

ARTIKELN | 5 OKTOBER 2019

FRAUDERISICOMANAGEMENT: WAT MAG VAN EEN INTERNAL AUDITOR WORDEN VERWACHT?

Auteur: Noortje de Rooij MSc RO – Mike Broekhof MSc – Maud Nijhuis MSc

Beeld: Michael Rogers – Nijwam Swargiary

Leestijd: 8 min



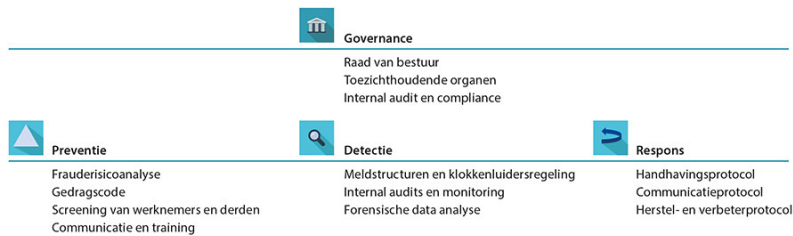
Als een donderslag bij heldere hemel. Zo voelt het voor veel organisaties als zij worden geconfronteerd met fraude. Maar kon een organisatie het echt niet zien aankomen of was zij onvoldoende bedacht op frauderisico's?

De maatschappij verwacht steeds meer van organisaties op het gebied van preventie en detectie van fraude. Hiermee komt ook steeds meer druk te liggen op fraudeafdelingen en internal auditfuncties (IAF's). Niet geheel onterecht, want uit onderzoek van KPMG blijkt dat 61% van de onderzochte fraudecases heeft kunnen gebeuren door gebrekkige interne controles. Echter, slechts 14% van de ontdekte fraudegevallen wordt gesignaleerd door IAF's.

Uit een later onderzoek van KPMG blijkt dat internal auditors moeite hebben met het structureel detecteren van fraude. Zie ook *figuur 1* voor het Frauderisico Management Raamwerk van KPMG. De vraag die opkomt is dan ook: wat wordt er nu eigenlijk verwacht van de internal auditor ten aanzien van preventie, detectie en opvolging van fraude?

AUDIT

MAGAZINE



Figuur 1. KPMG Frauderisico Management Raamwerk

Principes van frauderisicomangement

In dit artikel belichten wij de belangrijkste principes van frauderisicomangement door de lens van de IAF, zoals mede voorgeschreven door het IIA. Wij besteden aandacht aan de governance, het uitvoeren van een frauderisicoanalyse, preventieve, detectieve en responsieve maatregelen, en het geven van opvolging aan vermoedens van fraude.

Wanneer is sprake van fraude?

Ondanks dat fraude een veelgebruikte term is en we er regelmatig over lezen in kranten, bestaat toch vaak verwarring over wat nu wel of geen fraude is. Dit komt door een dunne scheidslijn tussen integriteit en fraude. In de auditwereld wordt fraude gedefinieerd als een opzettelijke handeling waarbij gebruik wordt gemaakt van misleiding om zo een onrechtmatig of onwettig voordeel te verkrijgen. In de praktijk blijkt dat het lastig is aan te tonen dat er sprake is van opzet. Dit komt vaak door gebrekkige interne beheersing en een laag fraudebewustzijn, waardoor het mogelijk is af te wijken van de processen zonder dat dat opzettelijk is. Dit benadrukt nogmaals het belang van het goed inrichten van frauderisicomangement en het belang van de rol van internal auditors.

Het implementeren van frauderisicomangement vraagt kennis, tijd en budget, maar dat is wel de basis voor het voeren van een integere bedrijfsvoering

De verantwoordelijkheid van de IAF

Dat in het internal audit charter de verantwoordelijkheden van de IAF zijn vastgelegd, is een professional wel bekend. Echter, in welke mate is hierin ook de verantwoordelijkheid ten aanzien van fraude opgenomen? De basis hierin zou moeten zijn dat de IAF voldoende kennis heeft om frauderisico's en de manier waarop die risico's beheerst worden door de organisatie te beoordelen.

Daarnaast moet een internal auditor conform de IIA Standaarden met zorgvuldigheid handelen door rekening te houden met de waarschijnlijkheid van belangrijke fouten, fraude of niet-naleving van wet- en regelgeving. Ook de kans op het bestaan van fraude en de wijze waarop de organisatie frauderisico's beheerst, moeten zij evalueren. Tot slot zou het hoofd van de IAF periodiek moeten rapporteren over risico's, inclusief frauderisico's, aan het management, de auditcommissie en het bestuur.

Vastleggen

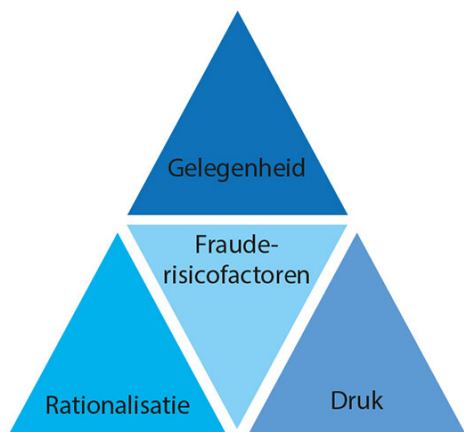
Indien de IAF ook verantwoordelijk is voor het uitvoeren van fraudeonderzoeken is het van belang dat dit is vastgelegd in het audit charter. Uit de praktijk blijkt dat in menig situatie audit charters en handboeken nog onvoldoende aandacht besteden aan de taken en verantwoordelijkheden van de IAF ten aanzien van fraude. Om verantwoordelijkheid te nemen en te voldoen aan de IIA Standaarden is het van belang dat audit charters en handboeken explicieter beschrijven wat internal audit wel, maar ook niet doet ten aanzien van fraude. Zeker daar waar het aankomt op het wel of niet uitvoeren van onderzoeken bij vermoedens van fraude.

Soms is de anonimiteit bij een meldstructuur niet gewaarborgd. Daarnaast weten medewerkers en zelfs internal auditors vaak niet wat de meldprocedure is binnen hun organisatie

Waarom volstaat een 'gewone' risicoanalyse niet?

Wat wij veel waarnemen bij organisaties is dat frauderisico's vaak wel impliciet worden meegenomen bij het uitvoeren van een risicoanalyse tijdens de start van een audit. Echter, frauderisico's worden niet expliciet geïdentificeerd voordat het audit jaarplan wordt opgesteld of tijdens het vooronderzoek van een audit. Fraude wordt door internal auditors veelal meegenomen als algemeen risico bij het uitvoeren van een risicoanalyse.

Fraude vereist echter een andere wijze van risico-inventarisatie, omdat bijvoorbeeld ingerichte beheersmaatregelen worden omzeild of informatie wordt gemanipuleerd door middel van vervalsing. Het uitvoeren van een aparte (periodieke) frauderisicoanalyse is een belangrijke stap in het opzetten en uitvoeren van een adequaat frauderisicobeleid. Dit doe je door eerst de frauderisicofactoren druk, gelegenheid en rationalisatie te identificeren alvorens je echte frauderisico's in kaart brengt (zie figuur 2).



Figuur 2. Frauderisicofactoren

Gelegenheid

Druk kan worden gecreëerd door bijvoorbeeld het moeten behalen van hoge targets. Maar ook persoonlijke financiële problemen kunnen van invloed zijn op het gedrag van mensen. Met gelegenheid wordt bedoeld de mogelijkheid die iemand heeft, al dan niet door een gebrekkige interne controle, fraude te plegen. Tot slot zorgt rationalisatie ervoor dat mensen hun eigen gedrag goedpraten, waardoor ze over de streep gaan. Dit kan worden getriggerd door de cultuur, waarin de baas ook afwijkt van de regels, of men het gevoel heeft oneerlijk te worden behandeld of onvoldoende waardering ervaart. Op basis van de geïdentificeerde frauderisicofactoren kan nader onderzocht worden welke frauderisico's van toepassing zijn.

Fraudebewustzijn is beperkt

Het management is uiteraard primair verantwoordelijk voor het inrichten van preventieve maatregelen. Dit begint bij het inrichten van screening van medewerkers, leveranciers en klanten. Daarnaast is het creëren van fraudebewustzijn van groot belang. Onze ervaring is dat financiële instellingen zich over het algemeen wel bewust zijn van frauderisico's, hetgeen gecreëerd wordt vanuit noodzaak door toezichthouders, maar ook door de grote hoeveelheid geld die binnen

deze sector omgaat.

Cultuur in een organisatie

Binnen corporates en non-profitorganisaties zijn medewerkers zich vaak minder bewust van fraude, of vooral gericht op externe fraude, maar niet op interne fraude. Dit komt, omdat veel organisaties berusten op vertrouwen. Het creëren van het bewustzijn begint allemaal met de cultuur binnen een organisatie. In hoeverre zijn soft controls aanwezig en in welke mate dragen deze bij aan effectief frauderisicomanagement. Er is bijna geen organisatie die nog geen gedragscode heeft, maar leeft deze ook? Communicatie en training zijn van groot belang om fraudebewustzijn te creëren.

Een e-learning is een effectief middel om het onderwerp bij alle medewerkers onder de aandacht te brengen. Tevens biedt dit de mogelijkheid om via de e-learning medewerkers te laten verklaren dat zij zich houden aan de gedragscode.

Fraudeurs sterven nooit uit. Dat komt doordat omstandigheden ertoe leiden dat goede mensen soms de verkeerde dingen doen

Rol van de internal auditor

Wat kan de internal auditor doen aan het creëren van bewustwording? Het begint al met de kennis die auditors hebben op het gebied van fraude en soft controls. Zijn zij in staat de frauderisico's te identificeren en hebben zij voldoende gevoel bij de cultuur van een organisatie, wat mogelijk een frauderisicofactor kan zijn? Het is van belang dat fraude bespreekbaar wordt gemaakt tussen de internal auditor en het management.

In de praktijk zien wij dat het hoger management meer aandacht krijgt voor fraude. Echter, internal auditors voelen zich nog niet altijd comfortabel bij het bespreken van het onderwerp met het management of het audit committee. Dit wordt vaak veroorzaakt door angst voor weerstand en het verzoek tot het doen van extra werkzaamheden waarvoor weinig tijd, capaciteit en kennis beschikbaar is. IAF's doen er verstandig aan om te beginnen met het zichzelf eigen maken van het onderwerp en dilemma's bespreekbaar te maken met elkaar.

Tot slot gaat het natuurlijk om het inrichten en implementeren van effectieve beheersmaatregelen. Preventieve maatregelen kunnen niet altijd voorkomen dat fraude gepleegd wordt, maar het is wel de basis om frauderisico's te mitigeren. Als preventieve beheersmaatregelen aanwezig zijn, deze effectief werken en algemeen bekend zijn, dienen ze als grote barrière voor potentiële fraudeurs.

AUDIT

MAGAZINE



IAF: de ogen en oren van de organisatie

Internal audit heeft een belangrijke rol in het (tijdig) detecteren van mogelijke fraude. Potentiële fraude kan op meerdere manieren binnen een organisatie aan het licht komen. Kan verdacht of ongewenst gedrag anoniem gemeld worden? Het is belangrijk dat organisaties medewerkers een kanaal bieden om schendingen te melden. Door het inrichten van een meldstructuur en klokkenluidersregeling kunnen medewerkers en derde partijen op een veilige manier een melding maken. Door gebruik te maken van in de organisatie verankerde meldpunten, draagt dit ook bij aan geanonimiseerde managementinformatie. Dit geeft een beeld van wat er binnen de organisatie speelt en waar de gaten zitten.

Waarborgen anonimiteit

Onze ervaring is dat soms de anonimiteit bij een dergelijke meldstructuur niet gewaarborgd is. Daarnaast weten medewerkers en zelfs internal auditors vaak niet wat de meldprocedure is binnen hun organisatie. Zeker voor internal auditors is het van belang te weten wanneer en waar ze een mogelijk vermoeden van fraude kunnen melden. Dit omdat een internal auditor in de uitgelezen positie zit fraude te ontdekken.

Het is uiteraard niet de primaire doelstelling tijdens het uitvoeren van een audit, maar gezien de kennis van de organisatie, inzicht en toegang tot processen en systemen en de vele interviews met medewerkers, hebben internal auditors veel kennis en informatie om fraude mogelijk te detecteren. Wat daarbij helpt is het gebruik van data-analyse. Hoewel de afgelopen jaren data-analyse vaker wordt ingezet, wordt nog steeds beperkt gebruikgemaakt van forensische data-analyse.

Medewerkers en zelfs internal auditors weten vaak niet wat de meldprocedure is binnen hun organisatie

Door middel van een goede frauderisicoanalyse worden scenario's geschetst die getoetst kunnen worden aan de hand van forensische data-analyse. Dit is een hele effectieve manier om ongestructureerde data te analyseren en vast te stellen of fraudescenario's mogelijk zijn. Het gebruik van forensische data-analyse is een tastbaar middel voor internal auditors om inzicht te bieden in welke mate frauderisico's effectief worden beheerst.

Wat als er een vermoeden van fraude is?

In hoeverre zijn er specifieke, gedocumenteerde instructies waaruit blijkt hoe een onderzoek naar een mogelijke fraude gevoerd moet worden? Het is van belang dat de wijze waarop onderzoek wordt gedaan bij vermoedens van fraude zijn vastgelegd in een onderzoeksprotocol. Dit protocol beschrijft wie verantwoordelijk is voor de uitvoering van het onderzoek en zorgt voor een consistente werkwijze, wat uitermate belangrijk is, zeker indien er juridische opvolging gegeven moet worden aan de melding.

In de praktijk zien wij dat het voorkomt dat IAF's verantwoordelijk zijn voor het uitvoeren van onderzoeken bij vermoedens van fraude. Dit zorgt voor een uitdaging, omdat internal auditors over het algemeen maar beperkte kennis en ervaring hebben in het doen van dergelijke onderzoeken. Daarnaast moet je als internal auditor met twee petten acteren, de ene keer als politieagent (zoals bij vermoedens van fraude), de andere keer als adviseur. Wat doet dit met het vertrouwen tussen de auditor en auditee? Het tijdig betrekken van de juiste expertise is daarom van belang.

Verschillende soorten protocollen

Een handhavingprotocol beschrijft tot welke gevolgen misstanden en fraude kunnen leiden, hetgeen essentieel is om herhaling van een incident te voorkomen. Uiteraard is het belangrijk niet alleen een protocol op te stellen, maar ook werkelijk sanctioneringsmaatregelen te nemen. Dit heeft ook een preventieve werking richting mogelijke andere fraudeurs.

Mocht er fraude hebben plaatsgevonden, dan is het van belang dat de juiste informatie wordt gedeeld. In een communicatieprotocol is vastgelegd hoe interne en externe communicatie plaatsvindt. Tot slot wil je als organisatie natuurlijk leren van fraudes, daarom is het van belang dat er een analyse wordt gedaan op het proces dan wel de cultuur waarbinnen de fraude heeft kunnen plaatsvinden. Het herstel- en verbeterprotocol beschrijft wat gedaan moet worden om vergelijkbare misstanden te voorkomen.

Waar te beginnen?

Het implementeren van frauderisicomanagement vraagt kennis, tijd en budget, maar dat is wel de basis voor het voeren

AUDIT

MAGAZINE

van een integere bedrijfsvoering. Internal audit kan hierbij een belangrijke rol spelen door te onderzoeken in welke mate frauderisicomanagement is ingebed in de organisatie. Daarnaast is het belangrijk dat de taken en verantwoordelijkheden van de IAF ten aanzien van fraude zijn vastgelegd in de audit charter en het internal audit handboek. Voer een jaarlijkse, organisatiebrede, frauderisicoanalyse uit en update deze periodiek. Probeer hierbij te denken als een fraudeur binnen ieder proces dat je audit. De frauderisicoanalyse is het vertrekpunt voor het denken in scenario's, wat de basis vormt voor een goede forensische data-analyse.

Fraudeurs zullen nooit uitsterven. Dat komt doordat omstandigheden ertoe leiden dat goede mensen soms de verkeerde dingen doen. Internal auditors moeten zich daarom extra bewust zijn van de omstandigheden waar binnen medewerkers opereren.

Over

Noortje de Rooij is senior manager bij KPMG Advisory en ondersteunt internal auditfuncties bij fraudepreventie, detectie en respons. derooij.noortje@kpmg.nl

Mike Broekhof MSc is manager bij KPMG Advisory en voert feitenonderzoeken uit en biedt forensische auditondersteuning. broekhof.mike@kpmg.nl

Maud Nijhuis MSc is consultant bij KPMG Advisory en voert feitenonderzoeken uit. nijhuis.maud@kpmg.nl

Tags: Risicomanagement

Bron url: <https://auditmagazine.nl/artikelen/frauderisicomanagement-wat-mag-van-een-internal-auditor-worden-verwacht/>