, zoals bijvoorbeeld veilige werkomgeving, cultuurperceptie, bekendheid met het meldpunt, inschatting frauderisico's door werknemers, werkdruk en ontevredenheid; • bespreekt de uitkomsten van het MTO en beoordeelt of, en zo ja, welke acties	• bewaakt dat het bestuur zorg draagt voor een open cultuur, waarin aandacht is voor het functioneren en de prestaties van alle werknemers; • ziet er op toe dat er een zichtbare en benaderbare vertrouwenspersoon aanwezig is binnen de organisatie, die onafhankelijk kan functioneren; • monitort dat werknemers en bestuursleden gelijk worden behandeld en er sprake is van een marktconform beloningsbeleid; • ziet erop toe dat een achtergrondonderzoek van werknemers, bestuurders en toezichthouders wordt uitgevoerd, voordat er een relatie met de organisatie wordt aangegaan; • laat zich (rekening houdend met de privacywetgeving) door het bestuur op de hoogte stellen van persoonlijke omstandigheden van werknemers ; • verkrijgt (rekening houdend met de privacywetgeving) inzicht in persoonlijke omstandigheden van bestuursleden die tot druk zouden kunnen leiden om fraude te plegen, zoals verslavingen of financiële problemen; • biedt waar mogelijk en/of gewenst, hulp aan bestuursleden bij moeilijke persoonlijke omstandigheden. • verkrijgt de uitkomsten van het anonieme medewerkers tevredenheidsonderzoek (MTO) van het bestuur en bespreekt en welke acties moeten worden genomen op deze uitkomsten met het bestuur; • adviseert het bestuur over acties op basis van de uitkomsten van het MTO en monitort de uitvoering daarvan.

moeten worden genomen op deze uitkomsten; • verstrekt opzet en de geanonimiseerde uitkomsten en de (voorgenomen) acties van het MTO aan de accountant en het toezichthoudend orgaan.	

6. Fraudemeldpunt en klokkenluidersregeling

Het bestuur:	Het toezichthoudend orgaan:
• draagt zorg voor een fraudemeldpunt en klokkenluidersregeling; • communiceert het bestaan van het fraudemeldpunt en de klokkenluidersregeling aan werknemers, klanten, leveranciers en eventuele derden, door publicatie op de website, opname in algemene voorwaarden en/of standaard tekst in contracten of orders; • waarborgt altijd een veilige omgeving, door het bieden en realiseren middel van de bescherming en anonimiteit aan de fraudemelders en klokkenluiders; • faciliteert dat de door het fraudemeldpunt en klokkenluidersregeling ontvangen meldingen en de resultaten van onderzoeken en (voor)genomen vervolgstappen tijdig worden gerapporteerd aan (de audit auditcommissie van) het toezichthoudend orgaan en aan accountant; • geeft opvolging aan de (voor)genomen vervolgstappen vanuit de fraudemeldingen en klokkenluidersmeldingen; • trekt lering uit fraudemeldingen en meldingen vanuit de klokkenluidersregeling en voorkomt herhaling.	• houdt toezicht op het bestaan en de werking van een fraudemeldpunt en klokkenluidersregeling; • houdt toezicht een veilige omgeving, door middel van bescherming en anonimiteit van de fraudemelders en klokkenluiders; • ziet erop toe dat de door het fraudemeldpunt en klokkenluidersregeling ontvangen meldingen en de resultaten van onderzoeken (voor)genomen vervolgstappen tijdig worden gerapporteerd aan rapporteren aan (de auditcommissie van) het toezichthoudend orgaan en aan de accountant; • ziet toe op de opvolging van de (voor)genomen vervolgstappen vanuit de fraudemeldingen en klokkenluidersmeldingen; • trekt lering uit fraudemeldingen en meldingen vanuit de klokkenluidersregelingen en ziet toe op het voorkomen van herhaling.

7. Contact met en medewerking aan de accountant

Het bestuur:	Het toezichthoudend orgaan:
• faciliteert direct contact tussen de ondernemingsraad, de accountant en het toezichthoudend orgaan; • stelt de ondernemingsraad in staat om zelfstandig en zonder inmenging van het bestuur aangelegenheden met de accountant en/of toezichthoudend orgaan te bespreken; • bevordert een open relatie met de accountant, waarin alle aangelegenheden, inclusief gevoelige zaken zoals, een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues met de accountant worden besproken; • communiceert actief met de accountant en verschaft de accountant volledig inzicht in de organisatiestructuur, juridische structuur, uiteindelijk belanghebbende, activiteiten en eventuele issues in verleden en heden ten aanzien van de integriteit van het bestuur; • besteed in het bestuursverslag aandacht aan de aard, de omvang en het aantal fraude incidenten en de fraude respons hierop; • verleent haar volledige medewerking aan de uitvoering van de werkzaamheden door de accountant; • verschaft proactief toegang tot alle informatie die relevant is voor het opmaken en de controle van de jaarrekening, zoals de vastleggingen, documentatie en andere aangelegenheden; • verstrekt alle aanvullende informatie, die de accountant vraagt voor het doel van de werkzaamheden; • verleent aan de accountant onbeperkt toegang tot personen binnen de organisatie die relevant zijn voor de uitvoering van de werkzaamheden; • geeft haar actieve rol in de beheersing van frauderisico's onder meer vorm door jaarlijks één of meerdere onderkende frauderisico's (en indien van toepassing de interne beheersingsmaatregelen die zijn genomen om deze frauderisico's weg te nemen dan wel tot een aanvaardbaar niveau te mitigeren)', nader te laten onderzoeken door de accountant of een gespecialiseerde (fraude)onderzoeker. Een voorbeeld hiervan is gerichte data-analyse ter identificatie van	• ziet toe op het direct contact tussen de ondernemingsraad, de accountant en het toezichthoudend orgaan zelf; • stelt de ondernemingsraad in staat om zelfstandig en zonder inmenging van het bestuur aangelegenheden met de accountant en/of toezichthoudend orgaan te bespreken; • kan in alle vrijheid contact opnemen met de accountant, zonder inmenging van het bestuur, om openlijk met de accountant te spreken; • bevordert een open relatie met de accountant, waarin alle aangelegenheden, inclusief gevoelige zaken zoals, een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues, worden besproken; • ziet erop toe dat in het bestuursverslag aandacht is besteed aan de aard, de omvang en het aantal fraude incidenten en de fraude respons hierop; • geeft (vanuit de auditcommissie) aanbevelingen voor de benoeming van de externe accountant; • houdt toezicht op het bestuur in haar contact met en medewerking aan de accountant; • plant in overleg met het bestuur, de accountant tenminste éénmaal per jaar de vergadering (van de auditcommissie), om daarin verslag te doen van de bevindingen ten aanzien van de jaarrekeningcontrole, inclusief de werking van interne beheersingsmaatregelen; • bespreekt de uitkomsten van haar toezicht op het door het bestuur gehanteerde fraude risicomanagement, inclusief de inschatting van frauderisico's met de accountant; • neemt kennis van de door de accountant gerapporteerde bevindingen, waaronder bevindingen met betrekking tot fraude en frauderisico's. In het bijzonder gaat daarbij de aandacht uit naar de frauderisico's, die samenhangen met doorbreking van de interne beheersingsmaatregelen door bestuurders; • bewaakt de follow-up door het bestuur van de door de accountant gerapporteerde bevindingen, waaronder bevindingen met betrekking tot fraude en frauderisico's;

ongebruikelijke financiële transacties die kunnen wijzen op fraude; • meldt een vermoeden van fraude in een zo vroeg mogelijk stadium aan accountant en toezichthoudend orgaan en houdt deze betrokken bij de vervolgstappen; • plant in overleg met het toezichthoudend orgaan en de accountant tenminste éénmaal per jaar de vergadering van de auditcommissie, om daarin verslag te doen van de bevindingen ten aanzien van de jaarrekeningcontrole, inclusief de werking van interne beheersingsmaatregelen; • neemt kennis van de door accountant gerapporteerde bevindingen waaronder bevindingen met betrekking tot fraude en frauderisico's; • geeft follow-up aan de door de accountant gerapporteerde bevindingen waaronder bevindingen met betrekking tot fraude en frauderisico's.	• faciliteert direct contact tussen de auditcommissie en de accountant. Waarbij de accountant naast verantwoording aan het bestuur ook verantwoording aflegt aan het toezichthoudend orgaan.

8. Fraudebewustzijn

Het bestuur:	Het toezichthoudend orgaan:
• draagt zorg voor periodieke trainingen fraudebewustzijn voor haar werknemers en bestuurders. Deze training dient passend te zijn bij de aard, omvang en complexiteit van de organisatie en onderstreept en communiceert het belang van fraudebewustzijn, inclusief de risico's van cyberfraude; • baseert de inhoud van de training fraudebewustzijn op de resultaten van een frauderisicobeoordeling; • stelt vast dat de training fraudebewustzijn wordt afgestemd op de behoeften van de afzonderlijke functies binnen de organisatie; • monitort de deelname (regelmaat en frequentie) aan de training fraudebewustzijn door de werknemers en bestuurders; • monitort de kwaliteit van de training fraudebewustzijn voor werknemers en bestuurders; • brengt via onder andere interne communicatie, nieuwsbrieven en bedrijfsinformatie fraudebewustzijn onder de aandacht van haar werknemers en bestuurders; • neemt kennis van fraude incidenten bij soortgelijke organisaties, en stelt zichzelf de vraag: Kan dit ook bij ons gebeuren?	• houdt toezicht op het periodiek verzorgen van de kwalitatieve training(en) fraudebewustzijn door het bestuur voor de werknemers en bestuurders. Deze training dient passend te zijn bij de aard, omvang en complexiteit van de organisatie en onderstreept en communiceert het belang van fraudebewustzijn, inclusief de risico's van cyberfraude; • neemt kennis van fraude incidenten bij soortgelijke organisaties, en stelt zichzelf de vraag: Kan dit ook bij ons gebeuren?

9. Administratie en jaarrekening, alsmede schattingsposten in de jaarrekening

Het bestuur:	Het toezichthoudend orgaan:

• draagt zorg voor een adequate vastlegging en gedocumenteerde onderbouwing en (een proces van) autorisatie van journaalposten in de administratie, met inbegrip van alle memoriaalboekingen en schattingsposten;
• documenteert, onderbouwt en autoriseert:
  ○ keuze grondslagen;
  ○ stelselwijzigingen;
  ○ schattingen;
  ○ foutherstel;
  ○ wijzigingen in methoden;
• rekent meerdere scenario's door (indien mogelijk) en onderbouwt de gemaakte gemotiveerde keuze;
• laat de uitkomsten van door haar gemaakte schattingen, toetsen door de internal auditor (indien aanwezig) of beoordelen door (de auditcommissie van) het toezichthoudend orgaan;
• verstrekt de onderbouwingen en uitkomsten van die toetsing aan het toezichthoudend orgaan en de accountant;
• draagt de verantwoordelijkheid voor het opmaken van de jaarrekening;
• beschikt over actuele kennis van de jaarverslaggevingsregels;
• heeft samen met het toezichthoudend orgaan, de primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude in de financiële overzichten, zoals de jaarrekening.
	• vormt een auditcommissie, welke actief toezicht houdt op het proces van het opmaken van de jaarrekening, waarbij specifieke aandacht uitgaat naar:
	  ○ keuze grondslagen;
	  ○ stelselwijzigingen;
	  ○ schattingen;
	  ○ memoriaalboekingen;
	  ○ foutherstel;
	  ○ wijzigingen in methoden;
	• (waaronder de auditcommissie) richt zich specifiek op het onderkennen van mogelijke tendenties bij het bestuur om resultaat en vermogen in de jaarrekening te hoog dan wel te laag weer te geven en bespreekt deze met de accountant;
	• in het bijzonder de auditcommissie is financieel onderlegd en heeft kennis van het opstellen van jaarrekeningen, financiële verslaggevingsregels, (fraude)risicomanagement en interne beheersingsmaatregelen;
	• houdt toezicht op de verantwoordelijkheid van het bestuur voor het opmaken van de jaarrekening;
	• beschikt over actuele kennis van de jaarverslaggevingsregels en ziet erop toe dat binnen het bestuur kennis van het jaarrekeningrecht aanwezig is;
	• Is verantwoordelijk voor de goedkeuring van de jaarverslaggeving;
	• heeft samen met het bestuur, de primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude in de financiële overzichten, zoals de jaarrekening.
	
	Voor organisaties van openbaar belang (OOB) is het instellen van een auditcommissie reeds wettelijk bepaald in het Besluit instelling auditcommissie.

10. Beloningsbeleid

Het bestuur:	Het toezichthoudend orgaan:
• bewaakt dat de doelstellingen van de organisatie en daaruit voortvloeiende targets voor bestuurders en werknemers realistisch zijn; • hanteert targets die passend zijn binnen de geldende normen en waarden vanuit de interne gedragscode en richtlijnen vanuit de sector/branche; • hanteert targets die zowel toezien op korte, als lange termijn; • hanteert een beloningsbeleid dat is geënt op integer handelen en eerlijk zakendoen; • hanteert een beloningsbeleid, welke niet alleen is geënt op financiële indicatoren, maar ook voorziet in zaken zoals klanttevredenheid, milieuprestaties en/of sociaal en maatschappelijk beleid; • beoordeelt het beloningsbeleid op het bestaan van prikkels die leiden tot ongewenst gedrag en neemt maatregelen om deze prikkels weg te nemen of te vermijden; • beoordeelt bij het opstellen van het beloningsbeleid frauderisico's en neemt maatregelen om deze frauderisico's weg te nemen dan wel tot een aanvaardbaar niveau te mitigeren; • voorkomt, in samenspraak met het toezichthoudend orgaan, dat de bestuurdersbeloningen voornamelijk zijn geënt op variabele beloningen (verhoogd frauderisico); • beoordeelt in samenwerking met (de remuneratiecommissie van) het toezichthoudend orgaan periodiek het beloningsbeleid; • hanteert een terugvorderingsbeleid als variabele bonussen achteraf zijn toegekend op basis van onjuist gebleken financiële resultaten.	• toetst of de doelstellingen van de organisatie en daaruit voortvloeiende targets voor bestuurders en werknemers realistisch zijn; • ziet er op toe dat deze targets passend zijn binnen de geldende normen en waarden vanuit de interne gedragscode en richtlijnen vanuit de sector/branche; • ziet erop toe dat gehanteerde targets zowel toezien op korte, als lange termijn; • ziet erop toe dat het beloningsbeleid is geënt op integer handelen en eerlijk zaken doen; • ziet erop toe dat het beloningsbeleid niet alleen is geënt op financiële indicatoren, maar ook voorziet in zaken zoals klanttevredenheid, milieuprestaties en/of sociaal en maatschappelijk beleid; • stelt vast dat er bij het opstellen van het beloningsbeleid een beoordeling is gemaakt van de frauderisico's en er maatregelen zijn genomen om deze frauderisico's weg te nemen of te vermijden; • ziet er op toe dat het beloningsbeleid vrij is van prikkels die leiden tot ongewenst gedrag en ziet toe op maatregelen om deze prikkels te wegnemen dan wel tot een aanvaardbaar niveau mitigeren; • voorkomt dat de bestuurdersbeloningen voornamelijk zijn geënt op variabele beloningen (verhoogd frauderisico); • beoordeelt in samenwerking met het bestuur periodiek het beloningsbeleid en ziet toe op de uitbetaling van beloningen conform het beloningsbeleid; • ziet erop toe dat er sprake is van een terugvorderingsbeleid en op de naleving van het terugvorderingsbeleid.

11. Fraude respons

Het bestuur:	Het toezichthoudend orgaan:
• is verantwoordelijk voor en dient adequaat en voortvarend te handelen bij een vermoeden van fraude, bij het niet-naleven van vigerende wet- en regelgeving en integriteitsissues, om schade voor de organisatie, in welke vorm dan ook, te voorkomen dan wel zoveel mogelijk te beperken; • is verantwoordelijk voor de uitwerking van een fraude respons plan, om voorbereid te zijn op de vraag hoe te handelen bij een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues. **Aanbevelingen hiervoor zijn in bijlage 1 beschreven;** • besteedt in het bestuursverslag aandacht aan de aard, de omvang en het aantal fraude incidenten en de fraude respons hierop; • informeert bij een vermoeden van fraude in een zo vroeg mogelijk stadium de accountant en het toezichthoudend orgaan; • handelt adequaat en voortvarend bij een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues, op basis van het door het bestuur uitgewerkte fraude respons plan; • betrekt de accountant in het fraude respons plan en zet fraude op de agenda van de periodieke overleggen van het bestuur en het toezichthoudend orgaan met de accountant.	• houdt toezicht op het adequaat en voortvarend handelen van de organisatie bij een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues, om schade voor de organisatie, in welke vorm dan ook,te voorkomen dan wel zoveel mogelijk te beperken; • stelt vast dat onder verantwoordelijkheid van het bestuur een fraude respons plan is uitgewerkt; • handelt adequaat en voortvarend bij een vermoeden van fraude, niet-naleving van wet- en regelgeving en integriteitsissues, op basis van het onder verantwoordelijkheid van het bestuur uitgewerkte fraude respons plan; • ziet erop toe dat in het bestuursverslag aandacht is besteed aan de aard, de omvang en het aantal fraude incidenten en de fraude respons hierop; • maakt afspraken over wie de leiding en coördinatie op zich neemt binnen het toezicht houdend orgaan bij de opvolging en afhandeling van een vermoeden van fraude waarbij het management/het bestuur betrokken is (zogenaamde managementfraude); • overlegt met de accountant op welke wijze en wie vanuit het toezichthoudend orgaan de accountant informeert bij een vermoeden van fraude waarbij het management/bestuur betrokken is; • heeft het mandaat om bij een vermoeden van managementfraude een jurist of onafhankelijk specialist te consulteren of in te schakelen, die niet de huis(jurist) is en/of de belangen van bestuurders verdedigt; • betrekt de accountant in het fraude respons plan en zet fraude op de agenda van de periodieke overleggen van het bestuur en het toezichthoudend orgaan met de accountant.

BIJLAGE 1

Aanbevelingen voor een door de organisatie op te stellen fraude respons plan

De aanbevelingen zijn uitgewerkt in zes aandachtsgebieden, te weten:

A. Leiding en coördinatie
B. Veiligstellen van data
C. Onderzoek naar een (vermoeden van) fraude
D. Communicatie intern en extern, inclusief omgang met de media
E. (tijdelijke) Maatregelen voorafgaand en gedurende het onderzoek jegens betrokkenen
F. Opvolging van uitkomsten fraudeonderzoek: te nemen maatregelen

A. Leiding en coördinatie

1. Het bestuur formuleert afspraken over wie de leiding en coördinatie op zich neemt bij de opvolging en afhandeling van een vermoeden van fraude waarbij werknemers betrokken zijn (zogenaamde personeelsfraude) en een vermoeden van fraude waarbij het management/het bestuur betrokken is (zogenaamde managementfraude).
2. Het bestuur formuleert afspraken over wie de leiding en coördinatie op zich neemt en hoe te handelen op klokkenluidersmeldingen, alsmede het communiceren met en beschermen van de klokkenluider.
3. De persoon die de leiding en coördinatie op zich neemt, heeft voldoende mandaat en bevoegdheden om maatregelen te nemen in de opvolging en afhandeling van een vermoeden van zowel personeelsfraude als managementfraude. Bij vermoeden van managementfraude vervult het toezichthoudend orgaan hierin een leidende en coördinerende rol.
4. In situaties dat er sprake is van een vermoeden van managementfraude dient het toezichthoudend orgaan direct geïnformeerd te worden.
5. De persoon die de leiding en coördinatie op zich neemt, krijgt voldoende tijd en middelen ter beschikking om een vermoeden van fraude adequaat op te volgen en kan zo nodig terugvallen op assistentie vanuit de organisatie.
6. Snel en adequaat handelen bij een vermoeden van fraude is cruciaal. Vaak ontstaat een impasse als niet snel duidelijk is wie de leiding en coördinatie op zich neemt bij de opvolging en afhandeling van vermoeden van fraude.
7. Betrek ook het toezichthoudend orgaan in de uitwerking van een fraude respons plan en richt informatielijnen in naar het toezichthoudend orgaan. Het toezichthoudende orgaan vervult in de uitwerking een leidende rol.
8. Een fraude respons plan wordt opgesteld onder verantwoordelijkheid van en goedgekeurd door het bestuur. Het fraude respons plan is te zien als een handreiking, die flexibel op iedere situatie kan worden toegepast.
9. Informeer bij een vermoeden van fraude in een zo vroeg mogelijk stadium de accountant. Neem de accountant mee in het fraude respons plan en zet fraude op de agenda van de periodieke overleggen van het bestuur en het toezichthoudend orgaan met de accountant.
10. Overleg ook met de accountant op welke wijze en wie vanuit de organisatie of het toezichthoudend orgaan, de accountant informeert bij vermoeden van fraude (personeelsfraude, managementfraude etc.).
11. Maak concrete afspraken met internal audit (indien aanwezig) over hun rol bij fraudeonderzoeken, zodat duidelijk wordt of en zo ja op welke wijze de internal auditor kan ondersteunen. De internal

auditor heeft goed zicht op de organisatie en controle-omgeving inclusief cultuur- en gedragscomponenten.

12. Betrek in een zo vroeg mogelijk stadium een ter zake kundig jurist die de organisatie adviseert bij te nemen vervolgstappen.
13. Formuleer afspraken over welke instanties en externe partijen vanaf welk moment en op welke wijze samenwerken.
14. Formuleer afspraken over vanaf welk moment en op welke wijze er samengewerkt wordt met opsporingsinstanties (zoals bijvoorbeeld FIOD, politie en OM) en/of externe toezichthouders (zoals bijvoorbeeld AFM en DNB) en de verzekeringsmaatschappij. Win hiertoe advies in van een ter zake kundige jurist.

B. Veiligstellen van data

1. Voorkomen is beter dan genezen: organiseer het databeheer en -management in de organisatie zodat bij vermoeden van fraude bepaalde (vaste) procedures hiervoor in werking gezet kunnen worden. Organiseer en regel hiervoor de noodzakelijke rollen en verantwoordelijkheden in de organisatie.
2. Stel bij een vermoeden van fraude in een zo vroeg mogelijk stadium data (digitale informatie en geprinte data) veilig om dataverlies te voorkomen. En overweeg dus het direct ontnemen van toegang tot de systemen door werknemers op wie een vermoeden rust van mogelijke betrokkenheid bij fraude.
3. Formuleer in een zo vroeg mogelijk stadium het doel van het onderzoek naar veiliggestelde data (digitale informatie en geprinte data). Dit stelt de organisatie in staat om zoveel als redelijkerwijs mogelijk is reeds bij het veiligstellen van data de beginselen van proportionaliteit en subsidiariteit in acht te nemen.
4. Houd in het fraude respons plan bij het veiligstellen van de data rekening met de geldende wet- en regelgeving ten aanzien van bescherming persoonsgegevens.
5. Bij het veiligstellen van data kunnen externe specialisten worden ingeschakeld, die zo mogelijk met medewerking van IT medewerkers van de organisatie zorgdragen voor het veiligstellen van data en het opslaan van data in een beveiligde omgeving. Laat dit uitvoeren door ter zake kundige specialisten die weten hoe de authenticiteit en integriteit van de data behouden blijft bij het veiligstellen ervan.
6. Stel naast digitale informatie en geprinte (werkplekonderzoek) data bepaalde hardware veilig, zoals laptops, mobiele telefoons, camera's, gegevensdragers, printers, etc.
7. Organiseer dat de (financiële) administratie en het e-mailverkeer over een werkende back-up-functionaliteit beschikt, alsmede een functie, waarmee mutaties en metadata over die mutaties kunnen worden geëxporteerd. Informeer hierover bij uw softwareleverancier.
8. Organiseer dat de organisatie te allen tijde beschikt over betrouwbare bestanden ten aanzien van haar historische betalingsverkeer. Organiseer dit op voorhand en niet pas als sprake is van vermoeden van fraude. Informeer hierover bij uw banken en financiële instellingen.

C. Onderzoek naar een (vermoeden van) fraude

1. Een vermoeden van fraude kan op vele manieren bekend worden, bijvoorbeeld via de werking van een klokkenluidersregeling of meldpunt.
2. Het is aan te bevelen om direct zorg te dragen voor bescherming van de melder van het signaal alvorens de melding te laten beoordelen (oriëntatie fase) op validiteit en echtheid. Voorts dient zoveel als mogelijk de anonimiteit van de melder te worden bewaakt.
3. Als de melding na de oriëntatie fase voldoende grond en rechtvaardiging geeft voor een vermoeden van fraude, formuleer dan een onderzoeksdoelstelling. Wat wil de organisatie met het onderzoek bereiken? Daarbij dient te worden nagedacht over mogelijke juridische vervolgstappen na afronding van het onderzoek.

4. Informeer de accountant voorafgaand aan de formulering van de onderzoeksdoelstelling. Stel de accountant in staat om input te leveren ten aanzien van de onderzoeksdoelstelling, scope en reikwijdte van het uit te voeren fraudeonderzoek.
5. Houdt de kring van geïnformeerde (circle of trust) zo beperkt mogelijk.
6. Als er sprake is van een vermoeden van managementfraude verdient het aanbeveling dat het toezichthoudend orgaan mandaat heeft om een jurist te consulteren of in te schakelen die niet de huis(jurist) is en/of de belangen van bestuurders verdedigt, teneinde de onafhankelijkheid te waarborgen.
7. Overweeg om het fraudeonderzoek te laten uitvoeren door een hierin gespecialiseerd en daarvoor aangewezen onderzoeksteam of door externe fraudeonderzoekers (bijvoorbeeld een forensisch accountant, een onderzoeksbureau, een certified fraud examiner of andere specialisten). Voor vermoeden van fraude van enige omvang en impact op de organisatie is de onafhankelijkheid van onderzoek(ers) essentieel, zodat de resultaten gebruikt kunnen worden bij eventuele juridische vervolgstappen.
8. Betrek bij het fraudeonderzoek tevens één of meerdere juristen ten aanzien van de relevante rechtsgebieden (veelal arbeidsrecht, ondernemingsrecht/civiel recht en/of financieel economisch strafrecht)[1] die de organisatie juridisch kan adviseren en eventuele stappen kan ondernemen voorafgaand aan, tijdens, of na het onderzoek.

D. Communicatie intern en extern, inclusief omgang met de media

1. Zorg ervoor dat bij een vermoeden van fraude het bestuur en/of het toezichthoudend orgaan zo snel mogelijk op de hoogte worden gesteld.
2. De opvolging en afhandeling van een vermoeden van fraude gaat met emoties gepaard en laat een organisatie niet onberoerd. Het is daarom cruciaal dat vertrouwelijk wordt omgegaan met een vermoeden van fraude totdat besluiten zijn genomen over de inhoud en wijze van interne communicatie (bijvoorbeeld aan werknemers) en eventuele externe communicatie (bijvoorbeeld aan de media en andere externe partijen).
3. Formuleer tijdig een persbericht ten behoeve van de externe communicatie en stem dit af met de onderzoekers. Schakel hierbij een (externe) jurist in. Bij beursgenoteerde organisaties dient voorts te worden afgestemd met de afdeling legal en compliance en/of het disclosure committee.
4. Verstrek bij brede interne communicatie niet meer informatie dan noodzakelijk en geef op hoofdlijnen aan op welke wijze een vermoeden van fraude wordt opgevolgd om de rust te bewaren.

E. (tijdelijke) Maatregelen voorafgaand en gedurende het fraudeonderzoek jegens betrokkenen

1. Ga zorgvuldig om met alle betrokkenen op wie een verdenking rust van betrokkenheid bij fraude.
2. Formuleer afspraken over welke (tijdelijke) maatregelen genomen kunnen worden tegen werknemers die zijn betrokkenen in een fraudeonderzoek.
3. Win altijd arbeidsrechtelijk juridisch advies in bij het nemen van (tijdelijke) maatregelen tegen werknemers.
4. Neem in arbeidscontracten op dat werknemers gehouden zijn mee te werken aan door de leiding van de organisatie ingelast (fraude)onderzoek.
5. Zorg ervoor dat het fraudeonderzoeksteam kan werken in niet voor anderen toegankelijke werkruimte(n) en (deel)systemen.

[1] Een jurist arbeidsrecht kan erop toezien dat de werkgever voortvarend, maar binnen de grenzen van het arbeidsrecht handelt. Een jurist ondernemings-/civielrecht kan vermogensbestanddelen veiligstellen in het kader van schadeverhaal, bewijsbeslag leggen en procesvoering in het kader van aansprakelijkheid en schade voorbereiden. Een jurist strafrecht kan adviseren over een strafrechtelijk traject, ondersteunen bij aangifte en communicatie met OM en/of opsporingsinstanties.

F. Opvolging van uitkomsten fraudeonderzoek: te nemen maatregelen

1. Ter afronding van een fraudeonderzoek volgt een rapport van bevindingen. Het bevoegde management of het toezichthoudend orgaan in geval van managementfraude bepaalt de vervolgstappen. Zij krijgen daartoe zo nodig en voor zover van toepassing advies van de afdeling legal, compliance, internal audit, HRM en/of de externe jurist.

2. Formuleer afspraken over welke personen binnen de organisatie betrokken zijn bij het inhoudelijk bepalen van vervolgstappen na afronding van fraudeonderzoek. Bijvoorbeeld (arbeids)jurist, HRM, compliance, bevoegd management.
3. Formuleer afspraken wie wanneer een (externe) jurist inschakelt ten behoeve van advisering bij te nemen maatregelen op basis van vervolgstappen na afronding van fraudeonderzoek. Het is in voorkomende gevallen mogelijk dat reeds tijdens het onderzoek stappen dienen te worden genomen, bijvoorbeeld schorsing van werknemers, of bewijsbeslag.
4. Formuleer afspraken over de vraag in welke gevallen de organisatie aangifte moet doen of melding moet maken bij opsporingsinstanties.
5. Evalueer eventuele op de organisatie rustende meldplichten aan externe instanties uit hoofde van wet- en regelgeving, zoals bijvoorbeeld AFM, DNB, of uit hoofde van de Wwft.
6. Formuleer afspraken indien sprake (b)lijkt van fraude en er arbeidsrechtelijke maatregelen (zoals bijvoorbeeld schorsing, ontheffing van functie/bevoegdheden, ontslag), civielrechtelijke maatregelen (zoals procedure met eis tot schadevergoeding), of strafrechtelijke maatregelen (zoals aangifte bij OM) genomen gaan worden.
7. Als daadwerkelijk sprake (b)lijkt te zijn van fraude, zorgt de organisatie voor een plan van aanpak voor herstel (correctie) van de fraude en implementatie van maatregelen om herhaling te voorkomen. Overleg met de accountant over de redres aanpak en de eisen die zij (minimaal) stellen aan een dergelijk herstelplan.
8. De accountant zal het plan van aanpak beoordelen en zal vaststellen dat de organisatie uitvoering heeft gegeven aan de in het plan van aanpak opgenomen maatregelen ter herstel en voorkoming van herhaling van de fraude.
9. Overleg met internal audit over hun mogelijke toegevoegde waarde richting toekomst. Denk aan hun kritische betrokkenheid en advies bij bijvoorbeeld de opzet of veranderingen van processen, voorschriften en beheersmaatregelen. Internal audit is door zijn organisatiesensitiviteit in een positie om verschil in gedragingen te onderkennen en de risico's en impact van veranderingen op rationalisatie en druk binnen de organisatie te beoordelen en hiermee rekening te houden in de risicoanalyses.

BIJLAGE 2

Voorbeelden van frauderisicofactoren

1. Inleiding

De in deze bijlage vermelde frauderisicofactoren zijn voorbeelden van factoren waarmee bestuurders, toezichthouders en accountants in een groot aantal verschillende situaties kunnen worden geconfronteerd.

Voorbeelden worden gepresenteerd van twee soorten fraude die vanuit perspectief van een accountant relevant zijn, namelijk:

- frauduleuze financiële verslaggeving en;
- oneigenlijke toe-eigening van activa.

Voor beide soorten fraude worden de risicofactoren verder ingedeeld op basis van de drie omstandigheden die gewoonlijk aanwezig zijn wanneer afwijkingen van materieel belang die het gevolg zijn van fraude zich voordoen:

1. stimulansen/druk;
2. gelegenheden en;
3. instelling/rechtvaardiging.

Deze drie omstandigheden worden tezamen de fraudedriehoek genoemd.

Hoewel de risicofactoren een breed scala aan omstandigheden beslaan, gaat het slechts om voorbeelden. Het is dan ook mogelijk dat de met governance belaste personen, het management van de organisatie en/of de accountant aanvullende of andere risicofactoren vaststellen. Niet al deze voorbeelden zijn in alle omstandigheden relevant, en sommige kunnen meer of minder significant zijn afhankelijk van de grootte van de organisatie, de eigendomskenmerken van de organisatie of de omstandigheden. Voorts weerspiegelt de volgorde waarin de voorbeelden van risicofactoren worden beschreven niet het relatieve belang ervan of de frequentie waarmee ze voorkomen.

2. Risicofactoren met betrekking tot frauduleuze financiële verslaggeving

Hieronder volgen voorbeelden van risicofactoren met betrekking tot afwijkingen die voortkomen uit frauduleuze financiële verslaggeving.

Stimulansen/druk

De financiële stabiliteit of de winstgevendheid wordt bedreigd door de economische omstandigheden, de omstandigheden in de sector of de exploitatieomstandigheden van de entiteit, zoals (of zoals blijkt uit):

- hoge mate van concurrentie of marktverzadiging, in combinatie met dalende winstmarges;
- grote kwetsbaarheid voor elkaar snel opvolgende veranderingen, zoals technologische veranderingen, productveroudering of rentevoeten;
- aanzienlijke daling van de vraag en een toename van het aantal faillissementen in de sector of in de economie als geheel;
- exploitatieverliezen die de dreiging van een faillissement, een executoriale verkoop of een vijandige overname acuut maken;
- terugkerende negatieve kasstromen uit operationele activiteiten of de onmogelijkheid uit de operationele activiteiten kasstromen te genereren, terwijl zowel winst als een winstgroei wordt gerapporteerd;
- een snelle groei of een ongewone winstgevendheid, vooral in vergelijking met andere ondernemingen in de sector;
- nieuwe vereisten op het gebied van financiële verslaggeving of nieuwe door wet- of regelgeving gestelde vereisten.

Het management staat onder overmatige druk om aan de vereisten of verwachtingen van derden te voldoen als gevolg van:

- verwachtingen van beleggingsanalisten, institutionele beleggers, (activistische) aandeelhouders, significante schuldeisers of andere derden ten aanzien van de winstgevendheid of ontwikkelingsniveaus (met name verwachtingen die bovenmatig ambitieus of onrealistisch zijn), met inbegrip van verwachtingen die door het management zelf zijn gewekt, bijvoorbeeld door te optimistische persberichten of berichten in jaarverslagen of “Capital Market Day” presentaties;
- de behoefte aan aanvullende financiering met eigen of vreemd vermogen om concurrerend te blijven, met inbegrip van de financiering van belangrijke kosten van onderzoek en ontwikkeling of investeringsuitgaven;
- het nauwelijks in staat zijn om aan de voorwaarden voor beursnotering te voldoen of om schulden af te lossen of clausules in financieringsovereenkomsten na te leven;
- verwachte of werkelijke negatieve gevolgen van het rapporteren van slechte financiële resultaten op significante lopende transacties, zoals bedrijfscombinaties of de gunning van contracten.

De beschikbare informatie duidt erop dat de persoonlijke financiële situatie van leden van het management of de met governance belaste personen wordt bedreigd door de financiële prestaties van de entiteit als gevolg van:

- significante financiële belangen in de entiteit;
- significante bestanddelen van hun beloning (zoals bonussen, aandelenopties en earn-out regelingen) zijn gekoppeld aan het bereiken ambitieuze doelstellingen met betrekking tot de aandelenkoers, de bedrijfsresultaten, de financiële positie of de kasstromen;
- verstrekte persoonlijke borgstellingen voor schulden van de entiteit;
- overmatige druk op het management of uitvoerend personeel om financiële doelstellingen te halen die door de met governance belaste personen zijn bepaald, met inbegrip van doelstellingen die betrekking hebben op de verkopen of de winstgevendheid.

Gelegenheden

De aard van de sector of de activiteiten van de entiteit biedt gelegenheid tot frauduleuze financiële verslaggeving die kan voortkomen uit:

- significante transacties met verbonden partijen buiten het kader van de normale bedrijfsvoering of transacties met verbonden entiteiten die al dan niet door een andere accountantseenheid worden gecontroleerd;
- een sterke financiële aanwezigheid of de mogelijkheid om een bepaalde sector te domineren waardoor de organisatie in staat is aan leveranciers of klanten voorwaarden op te leggen die kunnen leiden tot ongepaste transacties of transacties die niet marktconform zijn;
- activa, verplichtingen, opbrengsten of lasten die gebaseerd zijn op significante schattingen die steunen op moeilijk te staven subjectieve oordeelsvormingen of onzekerheden;
- significante, ongebruikelijke of zeer complexe transacties, met name transacties die vlak vóór het einde van de verslagperiode plaatsvinden en die moeilijke vragen oproepen met betrekking tot het prevaleren van de economische realiteit boven de juridische vorm ('substance over form');
- significante activiteiten in het buitenland of grensoverschrijdende activiteiten in jurisdicties waar andere bedrijfsomgevingen en -culturen bestaan;
- de inschakeling van tussenpersonen waarvoor geen duidelijke zakelijke reden lijkt te bestaan;
- off-shore bankrekeningen of activiteiten met dochtermaatschappijen of nevenvestigingen in belastingparadijzen waarvoor geen duidelijke zakelijke reden lijkt te bestaan.

De monitoring van het management is niet effectief als gevolg van het feit dat:

- het management (in een door een eigenaar-bestuurder geleide onderneming) door één persoon of een kleine groep personen wordt gedomineerd zonder dat compenserende interne beheersingsmaatregelen zijn genomen;
- het toezicht door de met governance belaste personen op het proces van financiële verslaggeving en op de interne beheersing niet effectief is.

Er bestaat een complexe of instabiele organisatiestructuur, zoals blijkt uit:

- de moeilijkheid om vast te stellen welke organisatie of personen een uiteindelijk belang met overheersende zeggenschap (“ultimate beneficiary owners”) hebben in de entiteit;
- een overmatig complexe organisatiestructuur waarbij gebruik wordt gemaakt van ongebruikelijke rechtspersonen of hiërarchische gezagslijnen;
- een groot verloop onder het senior management, de juridische adviseurs of de met governance belaste personen.

Componenten van de interne beheersing schieten tekort als gevolg van:

- inadequate monitoring van de interne beheersingsmaatregelen, met inbegrip van de geautomatiseerde interne beheersingsmaatregelen en de interne beheersingsmaatregelen die betrekking hebben op de tussentijdse financiële verslaggeving (indien externe rapportage vereist is);
- een hoog personeelsverloop of de inzet van niet-effectieve staf voor administratieve verwerking, interne audit of informatietechnologie;
- ineffectieve systemen voor administratieve verwerking en informatiesystemen, met inbegrip van situaties waarin zich significante tekortkomingen in de interne beheersing voordoen.

Instelling/rechtvaardiging

- ineffectieve communicatie, implementatie, ondersteuning of handhaving van de waarden of ethische voorschriften van de entiteit door het management, of de communicatie van ongepaste waarden of ethische voorschriften;
- bovenmatige betrokkenheid of preoccupatie van leden van het management die geen financiële functie uitoefenen bij respectievelijk met de keuze van grondslagen voor financiële verslaggeving of de bepaling van significante schattingen;

- een bekend verleden van overtredingen van de effectenwetgeving of andere wet- en regelgeving, dan wel aanklachten tegen de entiteit, haar senior management of de met governance belaste personen betreffende fraude of de niet-naleving van wet- en regelgeving;
- bovenmatige belangstelling van het management voor het handhaven of verhogen van de aandelenkoers of winstontwikkeling van de entiteit;
- de gewoonte van het management om zich tegenover analisten, schuldeisers en andere derden tot ambitieuze of onrealistische prognoses te verplichten;
- het management slaagt er niet in om bekende significante tekortkomingen in de interne beheersing tijdig te corrigeren;
- het management heeft er, vanuit fiscaal oogpunt belang bij niet passende middelen te hanteren om het gerapporteerde resultaat te drukken;
- een lage moraal onder het senior management;
- de eigenaar-bestuurder maakt geen onderscheid tussen transacties van zakelijke en private aard;
- onenigheid tussen aandeelhouders in een entiteit met weinig aandeelhouders;
- herhaaldelijk voorkomende pogingen van het management om administratieve verwerkingen die marginaal of niet passend zijn te rechtvaardigen op grond van materialiteit;
- de relatie tussen het management en de huidige dan wel de vorige accountant is gespannen, zoals blijkt uit:
    - regelmatige verschillen van inzicht met de huidige dan wel de voormalige accountant over aangelegenheden inzake verslaggeving, controle of rapportage;
    - onredelijke eisen gesteld aan de accountant, zoals niet te realiseren tijdschema's voor het uitvoeren van de controle of voor het uitbrengen van de controleverklaring;
    - aan de accountant opgelegde beperkingen die op niet passende wijze grenzen stellen aan de toegang bij personen of tot informatie dan wel aan de mogelijkheid om effectief aan hen belast met toezicht te communiceren;
    - overheersend gedrag van het management in de omgang met de accountant, in het bijzonder betreffende pogingen om de reikwijdte van de controlewerkzaamheden te beïnvloeden of invloed uit te oefenen op de keuze en het behoud van de personen die aan de opdracht worden toegewezen of van de personen die ter advisering in het kader van de controle worden ingezet.

3. Risicofactoren met betrekking tot het oneigenlijk toe-eigenen van activa

De risicofactoren die betrekking hebben op afwijkingen die voortkomen uit het oneigenlijk toe-eigenen van activa worden ook gegroepeerd naar de drie omstandigheden die gewoonlijk aanwezig zijn wanneer fraude zich voordoet:

1. stimulansen/druk,
2. gelegenheden en
3. instelling/rechtvaardiging.

Sommige risicofactoren die betrekking hebben op afwijkingen als gevolg van frauduleuze financiële verslaggeving kunnen ook aanwezig zijn als het oneigenlijk toe-eigenen van activa zich voordoet. Ineffectieve monitoring van het management en andere tekortkomingen in de interne beheersing kunnen zich bijvoorbeeld voordoen wanneer afwijkingen die het gevolg zijn van frauduleuze financiële verslaggeving dan wel van oneigenlijk toe-eigenen van activa voorkomen. Hiernaar zijn voorbeelden van risicofactoren opgenomen met betrekking tot afwijkingen die het gevolg zijn van oneigenlijk toe-eigenen van activa.

Stimulansen/druk

Persoonlijke financiële verplichtingen (bijvoorbeeld door verkeerde beleggingen, scheiding, verslavingen) kunnen druk uitoefenen op het management of op de personeelsleden die toegang hebben tot de liquide middelen of tot de andere daarvoor vatbare activa, om deze activa te oneigenlijk toe-eigenen. Een slechte verstandhouding tussen de entiteit en de personeelsleden die toegang hebben tot de liquide middelen dan wel tot de andere voor diefstal vatbare activa kan voor deze personeelsleden een reden inhouden om deze activa te oneigenlijk toe-eigenen. Een slechte verstandhouding kan bijvoorbeeld ontstaan door:

- aangekondigde of verwachte toekomstige ontslagen onder werknemers;
- recente of verwachte wijzigingen in de beloningen van werknemers of in toegezegde pensioenrechten;
- interne promoties, de vergoeding of andere beloningen die afwijken van hetgeen werd verwacht.

Gelegenheden

Sommige kenmerken of omstandigheden kunnen de vatbaarheid van het oneigenlijk toe-eigenen van activa vergroten. Zo kan meer gelegenheid daartoe wordt gecreëerd in de volgende situaties:

- grote hoeveelheden contant geld in kas of groot kasverkeer;
- voorraaditems die een geringe omvang maar een hoge waarde hebben of waarnaar de vraag hoog is;
- gemakkelijk te verzilveren activa, zoals effecten aan toonder, diamanten, edelmetalen, of computerchips, mobiles, laptops, sterke drank, sigaretten, medicijnen, aandelen aan toonder, waardepapieren;
- vaste activa die van een geringe omvang en gemakkelijk te verkopen zijn of waarvan niet op duidelijke wijze is aangegeven wie de eigenaar is.
- Verhandelbare informatie (bijvoorbeeld patenten, octrooien, ontwikkelplannen, koersgevoelige informatie)

Inadequate interne beheersingsmaatregelen met betrekking tot activa kunnen die activa vatbaarder maken voor oneigenlijk toe-eigening. Zo is het mogelijk dat activa oneigenlijk worden toegeëigend omdat de volgende factoren bestaan:

- inadequate functiescheiding of onafhankelijke controles;
- inadequaat toezicht op de uitgaven van het senior management, zoals vergoeding van reiskosten en andere kosten;

- inadequaat toezicht uitgeoefend door het management op werknemers die verantwoordelijk zijn voor activa, zoals inadequaat toezicht op of inadequate monitoring van afgelegen vestigingen;
- inadequate screening van de sollicitanten die na aanwerving toegang hebben gekregen tot activa;
- inadequate administratie met betrekking tot activa;
- inadequaat systeem van autorisatie en goedkeuring van transacties (bijvoorbeeld aan de inkoopzijde);
- inadequate fysieke veiligheidsmaatregelen voor liquide middelen, beleggingen, voorraden of vaste activa;
- het ontbreken van een volledige en tijdige aansluiting van activa;
- het ontbreken van een tijdige en adequate documentatie van transacties, bijvoorbeeld de creditering van geretourneerde goederen;
- geen verplichte vakantie voor werknemers in belangrijke posities binnen de interne beheersing;
- ontoereikende kennis bij het management van informatietechnologie, waardoor het IT-personeel in staat is activa oneigenlijk toe te eigenen;
- inadequate toegangsbeveiligingsmaatregelen voor geautomatiseerde bestanden, met inbegrip van interne beheersingsmaatregelen met betrekking tot de logbestanden van computersystemen en de beoordeling daarvan.

Instelling/rechtvaardiging

- het negeren van de noodzaak om risico's die betrekking hebben op de oneigenlijke toe-eigening van activa te monitoren of te beperken;
- het negeren van de interne beheersing met betrekking tot de oneigenlijke toe-eigening van activa door bestaande interne beheersingsmaatregelen te doorbreken of door het nalaten passende corrigerende maatregelen te nemen met betrekking tot bekende tekortkomingen in de interne beheersing;
- gedrag waaruit het ongenoegen dan wel de ontevredenheid blijkt met de entiteit of met de wijze waarop ze met haar werknemers omgaat;
- veranderingen in het gedrag of in de levensstijl die een aanwijzing kunnen vormen voor het feit dat activa oneigenlijk zijn toegeëigend;
- het tolereren van kruimeldiefstal.

BIJLAGE 3

Definities/Nadere duidingen

Hier zullen belangrijkste begrippen en hun definities dan wel omschrijvingen worden opgenomen:

Accountant een natuurlijk persoon die beroepsmatig jaarrekeningen controleert, jaarrekeningen opmaakt of financiële administraties voert. De term de accountant wordt ook wel gebruikt om een accountantsorganisatie te duiden.

Belangenverstrengeling een situatie waarbij iemand meerdere belangen dient en waarbij dezen met elkaar in conflict komen. Dit kunnen zowel zakelijke-, als privé belangen zijn niet met elkaar verenigbaar zijn.

Bestuurder de statutair bestuurder van een organisatie, die alleen of samen met anderen het bestuursorgaan van de organisatie vormt.

Commissaris houdt toezicht op het beleid en uitvoering van het beleid van een organisatie namens aandeelhouders en stakeholder. De commissaris is een lid van het toezichthoudend orgaan van de organisatie.

Corruptie een verschijningsvorm van fraude, we onderscheiden actieve (omkopen) en passieve corruptie (omgekocht worden), ambtelijke en niet-ambtelijke corruptie. Corruptie gaat vaak samen met andere strafbare feiten zoals valsheid in geschrifte, witwassen en deelname aan een criminele organisatie.

Cyberfraude een criminele manier om geld te verdienen op het internet. Doordat technologie zo'n grote impact heeft op het leven is internetfraude steeds winstgevender. Het kan helaas erg veel schade aanrichten.

Diversiteit de verscheidenheid aan mensen binnen één organisatie. We hebben het dan niet alleen over verschillen in geslacht en cultuur, maar ook over bijvoorbeeld leeftijd en kennis.

Ethisch handelen het handelen in overeenstemming met de waarden en de normen waaraan wij onszelf en anderen in redelijkheid gehouden achten. Ethisch handelen is meer dan je aan de wet houden. Wat is goed en wat is fout? En wie bepaalt dat?

Externe accountant een natuurlijke persoon die werkzaam is bij of verbonden is aan een accountantsorganisatie, en die verantwoordelijk is voor de uitvoering van de jaarrekening controle het opmaken van de jaarrekening of het voeren van de financiële administratie.

Forensisch accountant een gespecialiseerde accountant die zich bezighoudt met het onderzoeken van financiële informatie op basis van fraude ervaring en juridische en financiële kennis.

Foutherstel de organisatie komt tot de conclusie dat toepassing van het toegepaste stelsel onjuist is geweest of het stelsel onjuist heeft toegepast, en dient dit te herstellen.

Fraude het verrichten van een 'Een opzettelijke handeling door één of meer leden van het management, het toezichthoudend orgaan, werknemers of derden, waarbij gebruik wordt gemaakt van misleiding om een onrechtmatig voordeel te verkrijgen'. Fraude kent vele verschijningsvormen in deze best practices wordt gedoeld onrechtmatige toe eigenen van activa, fraude in de financiële verantwoording en corruptie.

Fraudebewustzijn het sneller en beter herkennen en aanvoelen van opmerkelijke situaties en daar vervolgens als een soort van automatisme opvolging aangeven. Het is uitdaging om iedereen binnen de organisatie te (blijven) stimuleren om (meer) fraudebewust te zijn.

Fraudedriehoek een theorie, waarbij wordt verondersteld dat voor fraude drie elementen nodig zijn: druk, gelegenheid en rationalisatie. Een fraudeur ervaart druk of stimulans om een fraude te plegen en acht zich in staat om vanuit zijn positie fraude te plegen (gelegenheid) en rechtvaardigt de door hem voorgenomen fraude voor zichzelf (rechtvaardiging).

Fraudemeldpunt voor iedereen binnen de organisatie moet duidelijk zijn bij wie een vermoeden van fraude gemeld kan worden en op welke manier deze melding kan plaatsvinden (bijv. mondeling/telefonisch/schriftelijk/email). Het fraudemeldpunt wordt vermeld de interne gedragscode en/of het huishoudelijk reglement.

Fraude respons plan een leidraad of spoorboekje te zijn voor hoe het bestuur en het toezichthoudend orgaan dient te handelen bij vermoeden van fraude. Een fraude response plan stelt een organisatie in staat om adequaat en voortvarend te handelen om schade voor de organisatie, in welke vorm dan ook, zoveel mogelijk te beperken.

Frauderisico-beheersing de interne beheersingsmaatregelen dienen passend te zijn binnen de organisatie, om op basis van de frauderisico-inschatting, geïdentificeerde frauderisico's te voorkomen en detecteren. De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude berust bij het toezichthoudend orgaan en het bestuur van de organisatie. Het is van belang dat het bestuur, onder het toezichthoudend orgaan, sterk de nadruk legt op het voorkomen van fraude, waardoor de gelegenheden tot het plegen van fraude kunnen afnemen, alsmede op het ontmoedigen daarvan, waardoor personen ervan kunnen worden weerhouden om fraude te plegen wegens de waarschijnlijkheid dat die fraude wordt gedetecteerd en bestraft.

Frauderisico-inschatting de werkzaamheden gericht op het verwerven van inzicht in de organisatie en haar omgeving, met inbegrip van haar interne beheersing, om mogelijke frauderisico's te identificeren. Op basis van aard, omvang en frequentie wordt een inschatting gemaakt van de kans dat een mogelijk frauderisico zich voordoet.

Fraude vermoeden van in bijlage 2 is uitgebreid ingegaan op voorbeelden van frauderisicofactoren en die kunnen leiden tot vermoeden van fraude. Ook door zelf alert te zijn kunt u signalen herkennen die op mogelijke fraude wijzen. Naast vermoeden en verdenking van fraude is echt bewijs en zijn feiten nodig, voordat fraude kan worden vastgesteld.

Governance orgaan het toezichthoudend orgaan van een organisatie, zoals de Raad van Commissarissen of de Raad van Toezicht. In de context van deze best practices wordt met governance orgaan het toezichthoudend orgaan van een organisatie bedoeld, ongeacht de benaming. In de praktijk komen ook andere verschijningsvormen van organen voor die óf een andere rol hebben óf anders of niet zijn geformaliseerd. Bijvoorbeeld de Raad van Advies, die geen toezichthoudende rol vervult maar een advies- of klankbordrol, aandeelhouders of een selectie daarvan (bijvoorbeeld bestuurders van een stichting administratiekantoor) of andere verschijningsvormen. Het voert voor deze best practices te ver om voor dergelijke afwijkende organen separate aanbevelingen uit te werken. Wij bevelen dergelijke organisaties aan de best practices voor naar eigen inzicht in te passen die het best past bij de positie en rol van het desbetreffende orgaan.

Grondslagen – keuze (hoofdstuk 10) de grondslagen van waardering en bepaling van het resultaat zijn de specifieke principes, beginselen, conventies en regels die een organisatie toepast bij het opmaken van de jaarrekening. Titel 9 Boek 2 BW is van toepassing op Nederlandse statutaire jaarrekeningen en schrijft een set aan grondslagen voor. De Raad voor de Jaarverslaggeving heeft in de Richtlijnen voor de Jaarverslaggeving (RJ) deze grondslagen nader uitgewerkt en ingevuld. Op verschillende onderwerpen zijn vrijheden gelasten aan organisaties in de keuze voor bepaalde grondslagen. Indien de RJ een bepaalde situatie niet behandelen, dan moet het bestuur een verwerkingswijze kiezen die relevante en betrouwbare informatie oplevert voor de besluitvorming van de gebruikers van de jaarrekening. Zie ook: Stelselwijzigingen

Integere bedrijfsvoering het handelen binnen de kaders van wet- en regelgeving met inventief gebruik van professionele expertise. Kenmerkend voor een integere organisatie is het tegengaan van belangenverstrengeling, corruptie, fraude, wetsovertredingen en/of andere handelingen die maatschappelijk ongewenst zijn.

Internal auditor een natuurlijk persoon die in dienst is van de organisatie en beroepsmatig beoordeelt in welke mate zijn organisatie erin slaagt om het bedrijfsproces en de daarmee samenhangende risico's te beheersen. De internal auditor helpt een organisatie haar doelstellingen te realiseren door op basis van een systematische en gedisciplineerde aanpak de effectiviteit van de processen van governance, risicomanagement en beheersing te evalueren en te verbeteren.

Interne beheersing het proces dat is opgezet, wordt geïmplementeerd en onderhouden door het bestuur en het toezichthoudend orgaan, het management en andere werknemers met als doel een redelijke mate van zekerheid te verschaffen dat de doelstellingen van de organisatie met betrekking tot de betrouwbaarheid van de financiële verslaggeving, de effectiviteit en efficiëntie van de activiteiten alsmede de naleving van de van toepassing zijnde wet- en regelgeving worden bereikt. Interne beheersing bestaat uit:

- het interne beheersingssysteem zelf: welke maatregelen zijn getroffen om de organisatie als geheel aan te sturen?
- de inhoud van het beheersingssysteem: de kwaliteit van de diverse beheersmaatregelen die zeker moeten stellen dat doelen en normen worden gerealiseerd.

Goed ingerichte processen in combinatie met een zorgvuldig vormgegeven systeem voor interne beheersing is cruciaal om als organisatie "in control" te zijn. Om adequaat te kunnen sturen en de (fraude)risico's binnen een organisatie te beheersen.

Interne gedragscode een interne gedragscode maakt duidelijk wat van iedereen binnen de organisatie wordt verwacht en wat van de organisatie mag worden verwachten en welk gedrag je wel en niet accepteert. Als de normen en waarden voor iedereen duidelijk zijn, voorkom je discussies en draagt dit bij aan een betere werksfeer. Een interne gedragscode kan nooit in elke denkbare situatie voorzien, maar doet onder andere een beroep op verantwoord, vertrouwelijk, transparant, zorgvuldig en onpartijdig handelen van werknemers. Integriteit gaat pas werkelijk leven in de dagelijkse praktijk en in de gesprekken die je met elkaar hierover voert.

Klokkenluiders(regeling) een klokkenluider stelt misstanden in een organisatie aan de kaak. Werkgevers met 50 werknemers of meer moeten een procedure hebben voor het melden van een (vermoeden van een) misstand bij de werkgever. De beschreven verplichting van een interne klokkenluidersregeling is onderdeel van de Wet huis voor klokkenluiders en het doel is de voorwaarden voor het melden van maatschappelijke misstanden binnen organisaties te verbeteren, door onderzoek naar misstanden mogelijk te maken en de klokkenluider beter te beschermen. In uw klokkenluidersregeling staat beschreven hoe u binnen uw organisatie omgaat met het melden van een vermoeden van een misstand.

Meldplicht de verplichting om volgens wet- of regelgeving gebeurtenis of overtreding van een wet of regel te melden aan een specifieke instantie. Daarnaast is het ook mogelijk dat op basis van een gedragscode over te gaan tot een interne melding c.q. signalering als sprake is van een specifieke situatie.

Ondernemingsraad organisaties met 50 werknemers of meer moeten een ondernemingsraad (OR) hebben. Een OR is een inspraak- en medezeggenschapsorgaan binnen een organisatie en bestaat uit werknemers die namens het personeel overleg voeren met de werkgever over het ondernemingsbeleid en de personeelsbelangen. In de Wet op de ondernemingsraden zijn de rechten en plichten van de OR vastgelegd.

Organisatie in dit document wordt de term "organisatie" gebruik, hier kan ook onderneming, non-profit organisatie, instelling of entiteit worden gelezen.

Privacywetgeving In artikel 10 van de Grondwet is het recht op privacy geregeld: 'Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.' In andere wetten staan regels over wat wel en niet mag in het kader van privacy. De belangrijkste is de Algemene Verordening Gegevensbescherming (AVG), deze geldt in de hele EU en geldt voor alle organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen uit de EU. In Nederland houdt de Autoriteit Persoonsgegevens (AP) toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.

Schattingen (hoofdstuk 10) de organisatie schat de omvang van bijvoorbeeld een post in de jaarrekening zo goed mogelijk bepaald, rekening houdende met alle beschikbare relevante informatie. Als gevolg van onzekerheden zijn schattingen noodzakelijk. Het kan nodig zijn om een eerder gedane schatting te herzien. Dit kan noodzakelijk zijn op grond van wijzigingen in de omstandigheden waarop de schatting is gebaseerd of het beschikbaar komen van nieuwe informatie.

Stelselwijzigingen (hoofdstuk 10) de organisatie kiest ervoor om een eerder gekozen stelsel te wijzigen Eén of meer grondslagen en/of regels zijn anders dan die welke bij de opstelling van de voorafgaande jaarrekening zijn gebruikt. Een dergelijke wijziging is maar beperkt toegestaan omdat consistentie in een reeks jaarrekeningen van groot belang is en omdat vermeden moet worden dat de grondslagen steeds in het voordeel van de opsteller worden gewijzigd.

Tone at the top het gedrag en de houding van het topmanagement, waaronder het bestuur en het toezichthoudend orgaan van een organisatie, waarbij het goede voorbeeld wordt gegeven.

Vertrouwenspersoon een persoon binnen een organisatie, aan wie men vertrouwelijke zaken, zoals misstanden en integriteitsschendingen kwijt kan. Ook kan de vertrouwenspersoon ongewenste omgangsvormen als pesten, intimidatie en discriminatie op het werk aanpakken en voorkomen. De integriteit en vertrouwelijkheid staan hierin centraal. Het contact moet voor de werknemer veilig zijn.

Zerotolerance beleid een beleid waarbij zelfs het kleinste vergrijp (hard) bestraft wordt.