voka

WIJZER

OKTOBER 2017

GIDS
OM UW ONDERNEMING TE BESCHERMEN TEGEN FRAUDE

FRAUDEPREVENTIE IN UW ONDERNEMING

Een uitgave van **Voka** vzw | Jaargang 7 – Oktober 2017 | Afgiftekantoor Gent x – Erkeningsnummer P708123

Voorwoord

Fraude brengt bedrijven schade toe, meer dan u als ondernemer misschien zou denken. Van de bedrijfsinkomsten verdampt gemiddeld vijf procent door fraude.[1] Zonder fraude zou de winstgevendheid kunnen verdubbelen tot 10 procent van de omzet.[2]

De meeste bedrijfsleiders denken dat dit niet voor hun onderneming geldt, omdat ze ervan overtuigd zijn dat ze zelden last hebben van fraude. Dat is een denkfout die ontstaat doordat veel fraude onontdekt blijft. Fraude wordt vaak pas zichtbaar als ze groot is geworden. Zolang de fraude niet gemerkt wordt, kan de fraudeur doorgaan. Bedrijven moeten dus niet alleen maatregelen treffen om fraude te voorkomen, maar ook maatregelen om gebeurlijke fraude op tijd te detecteren.

De antifraudemaatregelen die in deze gids worden besproken, zijn niet zomaar gekozen. Het gaat namelijk over de meest effectieve antifraude-acties: bedrijven die deze maatregelen hebben getroffen, lijden aantoonbaar minder schade.[2]

Bovendien is een bedrijf met een helder antifraudebeleid duurzamer en aantrekkelijker als werkgever en voor alle belanghebbenden – klanten, leveranciers, aandeelhouders, ... Last but not least beperkt een zichtbaar antifraudebeleid het risico op aansprakelijkheid van de vennootschap en haar bestuurders.

De auteurs van deze Voka Wijzer – Sonny Luypaert en Evert-Jan Lammers van advies- en onderzoeksbureau EBBEN Partners en Dylan Casaer en Kristof De Creus van advocatenkantoor Olislaegers & De Creus – weten door hun achtergrond en hun ervaring welke stappen bedrijven moeten zetten. Met deze gids willen we bedrijven ervan overtuigen dat het belangrijk is om zich te wapenen tegen fraude. We zetten de belangrijkste fraudeproblemen en de absolute must-do antifraudemaatregelen op een rij en we reiken ook een handige checklist aan, die het voor elke onderneming mogelijk maakt om te evalueren of ze er klaar voor is om fraude-incidenten snel en efficiënt aan te pakken.

"Met deze gids willen we bedrijven ervan overtuigen dat het belangrijk is om zich te wapenen tegen fraude."

EBBEN PARTNERS

Olislaegers & De Creus advocaten - avocats

Lees meer over de auteurs op pagina 45.

Hans Maertens
Gedelegeerd bestuurder Voka - Vlaams netwerk van ondernemingen

"Een bedrijf met een antifraudebeleid is duurzamer en aantrekkelijker als werkgever en voor alle belanghebbenden - klanten, leveranciers aandeelhouders, ..."

inhoud

2 Voorwoord

4 Inleiding

5 Fraudevarianten

20 Antifraudemaatregelen

31 Frauderesponsplan

34 Zelftest

37 Welke maatregelen voor welke fraude?

38 Een selectie van juridische topics

44 Bronnen

45 Over de auteurs

Inleiding

Deze gids gaat over de maatregelen die u kunt treffen om fraude te voorkomen en tijdig te ontdekken. Het gaat om loyale medewerkers die al jaren in uw onderneming werken en die u volledig vertrouwt. Medewerkers die betrokken zijn bij fraude hebben altijd dit profiel, omdat ze bevoegdheden hebben én onverdacht zijn, zoals Hans, Hilde en Hugo.

SCHADE DOOR FRAUDE WORDT VEROORZAAKT VIA ONVERDACHTE PERSONEN

De zoon van **Hans** heeft een uitzonderlijke ziekte die handenvol geld kost en die Hans met moeite kan bekostigen. Hans nam telkens geld uit de bedrijfskas, en wilde dat later terugbetalen. De 'lening' was opgelopen tot 60.000 euro.

Hilde had een vertrouwenspositie. Daarom viseerde een criminele organisatie haar voor een CEO-fraude. Zij dacht dat u haar had gevraagd om die spoedbetaling van 300.000 euro voor te bereiden.

Hugo was onvervangbaar. U vroeg hem om in het weekend van thuis uit een offerte naar u te mailen. De huis-router was onbeveiligd, en uw concurrent won de offerteprocedure. Schade: 550.000 euro.

Fraudeurs maken misbruik van het vertrouwen en van de zwakke plekken in de organisatie. Zwakke plekken kunnen in de structuur, de cultuur of het gedrag zitten. Wanneer bijvoorbeeld een belangrijke functiescheiding ontbreekt of als medewerkers elkaar niet aanspreken op fout gedrag, spreken we van een zwakke structuur. Ook het aanvaarden van dure cadeaus is een teken van zwak gedrag.

Functiescheiding: het toewijzen van taken en bevoegdheden aan verschillende personen, zodat interne controle mogelijk wordt. Het gaat vooral om de volgende functies: uitvoering - bewaring - registratie - controle.

In al die gevallen hebben we het over een verhoogd frauderisico. Als fraude plaats vindt, spreken we niet van een accident (per ongeluk, ondanks de sterktes) maar van een incident (onvermijdelijk, gezien de zwaktes).

Een antifraudebeleid dient ter compensatie van dergelijke zwakke plekken die elk bedrijf wel heeft, het ene bedrijf al wat meer dan het andere.

Deze Voka Wijzer toont achtereenvolgens:

- van welke vormen van fraude bedrijven last hebben (Hoofdstuk 1)
- wat de meest effectieve antifraudemaatregelen zijn (Hoofdstuk 2)
- hoe u moet handelen in geval van een vermoeden van fraude (Hoofdstuk 3)
- of u de belangrijkste antifraudemaatregelen al hebt genomen (Hoofdstuk 4)
- welke maatregelen bij welke fraudetypen horen (Hoofdstuk 5)
- met welke belangrijke juridische overwegingen u rekening moet houden (Hoofdstuk 6).

Naleving van de aanbevelingen in deze gids biedt extra bescherming aan vennootschappen en bestuurders tegen aansprakelijkheid in geval van fraude. De aanbevelingen sluiten aan bij internationale standaarden[6,7] en nationale regels[8,9].

We richten ons op het Belgische bedrijfsleven in zijn algemeenheid, en we gaan niet specifiek in op de typische fraudegevoeligheden van bepaalde sectoren, zoals e-commerce, banken en verzekeringen.

Evenmin wordt dieper ingegaan op bepaalde fraudevarianten. Zo verwijzen wij voor een diepgaande behandeling van cybersecuritymaatregelen naar de Belgische Gids voor Cyberveiligheid uit 2014[8]; voor een grondige behandeling van anticorruptiemaatregelen naar de Anticorruptiegids voor Belgische Ondernemingen in het Buitenland uit 2016[9]; en voor een gedetailleerde behandeling van de juridische context naar de Belgische gids Strafrecht in de onderneming uit 2016[11].

1. Fraudevarianten

Fraude is geen wettelijk begrip, maar een containerbegrip voor tientallen fraudevarianten. Alle varianten hebben de volgende kenmerken: ze zijn opzettelijk, ze worden verborgen om ontdekking te voorkomen, en ze veroorzaken schade. In deze compacte gids behandelen we tien fraudevarianten die samen een goed beeld geven van fraude.

Vooral het opgezet spel leidt tot emotionele en verdedigende reacties achteraf: "Je moet je medewerkers toch kunnen vertrouwen?" Zeker, geen enkel bedrijf kan functioneren zonder een basis van vertrouwen. Tegelijk moet het bedrijf zich bewust zijn van de risico's die daarmee samenhangen, en maatregelen nemen.

Dit bewustzijn begint met het verzamelen van voldoende kennis over fraude. Daarom beschrijven we hieronder de voornaamste varianten. Voor meer fraudevarianten, verwijzen we naar de bronnen achterin.

CYBERCRIME	1.1 Lekken en hacken 1.2 Identiteitsfraude
AANKOPEN EN VERKOPEN	1.3 Conflicterende belangen 1.4 Manipulatie van offerteprocedures 1.5 Omkoping in het buitenland
MISBRUIK EN DIEFSTAL	1.6 Bedrijfsmiddelen en voorraden 1.7 Financiële middelen
VERSLAGGEVINGSFRAUDE	1.8 Financiële rapportages 1.9 Werving en selectie 1.10 Niet-financiële rapportages

Deze selectie sluit aan bij de dagelijkse praktijk, bij gezaghebbende gidsen zoals Strafrecht in de Onderneming (2016)[11], Report to the Nations (2016)[1] en Fraud Risk Management Guide (2016)[10] en bij de keuze van de auteurs.

De indeling van de volgende paragrafen is telkens als volgt: Risico's - Oorzaken - Fraudetechnieken - Voorbeeld - Varianten.

1.1 Lekken en hacken

Risico's

Uw bedrijf werkt soms dagen aan een offerte, weken aan een target of maanden aan een nieuwe technologie of product. Het lekken van sleutelinformatie of een inbraak in uw computersysteem kunnen het verlies betekenen van de aanbesteding, het verdwijnen van de target of het verspelen van het concurrentievoordeel. Bedrijfsspionage kan overal en op alle niveaus gebeuren.

Bijzondere varianten, zoals trojans en ransomware, kunnen bedrijfsprocessen stilleggen en de veiligheid van producten en diensten in gevaar brengen. Ze worden vaak verspreid via e-mails en chatprogramma's. In het voorjaar van 2017 deed dit zich voor het eerst op wereldschaal voor: een criminele organisatie perste in meer dan honderd landen bedrijven af door te dreigen met het deleten van de data op de computer (wannacry virus). Plots bleken bedrijven perfect te weten hoe ze dit hadden kunnen voorkomen, echter die kennis was vaak niet gedeeld of toegepast.

TROJAN EN RANSOMWARE

Een trojan is een functie die verborgen zit in een computerprogramma dat door de gebruiker wordt geïnstalleerd. De functie kan zelfstandig schade toebrengen aan computer, data en privacy.

Ransomware is kwaadwillige software die de computer en/of de data van het slachtoffer blokkeert. Meestal wordt er een betaling gevraagd om te deblokkeren, wat echter in veel gevallen niet helpt.

Oorzaken

De oorzaken van lekken en hacken zijn divers: een personeelslid praat zijn mond voorbij over de prijs in een uitgebrachte offerte; een jonge manager laat zijn laptop 's avonds voor het restaurant in de auto liggen; een directeur vindt het handig dat het secretariaat over zijn paswoord beschikt; een medewerker klikt op een phishing-mail en geeft zo ongewild toegang tot zijn computer of tot het systeem. Deze situaties kunnen door een slordigheid gebeuren, maar ze kunnen ook worden uitgelokt of afgedwongen middels bepaalde fraudetechnieken.

Cybersecurity schreeuwt om aandacht

Meer dan de helft van de personeelsleden opent e-mails van onbekende afzenders. Een substantieel deel opent de link in zo'n e-mail en geeft vervolgens zelfs zijn pincode of paswoord in.

Fraudetechnieken

Een fraudeur is een individu. Vaak gebruikt hij trucs en technieken om de fraude te plegen. Een personeelslid kan per ongeluk zijn mond voorbijpraten, dat is dan een accident. Maar een personeelslid zal zich niet zomaar verspreken. Als

dat gebeurt, bestaat de kans dat hij werd misleid, verleid, opgelicht, omgekocht, gechanteerd, ... om de vertrouwelijke informatie te geven.

VERTROUWELIJKE DATA

Uw bedrijf werkt aan een nieuw product op basis van een nieuwe technologie. Hilde is een trouwe medewerkster, werkzaam bij productontwikkeling. Hilde heeft een vriendin met wie ze regelmatig over haar werk spreekt. Zo krijgt de echtgenoot van deze vriendin lucht van het nieuwe product. Hij besluit om voor de beide koppels samen een wandelweekend in de Ardennen te organiseren. Na het zondagontbijt vraagt hij Hilde om haar laptop, zogenaamd om zijn e-mails te checken. Ongezien kopieert hij vertrouwelijke data naar een usb-stick en verkoopt deze aan uw grootste concurrent.

Hilde had die vertrouwelijke data niet op haar laptop mogen zetten, maar dat doet ze altijd om er in het weekend aan te kunnen werken. Evenmin had ze haar laptop mogen uitlenen aan een derde, maar zij zat aan de ontbijttafel in hetzelfde vertrek als hij. De data waren beveiligd met een paswoord maar niet geëncrypteerd.

Door middel van eenvoudige screeningapparatuur wordt genadeloos zichtbaar of er een laptop/tablet ligt in de auto die is geparkeerd voor het bedrijf, de supermarkt, het restaurant, de cinema, of de woning. Wachtwoorden kunnen op vele manieren worden gekraakt of ontfutseld, niet in de laatste plaats omdat we er slordig mee omgaan; we delen ze zelfs met collega's!

Encryptie
Encryptie ('versleutelen') betreft de beveiliging van data op een computer op basis van een bepaald algoritme ('sleutel') die de geautoriseerde gebruikers slechts aan elkaar bekend maken. De versleutelde gegevens kunnen nadien gedecrypteerd worden, zodat men de originele informatie weer terugkrijgt.

Varianten
- Ongeautoriseerd meenemen van vertrouwelijke informatie naar een volgende job.
- Een bevriende partij informeren over een aanbesteding/offerte.
- Paswoord delen met collega, tijdens vakantie, etc.

1.2 Identiteitsfraude

Risico's

Identiteitsfraude gaat een stap verder dan hacken. Bij hacken probeert de hacker ongezien binnen te komen via de zwakke plekken in het systeem, terwijl bij identiteitsfraude de hacker tracht om niet op te vallen door zich in het systeem voor te doen als een geautoriseerde gebruiker. De fraudeur kan een collega zijn of een externe partij. De gevolgen zijn afhankelijk van de verkregen informatie en van de bedoelingen van de fraudeur. Ze kunnen technisch zijn, commercieel, financieel of operationeel en ze kunnen ook leiden tot reputatierisico, continuïteitsrisico, maatschappelijke risico's en aansprakelijkheid. We hebben het over de hoogste risicocategorie. De verwachting is dat ransomware (1.1) en identiteitsfraude (1.2) in de komende jaren een hoge vlucht gaan nemen.

Oorzaken

Het gaat erom dat de geautoriseerde persoon niet merkt dat zijn account wordt benut door een ongeautoriseerde fraudeur. Vaak heeft het bedrijf niet genoeg technische maatregelen getroffen (structuur), is het personeel onvoldoende bewust gemaakt van de gevaren (cultuur), en let de geautoriseerde persoon niet goed op (gedrag).

Fraudetechnieken

De gehanteerde technieken variëren naargelang het doel van de fraudeur. Om een paar duizend euro te stelen van een bankrekening, moet de fraudeur slechts beschikken over de pincode en de bankpas van het bedrijf. Bij sommige bedrijven kan de bankkaart door meerdere personen worden gebruikt, is deze voor meerdere personen toegankelijk en is de code bij meerdere personen gekend. Middels een CEO-fraude kunnen grotere bedragen worden gestolen, maar dit vereist een meer professionele aanpak en voorbereiding van de fraude.

CEO-FRAUDE

From: Hugo.De.Mol<HDM@M0LBROUW.be>
Sent: 13 April 2017 09:34
To: Hilde.Van.Maes<HVM@Molbrouw.be>
Copy: Irena Vjildip<Irena.Vjildip@SplitLaw.cz>
Subject: Betaling

Goedemorgen Hilda,
Het volgende is vertrouwelijk. We nemen een brouwerij over in Tsjechië. De naam mag ik je nog niet geven. Beloof me dat je er met niemand over spreekt, ook niet met mij of met Gert of de andere bestuurders. Morgen moeten we 300.000 EUR betalen op rekening XXXXXXXXXXXX op naam van Splitlaw onze advocaten in Praag. Als je meer informatie nodig hebt, contacteer dan Irena Vjildip, onze advocate, zij leest ook Nederlands. Kun je die betaling vandaag voorbereiden en me een seintje geven?
HDM

Bij CEO-fraude merken we niet dat het e-mailadres van de verzender een leesteken afwijkt (M0LBROUW met een 0 in plaats van en O). Social engineering is een sleutelcomponent van CEO-fraude: het manipuleren van een sleutelfiguur, in dit geval Hilde. De oplichters hadden eerst de mailserver van Molbrouw gehackt om de interne communicatie en de betalingsprocedure te bestuderen.
De e-mailadressen van Hugo en Irena zijn vals, maar die ene '0' valt niet op. Hugo is de enige die Hilde altijd Hilda noemt en hij ondertekent meestal met HDM. Uiteraard reageren Irena en Hugo vlot op de vragen van Hilde. Dan stuurt Hilde het sein dat de betaalopdracht getekend kan worden ...
Deze fraude was mogelijk dankzij het ontbreken van dubbele handtekeningsbevoegdheid (structuur). Gegeven deze zwakke plek, het grote bedrag en de bijzondere omstandigheid was Hilde te volgzaam (cultuur). Ondanks haar sleutelpositie had Hilde nooit een training ontvangen over fraude (gedrag).

Varianten
- Diefstal van bankkaart/badge met pincode.
- CEO-fraude (ook: Presidents fraud).
- Verwisselen van toegangsbadges.

1.3 Conflicterende belangen

Risico's

Directie, personeel en ingehuurde krachten moeten handelen in het belang van het bedrijf. Deze verplichting heeft een contractuele basis: arbeidscontract, managementcontract, inhuurcontract, SLA, ... Wanneer deze verplichting niet wordt nageleefd, kan het bedrijf opdrachten mislopen, te duur inkopen, te veel korting weggeven, ongeschikt personeel in dienst nemen, ongeschikte materialen en diensten inkopen, gevaarlijke producten en diensten verkopen, ...

Oorzaken

Regelmatig ontstaat een belangenconflict omdat er een privébelang om de hoek komt kijken: ga je het bedrijfsbelang dienen of het privébelang? Dit kan zelfs structureel zijn, zoals wanneer een manager een nevenfunctie heeft bij een concurrerende organisatie of zijn echtgenote werkt bij een klant/leverancier. Maar het kan ook incidenteel voorkomen, zoals wanneer een medewerker om een gunst wordt gevraagd.

Fraudetechnieken

Laten we beginnen met stellen dat er heel wat belangenconflicten zijn die niet tot problemen leiden. Een belangenconflict wordt pas problematisch als het bedrijf niet weet dat het belangenconflict bestaat, zodat de betrokken medewerker er ongemerkt misbruik van kan maken. Door er misbruik van te maken én het belangenconflict nog steeds niet te melden, wordt het fraude.

PROMOTIE MET GEVOLGEN

Hilde is een van uw salesmanagers. Zij heeft al jaren bedrijf ABC in haar portefeuille. U wist dat haar echtgenoot bij ABC werkte op de technische dienst. Op een gegeven moment maakte haar echtgenoot promotie naar de aankoopdienst van ABC. Hierover heeft zij u niet geïnformeerd. Sindsdien is uw omzet aan ABC verdubbeld.

Uw bedrijf heeft geen interne procedure die melding van conflicterende belangen verplicht stelt (structuur). Diverse collega's waren op de hoogte maar wilden Hildes omzetbonus niet in gevaar brengen (cultuur). Hilde had nooit training of voorlichting gekregen over conflicterende belangen (gedrag).

Varianten

- Een familielid van een aankoper werkt bij de verkoopdienst van uw leverancier.
- Een toezichthoudend bestuurder vraagt een van uw directieleden om een stageplaats voor zijn dochter te regelen.
- Een van uw onderhoudsmonteurs neemt de bestelwagen met gereedschap vrijdagavond mee naar huis om in het weekend bij te klussen.

1.4 Manipulatie van offerteprocedures

Risico's

Aanbestedingsprocedures worden vaak gezien als een noodzakelijk kwaad en worden ook vaak doorbroken, zowel door de aanbestedende partij als door de partijen die de offerte uitbrengen. De risico's van doorbreking van deze procedures zijn groot voor alle betrokken partijen. Zelfs het doorbreken van de aanbestedingsprocedures in kleinere of besloten procedures kan strafbaar zijn onder de Belgische corruptiewet. Als bijkomende sanctie kunnen de betrokken bedrijven worden uitgesloten van internationale aanbestedingsprocedures. Bepaalde varianten van aanbestedingsfraude vallen onder de kartelwetgeving.

Oorzaken

Aanbestedingsprocedures dienen precies om toezicht te kunnen houden op de kwaliteit van de aanbesteding, inbegrepen de vrije concurrentie tussen de inschrijvers. De procedures zijn kostbaar en tijdrovend voor alle betrokken partijen. Vaak dreigt de uitkomst niet te worden wat men verwacht of hoopt. De prijsfactor domineert. Vaak ontstaat de neiging om de procedure 'onzichtbaar bij te sturen'.

Fraudetechnieken

Een groep leveranciers kan een kartel vormen om telkens een van de kartelleden de offerte te laten winnen, zodat alleen dure offertes hoeven te worden gemaakt wanneer deze ook gewonnen worden. Een individuele leverancier kan het indienen van zijn offerte uitstellen tot de vraagprijs van de grootste concurrent bekend is; die prijsinformatie kan worden verkregen bij een 'bevriende' partij binnen de muren van de concurrent of van de aanbestedende organisatie. Ten slotte zijn er vele mogelijkheden om klanten te beïnvloeden door middel van bijvoorbeeld cadeaus, diners, reizen, sportwedstrijden en conferenties. Geschenken en representatiekosten zijn nog slechts beperkt toelaatbaar. Ze worden al snel beschouwd als corruptie, met alle risico's voor de betrokken personen en bedrijven.

OP MAAT VAN DE LEVERANCIER

Uw technische dienst wil graag met leverancier DEF werken, omdat hij daar goede ervaringen mee heeft. De aanbestedingcriteria zijn echter dwingend: 40% prijs, 40% voorstel, en 20% referenties. Uw technische dienst stelt het lastenboek op. DEF is niet de goedkoopste en moet dus zowel op inhoud als op referenties de concurrenten verslaan. De gedetailleerde criteria worden zo geformuleerd dat het DEF moet worden. Zo werkt uw bedrijf al jaren met DEF en betaalt altijd meer dan wellicht nodig.

Binnen de directie zijn er onvoldoende technische competenties om het lastenboek en de selectie van de technische dienst goed te kunnen beoordelen (structuur). Binnen de technische dienst houdt iedereen zijn mond hoewel bekend is dat er systematisch 10% te duur wordt ingekocht (cultuur). De technische dienst is niet bereid om naar een oplossing voor dit probleem te zoeken en hierover te spreken met de directie (gedrag).

Varianten

- Het lastenboek wordt op maat van een bepaalde leverancier geschreven, die hierdoor een hogere prijs kan zetten.
- Een leverancier mag de envelop met zijn offerte na de deadline inleveren.
- Bid rigging: samenspanning door een groep leveranciers om de offerteprocedure te winnen[16].

1.5 Omkoping in het buitenland

Risico's

In sommige landen is het risico groot dat er steekpenningen betaald moeten worden om een order binnen te halen, een vergunning te bekomen of goederen door de douane te krijgen. De omkoping aldaar is strafbaar in België, of het nu een ambtenaar betreft dan wel een organisatie. Zowel direct als via een tussenpersoon. Zowel actief (u bood het aan) als passief (de andere vroeg erom). Ook verboden zijn facilitation payments, dat zijn kleine bedragen smeergeld, te betalen voor een dienst waar men gewoon recht op heeft. Omkoping in het buitenland kan ook worden vervolgd vanuit het VK of de VS[7] als er bedrijven uit deze landen bij betrokken zijn. De straffen kunnen hoog oplopen, zowel voor de betrokken managers als voor het Belgische bedrijf, inclusief gevangenisstraf, boetes en jarenlange uitsluiting van openbare aanbestedingen.

Oorzaken

Belgische bedrijven komen hiermee in aanraking zodra ze gaan exporteren, zelfs wanneer ze slechts een tussenschakel zijn in de leveringen aan zo'n land. Als andere bedrijven in die keten steekpenningen betalen, kan het Belgische bedrijf worden meege-

trokken in de vervolging, omdat er wordt verondersteld dat het er baat bij heeft gehad. Dit lijkt op ketenaansprakelijkheid, een gevaarlijke ontwikkeling voor bedrijven. Belgische bedrijven blijken vaak onvoldoende geïnformeerd over deze risico's en over de maatregelen die ze moeten nemen om zich hiertegen te beschermen. Te goeder trouw zijn is op zich niet voldoende, je moet kunnen aantonen dat je te goeder trouw was op het moment van de feiten. Je kunt dus worden vervolgd in België, in het VK, in de VS en last but not least in het land waar de corruptie plaatsvond. Daar worden bedrijven steeds vaker vervolgd, wat niet altijd even rechtvaardig verloopt. Als de oorzaak niet bij een van uw eigen medewerkers ligt, dan ligt die wel bij een tussenpersoon, consultant of ander bedrijf in de keten die u meetrekt in de problemen.

Fraudetechnieken

Bij corruptie zijn er twee daders: een actieve en een passieve. Aangezien ze er beiden voordeel van hebben, zullen ze beiden zwijgen. Facilitation payments worden door de betrokkenen vaak gezien als een victimless crime: "Niemand heeft er last van als wij honderd dollar aan die ambtenaar betalen. Trouwens, hij moet ons die vergunning geven want we voldoen aan alle voorwaarden. Het is ons die honderd dollar dik waard." Het ethisch debat over wie er precies slachtoffers zijn, gaan we hier niet voeren. Bij grote corruptie, om grote deals te sluiten, is er evident sprake van fraude: er worden grote bedragen betaald die in de zakken verdwijnen van lokale ambtenaren en hun tussenpersonen.

"Bij corruptie zijn er twee daders: een actieve en een passieve. Aangezien ze er beiden voordeel van hebben, zullen ze beiden zwijgen."

OMKOPING VIA-VIA

Uw bedrijf is actief geworden in de Balkan-regio. Met uw team hebt u afgesproken dat er geen steekpenningen betaald zullen worden om deals binnen te halen. Na een jaar hebt u er nog geen grote projecten gerealiseerd. Er wordt aangeraden om met een lokale vertegenwoordiger te werken, eentje die de cultuur kent. De locale consultant die u inhuurde, haalde na twee maanden de eerste grote deal binnen. U kwam een 'success fee' overeen van 10%. Na de deal werd zij uw vaste vertegenwoordiger in de Balkan: zij wist duidelijk hoe het moest. Een jaar na de start van het project wordt uw bedrijf aangeklaagd wegens corruptie. De lokale consultant had een deel van haar fee gebruikt om een lokale ambtenaar om te kopen.

Met de consultant had u destijds gedetailleerde afspraken gemaakt over de te leveren inspanningen, maar geen clausule toegevoegd om omkoping uit te sluiten (structuur). U meende de lokale cultuur te kennen door met een lokale consultant te werken (cultuur). U stond onder druk om de deal binnen te halen en was daardoor te weinig kritisch naar de consultant (gedrag).

Varianten

- Uw vertegenwoordiger in Azië vraagt om voor een bepaalde deal de helft van zijn commissie te storten op een bankrekening van een Panamese vennootschap.
- Uw regiomanager Oost-Europa nodigt een Kroatische ambtenaar uit om samen met zijn echtgenote naar de voetbalinterland België-Kroatië te komen kijken met hotel en diner.
- De door u verkochte machines staan al een maand bij de douane in Afrika die u informeert dat de invoerrechten zojuist zijn verhoogd naar 150%, waarvan de helft contant te betalen.

1.6 Bedrijfsmiddelen en voorraden

Risico's

Veel bedrijfsmiddelen zijn gevoelig voor diefstal, de ene soort wat meer dan de andere. Denk vooral aan kleine hoogwaardige zaken zoals computers, gereedschappen en elektronica die gemakkelijk kunnen verdwijnen. Maar ook opleggers, bestelwagens en hele treinwagons verdwijnen. Normaal gezien bent u daarvoor verzekerd. Immateriële activa, waaronder bedrijfsgeheimen, zijn een ander verhaal, maar hiervoor verwijzen we naar de paragrafen 1.1. en 1.2. Een computer die wordt weggenomen van een bureau zal snel worden gemist, maar eentje meer of minder in de voorraad hoeft niet meteen op te vallen. Diefstal moeten we dan weer onderscheiden van misbruik: bent u akkoord dat uw techniekers in het weekend bijklussen met uw bestelwagens en uw gereedschap? Misschien geven ze zelfs garantie op de werken onder uw naam?

Oorzaken

Veel medewerkers hebben het gevoel dat het bedrijf wel iets kan missen. Als er iets kapot gaat of verdwijnt, wordt het altijd snel gerepareerd of vervangen. Dat varieert van printerpapier tot gereedschap en van smartphones tot computers. Van misbruik naar diefstal is een hellend vlak, net als van diefstal naar heling. Daarnaast moeten de procedures zorgvuldig toegepast worden om diefstal door derden te voorkomen. Als het bedrijf hier niet regelmatig aandacht aan geeft, dan ontstaat de indruk van 'gedogen'.

Fraudetechnieken

Medewerkers van een bedrijf kennen als geen ander de sterke en zwakke plekken van de controle rond de bedrijfsmiddelen en de voorraden. Wanneer een medewerker druk voelt om misbruik te maken van bedrijfsmiddelen en voorraden, of om deze te stelen, dan ontstaat er meteen een groot risico. Personeel wordt immers vertrouwd. "Ik let wel even op. Ik kom dit weekend mijn project afmaken. Ik heb niks gezien." Diefstal wordt fraude wanneer er sprake is van misleiding. Zoals wanneer de boekhouding wordt aangepast waardoor het lijkt alsof alle bedrijfsmiddelen er zijn, alsof alle voorraad er ligt, alsof die voorraad ons eigendom is. Of wanneer de magazijnier wel degelijk heeft gezien dat er voorraad verdween, maar dit verzwijgt. Dan is er sprake van fraude, corruptie, chantage of spionage.

KLUSSEN IN HET WEEKEND

Medewerkers van uw bedrijf lenen regelmatig bedrijfsmiddelen voor activiteiten in het weekend, die maandagochtend onvolledig en beschadigd teruggebracht worden. De bestelwagens moeten worden volgetankt, gereedschap is beschadigd of ontbreekt, materiaal is verbruikt. Er worden duidelijk grenzen overschreden maar u stelt de confrontatie uit om geen oorlog te ontketenen met uw personeel.

De 'grenzen' werden nooit helder afgesproken of vastgelegd in een gedragscode (structuur). Een groot deel van het personeel is op de hoogte en profiteert er zelf van en zal een klussende collega niet aan de galg praten (cultuur). Het gebeurt al zo lang en bij andere bedrijven gebeurt het ook (gedrag).

Varianten

- Medewerkers zijn niet zuinig op uw bedrijfsmiddelen: gsm's en computers zijn vaak stuk. U hebt de indruk dat dit meer gebeurt wanneer er een nieuw model op de markt verschijnt.
- Regelmatig verdwijnen er bedrijfsmiddelen en voorraden uit het magazijn. De magazijnier zegt dat hij niets heeft gezien en dat hij niet overal tegelijk kan zijn.
- Diverse personeelsleden hebben een firmawagen. U vermoedt dat deze soms worden uitgeleend en ook dat familieleden tanken met de tankkaarten.

1.7 Financiële middelen

Risico's

Financiële middelen zijn effecten, bankrekeningen, kasgeld, en ook de daarmee samenhangende posten debiteuren en crediteuren. Deze zijn kwetsbaar voor diefstal en fraude, nog meer dan de overige bedrijfsmiddelen. Gelukkig worden deze posten scherp opgevolgd in de boekhouding. Maar door een kleine manipulatie van de stukken kan het lijken alsof het saldo er nog is, terwijl dat niet waar is. De saldobevestiging van een bank, klant of leverancier duurt vaak zo lang, dat de boekhouding kan worden aangepast door te schuiven met transacties die ondertussen hebben plaatsgevonden. Als financiële middelen frauduleus verdwijnen, gebeurt dat vaak razendsnel, naar een andere rekening, in een ander land, en probeer het dan maar eens terug te krijgen ...

"Fraude kost 5% van de omzet. Zonder fraude zou de winst kunnen verdubbelen."

Oorzaken

Fraude met financiële middelen is aantrekkelijk omdat de fraudeur het gestolen bedrag binnen zeer korte tijd privé kan besteden. In tegenstelling tot bankbiljetten, zijn geldbedragen niet individueel genummerd: niet in de kassa, niet op een grootboekrekening en niet op een bankrekening. Het is de transactie die aantoont waar die 1.000 euro vandaan komt en waar die 1.000 euro is heengegaan. Door deze transactie in de boekhouding te manipuleren, wordt een vals

EEN CIJFERTJE EXTRA

Boekhouder Hans beheert al jaren de kas van het hoofdkantoor. Op een dag is Hans ziek en moet er juist een levering van 250 euro cash worden betaald. De directie-assistente doet de betaling en daarna telt zij de kas na: er zit precies 100 euro minder in dan verwacht. Uit nader onderzoek blijkt dat tussen de weekbetalingen een bon van Bpost zit van 71 euro die werd ingeboekt voor 171 euro. Bij nazicht worden in de weken ervoor meerdere vervalste bonnen van meerdere leveranciers ontdekt. Meestal is vakkundig een 0 veranderd in een 6 of een 9, of is er een 1 voor het hele bedrag gezet. Zo verdween telkens 60, 90 of 100 euro uit de kas. Hans blijkt een ongezond kind te hebben dat hij met moeite kan onderhouden. Hij nam telkens geld uit de bedrijfskas en wilde dat later terugbetalen. Na enkele jaren was de 'lening' opgelopen tot meer dan 60.000 euro.

Een financieel steunprogramma voor personeel is een effectieve antifraudemaatregel. Net als het tijdelijk vervangen van medewerkers tijdens ziekte; het verplicht opnemen van vakantie, pre-employment screening, en exitgesprekken.

Varianten

- Greep uit de kas.
- Het 'kasrondje', 'slepen' of 'verjongen van klantsaldi': een betaling door een klant wordt afgeboekt van een oude openstaande post. De oude post was destijds wel betaald door de klant maar die betaling was afgeroomd, waardoor die vordering in de boekhouding nog open stond. Naar jonge vorderingen wordt minder kritisch gekeken.
- Effecten worden als onderpand gegeven, terwijl daarvoor geen toestemming is.

beeld gegeven van de herkomst en de bestemming. Hierna geven we enkele veelgebruikte technieken.

Fraudetechnieken

Uw klant betaalt uw factuur ter waarde van 1.000 euro via de bank. Wanneer u het bankafschrift inboekt, schrijft u 1.000 euro bij op de grootboekrekening 'Bank' en trekt u 1.000 euro af van de vordering op uw klant. Als een personeelslid dat bedrag steelt, dan kan hij ontdekt worden bij een controle van de post 'Bank' of bij een controle van de post 'Klanten'. Afhankelijk van de zwakke plekken in de organisatie, zal hij kiezen voor manipulatie van de rekening 'Bank' of van de rekening 'Klanten'. Hier zijn functiescheidingen cruciaal, maar ook transactiecontroles. Is uw organisatie daar juist zwak, dan moet u regelmatig onverwacht controles doen op de boekhoudkundige verwerking van de transacties op de rekeningen 'Bank' en 'Klanten'. (Het aankondigen van deze controles zou de fraudeur immers de mogelijkheid geven om de gaten te dichten door nieuwe gaten te creëren.)

1.8 Financiële rapportages

Risico's

De bekendste financiële rapportages zijn jaarrekeningen, belastingaangiftes, bankrapporteringen en interne rapportages. Wanneer deze rapportering de werkelijkheid beter voorstelt dan ze is, kunnen het bedrijf en de belanghebbenden verkeerde beslissingen nemen, met grote gevolgen. Zo is het financieren van een acquisitie met vreemd geld alleen verstandig wanneer rentabiliteit en solvabiliteit dat toelaten. Als deze te rooskleurig voorgesteld worden, dan kan de lening een molensteen om de nek van het bedrijf worden. Hetzelfde geldt voor het ophalen van vers kapitaal voor product- of marktontwikkeling. Of het voorbereiden van het bedrijf om te worden overgenomen.

Oorzaken

Op veel managers staat grote druk om te bewijzen dat ze de aangekondigde targets hebben gehaald: groei, omzet, winst, marktaandeel, bankconvenanten of een overname. Eenzijdige druk op het tonen van prestaties is een belangrijke risicofactor voor fraude in financiële rapportages. Deze kan ontstaan door volumegedreven prestatie-indicatoren (KPI), door een CEO die alleen succesverhalen wil horen, door overdreven prestatiedruk, door een greedy manager, enzovoort. Als een target niet wordt gehaald, is de verleiding groot om de cijfers te manipuleren. Vaak loopt het goed af. De financiële controller gelooft dat ook en wil eraan meewerken. "Volgend kwartaal draaien we het

"Het management heeft als geen ander de gelegenheid om te schuiven met de resultaten: potjes aanleggen wanneer de resultaten goed zijn, potjes laten vrijvallen wanneer de resultaten tegenvallen."

GEPIMPTE VERKOOPCIJFERS

Regiomanager Hugo vreest zijn verkooptargets in het vierde kwartaal niet te halen. Hij besluit om in te grijpen. Aan enkele grote klanten geeft hij een extra korting én een eenmalige terugnamegarantie voor verkopen boven het normale volume. De verkopen in december stijgen zoals verwacht en Hugo legt uit aan het management dat dit komt door de extra korting. Over de terugnamegarantie spreekt hij niet. Als de verkopen van Hugo in het volgende jaar niet stijgen, worden de excess-verkopen uit december teruggedraaid en krijgt de omzet van het nieuwe jaar een dubbele knauw. Dit heet channel stuffing.

Varianten

- Niet aanleggen van noodzakelijke voorzieningen.
- Niet vermelden van gegeven waarborgen en garanties.
- Niet afwaarderen (impairment) van activa die minder waard zijn dan de boekwaarde.

weer terug." Maar het volgende kwartaal zakt de groei lichtjes en is er geen ruimte om de fraude terug te draaien zonder dat ze zichtbaar wordt. De kortstondige manipulatie kan zo een langdurige fraude met financiële rapportages worden.

Fraudetechnieken

Manipulaties hebben veelal betrekking op het aanleggen en laten vrijvallen van potjes: impairment, afwaardering of het aanleggen van voorzieningen. Bijvoorbeeld met betrekking tot klanten, onderhanden werk, garanties of geactiveerde goodwill. Vaak worden voorzieningen voor oninbaarheid van vorderingen volgens vaste regels opgesteld. Manipulatie van zo opgestelde voorzieningen zou meteen opvallen. Manipulatie gaat dan ook altijd om posten die worden gewaardeerd op basis van inschattingen door het management. Het management heeft als geen ander de gelegenheid om te schuiven met de resultaten: potjes aanleggen wanneer de resultaten goed zijn, potjes laten vrijvallen wanneer de resultaten tegenvallen.

1.9 Werving en selectie

Risico's

Personeelsverloop van 10-20 procent per jaar is niet ongebruikelijk in bepaalde afdelingen en sectoren. Zelfs zonder groei en acquisities kan uw personeelsbestand in enkele jaren grondig veranderen. Wervings- en selectieprocedures moeten u beschermen tegen verkeerde rekrutering. Voor kandidaten die iets te verbergen hebben, is het vaak geen moeite te veel om deze procedures te manipuleren en de betrokken functionarissen te misleiden. U hebt het allemaal wel eens meegemaakt met een vaste kracht, een tijdelijke medewerker, een uitzendkracht of een freelancer. De gevolgen kunnen variëren van incompetentie tot diefstal, heling, fraude, corruptie en spionage. Dat geldt in principe ook voor consultants, al wordt de verantwoordelijkheid daar doorgaans bij het consultantskantoor gelegd.

Oorzaken

Bij elke rekrutering gaat 90 procent van de aandacht uit naar de inhoud (kennis en vaardigheden) en 10 procent naar de formaliteiten (CV). Een bedrijf is kwetsbaar wanneer het te weinig aandacht besteedt aan het risico van misleiding, zowel in het inhoudelijke deel als bij de verificatie van het CV. Vaak is een 'lichte procedure' maar al te zichtbaar.

Een gevaarlijke trend de laatste jaren is infiltratie: de kandidaat solliciteert om later vanuit zijn functie bedrijfsgeheimen te kunnen doorspelen aan een criminele organisatie. Denk dan aan paswoord, pincode, research, development, encryptiesleutel, ... Hiermee doet social engineering zijn intrede in wervings- en selectieprocedures.`

Fraudetechnieken

- Het CV vermeldt een diploma van een opleiding die niet of niet geheel werd afgemaakt.
- Diploma's zijn te koop. Op het internet kost een MBA-certificaat maar een paar duizend euro.
- Een gemanipuleerde scan van het Uittreksel uit het Strafregister en niet het origineel.
- De kandidaat werkte slechts voor kleine organisaties, maar vermeldt de naam van een multinational in het begin van de loopbaan. Hij rekent erop dat u alleen recente referenties natrekt.
- De kandidaat werd in het verleden ontslagen wegens fraude. Hij verzwijgt deze job op zijn CV en past de begindata en einddata van de jobs eromheen aan.
- De kandidaat geeft referenties op die niet bij dat bedrijf blijken te werken of die niet meer bij dat bedrijf werken waardoor de kans klein is dat ze nog zullen getuigen.
- De kandidaat vergroot ervaringen uit, zoals een leidinggevende rol in een project terwijl hij feitelijk een uitvoerende rol bekleedde.

VALS DIPLOMA

Hilde slaagde er niet één maar twee keer in om met een vals diploma vol schrijffouten een job te versieren bij de bank. Bij het filiaal in B. werkte ze negen maanden vooraleer ze ontslagen werd omdat ze te veel fouten maakte. Kort daarna mocht ze aan de slag in H. Daar viel ze door de mand omdat ze al binnen een week om opslag vroeg. Het diploma fiscaliteit en accountancy had ze kunnen kopen op het internet. "Ik kocht het omdat ik schrik had van mijn ouders. Die begonnen zich vragen te stellen over de duur van mijn studies." Lange tijd had ze een goede job zonder gebruik te maken van het valse diploma, tot ze door besparingen aan de deur werd gezet. "Ik was een huis aan het bouwen en kon dat plots niet meer afbetalen. Bij toeval zag ik dat je op het internet diploma's kan kopen."

1.10 Niet-financiële rapportages

"De risico's van manipulatie van niet-financiële rapportages zijn minder eenvoudig te becijferen omdat de prestaties van het bedrijf er vaak indirect en pas laat door worden beïnvloed."

Risico's

De risico's van manipulatie van niet-financiële rapportages zijn minder eenvoudig te becijferen omdat de prestaties van het bedrijf er vaak indirect en pas laat door worden beïnvloed. Denk aan niet vermelde kwaliteitsproblemen in een controleverslag, gunstiger voorgestelde uitstootcijfers van motoren, opgepoetste productiviteitscijfers van afdelingen, ...

Oorzaken

Zoals gezegd, managers staan vaak onder hoge druk om hun doelstellingen te halen. En dat zijn er heel wat: de kwaliteit van een bedrijfsproces, de productkwaliteit, milieuprestaties, onderzoeksresultaten (R&D, marktstudies en andere surveys), ... En dat kan ook in niet-financiële rapportering risico's op fraude meebrengen. Zeker als alleen de naakte cijfers tellen, als de CEO vooral wil bewijzen hoe goed hij is, als hij/zij in de eerste plaats de bonus wil halen, ... Zo gebeurt het dus ook in niet-financiële rapportage wel eens dat het rapport wordt vervalst.

VERVALST MILIEURAPPORT

De buitenlandse moedermaatschappij dreigt één van de Belgische fabrieken te sluiten als ze de strengere milieunormen niet haalt. De fabrieksdirecteur heeft het management en de vakbonden ervan overtuigd dat hij de fabriek zal redden. Door pech loopt de reddingsoperatie vertraging op en de maatregelen komen te laat op gang. De fabrieksdirecteur besluit de uitstootrapporten te manipuleren om tijd te winnen voor zijn reddingsoperatie en zo zijn toezegging waar te maken.

Varianten

- Milieurapporten, uitstootrapporten.
- Research & Development-rapporten.
- Kwaliteitscontrolerapporten.

2. Antifraudemaatregelen

Deze Voka Wijzer behandelt de tien meest effectieve antifraudemaatregelen. Bedrijven die deze maatregelen hebben genomen, lijden substantieel minder schade door fraude dan bedrijven die deze maatregelen (nog) niet hebben genomen.

ORGANISATIE EN LEIDING	2.1 Leadership 2.2 Toezicht 2.3 Cultuur 2.4 Audit
FRAUDERISICO-EVALUATIES	2.5 Frauderisico-evaluaties
PREVENTIE EN DETECTIE	2.6 Bewustzijn en training 2.7 Data-analyse 2.8 Controles 2.9 Personeelsbeleid
MONITORING EN RESPONS	2.10 Monitoring en respons

Een antifraudebeleid is een continu gegeven

De basis voor antifraudebeleid is een degelijke corporate-governancestructuur. Deze bevat een heldere organisatiestructuur, met functiescheidingen tussen cruciale functies, alsmede een ondubbelzinnige delegatie van taken en bevoegdheden. Grote zwaktes in de corporate-governancestructuur kunnen niet worden gecompenseerd door antifraudebeleid. First things first.

“Grote zwaktes in de corporate-governancestructuur kunnen niet worden gecompenseerd door antifraudebeleid.”

Het invoeren van antifraudemaatregelen gebeurt in vijf stappen:

- Ontwerp een samenhangend antifraudebeleid (fraud risk governance).
- Schat regelmatig het frauderisico in voor de eigen organisatie (fraud risk assessment) en beoordeel of er voldoende antifraudemaatregelen zijn genomen.
- Ontwerp en implementeer concrete preventie- en detectiemaatregelen (fraud control).
- Ontwerp en implementeer een frauderesponsplan (fraud response).
- Volg regelmatig op of de getroffen maatregelen werken (monitoring).

2.1 Leadership

De antifraudemaatregelen van een bedrijf zijn gebaseerd op het integriteitsbeleid uitgestippeld door de directie. De directie moet daarbij zelf het goede voorbeeld geven (tone at the top) anders is het integriteitsbeleid ongeloofwaardig. De toezichthoudende bestuurders volgen dit op en moeten ingrijpen wanneer het fout loopt.

De directie ontwikkelt een visie die aangeeft hoe een goed renderend bedrijf kan worden gerund, alsook een strategie waarin is bepaald wat daarvoor zal worden ondernomen. Daarbij gaat het niet alleen om economische afspraken (wie, wat, wanneer, waarom) maar ook om afspraken over de stijl (hoe wel, hoe niet). Hoe het bedrijf deze stijl bepaalt en bijstuurt, is vastgelegd in het integriteitsbeleid. Dat verbindt de medewerkers en biedt steun in hun dagelijks gedrag en handelen. Het integriteitsbeleid gaat over de manier waarop de leiding wenst dat de medewerkers handelen en omgaan met elkaar en met de belanghebbenden.

De kernwaarden van het bedrijf liggen aan de basis van de stijl van ondernemen, en zij vormen een richtlijn voor het dagelijkse doen en laten op het werk. Ze gelden niet alleen voor medewerkers, directie en toezichthoudende bestuurders maar ook voor diegenen die in opdracht van het bedrijf werken, zoals uitzendkrachten en consultants.

"De directie moet zelf het goede voorbeeld geven (tone at the top) anders is het integriteitsbeleid ongeloofwaardig."

De gedragscode legt uit hoe de kernwaarden worden toegepast in concrete situaties, zoals de omgang met collega's, klanten, leveranciers en aandeelhouders. De gedragscode bevat intenties (hoe wel) en grenzen (hoe niet), en helpt medewerkers bij het denken over hun handelen, ook in geval van dilemma's.

Er zijn onderwerpen die extra gevoelig liggen en daarom bijzondere aandacht vragen, zoals omkoping in het buitenland, belangenconflicten, voorkennis en privacy. Hiervoor worden best nadere interne regels uitgewerkt. Draagvlak is cruciaal, dus de gedragscode en de interne regels worden ontwikkeld in nauw overleg met het personeel.

Het management gebruikt bovengenoemde tools actief om zijn visie en leiderschap te ondersteunen en uit te dragen.

Bedrijven die een gedragscode hebben ontwikkeld en die toch een fraude meemaken, hebben de helft minder schade dan bedrijven die geen gedragscode hebben. De gedragscode bevat praktische aanwijzingen voor het handelen door het personeel in gevoelige en moeilijke omstandigheden, zoals ethische dilemma's. Deze proactieve bedrijven hebben minder fraude, ontdekken fraude in een vroeger stadium, en hebben een meer succesvolle respons.

2.2 Toezicht

Effectief toezicht door de directie op de bedrijfsprocessen en de procedures (management review) is een belangrijk aspect van succesvol antifraudebeleid. Onderzoek toont aan dat bedrijven waar de directie effectief toezicht houdt op bedrijfsprocessen en procedures, en die toch een fraude meemaken, de helft minder schade lijden dan bedrijven waarvan de directie geen effectief toezicht houdt.

Effectief toezicht betekent niets anders dan dat invulling wordt gegeven aan de toezichtstaak die hoort bij de verantwoordelijkheid van de directie en het bestuur. Een management dat altijd op reis gaat, aan het vergaderen is, op restaurant zit, of op de baan is om verkooporders binnen te halen, en dat geen tijd heeft om effectief toezicht te houden, creëert een organisatie die kwetsbaar is voor fraude en andere onregelmatigheden.

Bedrijven waarvan de raad van bestuur systematisch de financiele verslagen aftekent, en die toch verslaggevingsfraude meemaken, hebben de helft minder schade dan bedrijven waarvan bijvoorbeeld alleen de boekhouder of de financieel directeur tekent. Deze proactieve bedrijven hebben minder fraude, ontdekken fraude in een vroeger stadium, en hebben een meer succesvolle respons.

90 procent van de financiële controllers heeft al te maken gehad met manipulatie van financiële verslagen of verzoeken daartoe. Het kan overal gebeuren. De raad van bestuur moet effectief toezicht houden op de totstandkoming van financiële verslagen en deze na controle ondertekenen. Dit is een van de meest effectieve antifraudemaatregelen.

2.3 Cultuur

Het doel van elk bedrijf is om de strategie te realiseren én zich daarbij aan de gedragscode te houden. Dat samenspel kan soepel verlopen als de afspraken die zijn vastgelegd in de gedragscode, passen in de bedrijfscultuur. Het handelen en het gedrag van het personeel worden in belangrijke mate bepaald door het voorbeeldgedrag van het management en door de bedrijfscultuur.

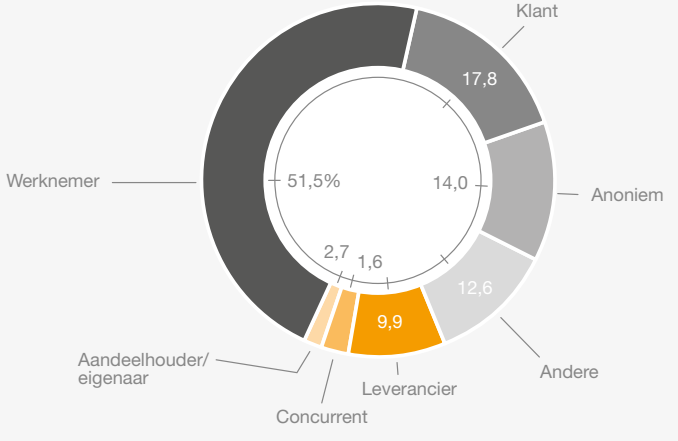
Antifraudebeleid werkt het best in een cultuur van vertrouwen waarin het personeel wordt gestimuleerd om zelfstandig en kritisch te zijn. In een speak-up culture zullen collega's elkaar aanspreken op ongewenst gedrag.

Vertrouwenspersonen moeten echt te vertrouwen zijn en toegankelijk zijn voor alle lagen van het personeel, in alle vestigingen. En je moet er met alle soorten problemen bij terecht kunnen: niet alleen met pesten of discriminatie, maar ook met andere afwijkingen van de gedragscode. En met dilemma's. Het is aan te raden om de vertrouwenspersonen breed op te leiden, en ook externe vertrouwenspersonen achter de hand te hebben voor wanneer zelfs de eigen vertrouwenspersonen niet worden vertrouwd. Dit laatste is niet zeldzaam en verklaart vaak waarom vertrouwenspersonen nauwelijks geraadpleegd worden.

Voor een aantal arbeidsrechtelijke zaken zoals in het kader van een beleid rond psychosociaal welzijn, is elke onderneming verplicht een interne en externe vertrouwenspersoon/ preventieadviseur aan te stellen. Op zich hebben deze personen geen wettelijke taak op het vlak van een fraudebeleid, maar niets sluit uit dat hun taak binnen de onderneming - los van het wettelijk verplichte kader - verruimd wordt.

Een meldpunt of ethics hotline is van groot belang. Bij het meldpunt kunnen alle personeelsleden - en ook derden - zaken melden die langs de normale kanalen niet opgelost raken, zoals een manager die ernstige misstanden pleegt, toedekt of niet aanpakt. Iemand die vermoedt dat de directie een probleem niet daadkrachtig aanpakt of zelfs toedekt, kan dat ook rechtstreeks melden aan de onafhankelijke bestuurders of het auditcomité. Indien anonieme meldingen mogelijk zijn, moet het meldpunt interactief zijn, dat wil zeggen dat aan de melder kan worden gevraagd om aanvullende informatie te verstrekken ten behoeve van het onderzoek.

2/3 van de tips komt van binnen de organisatie, 1/3 van buiten



Bron: ACFE 2016 Report to the Nations

2.4 Audit

Veel bedrijven hebben een commissaris (statutory auditor). De commissaris moet volgens zijn wettelijke controlenormen elk jaar het frauderisico evalueren. In zijn jaarlijkse adviesbrief aan het management (management letter) kan hij adviezen geven hoe eventuele zwakke plekken van het fraud risk management kunnen worden aangepakt. Minstens één keer per jaar moet de commissaris een gesprek voeren met de directie over het frauderisico van het bedrijf. Dat is een geschikt moment om zijn mening te peilen over uw antifraudebeleid.

Grote bedrijven hebben een interne auditor. Middelgrote bedrijven die deze functie hebben gecreëerd, hebben de taken soms uitbesteed aan een derde. Ook de interne auditfunctie moet volgens zijn controlerichtlijnen jaarlijks het frauderisico evalueren. De interne auditor besteedt hier doorgaans meer tijd aan dan de externe auditor (de commissaris). De interne auditfunctie moet onafhankelijk van de directie kunnen rapporteren aan de onafhankelijke bestuurders van het auditcomité. Vreemd genoeg is dit bij diverse Belgische organisaties nog steeds niet het geval.

> "Minstens één keer per jaar moet de commissaris een gesprek voeren met de directie over het frauderisico van het bedrijf."

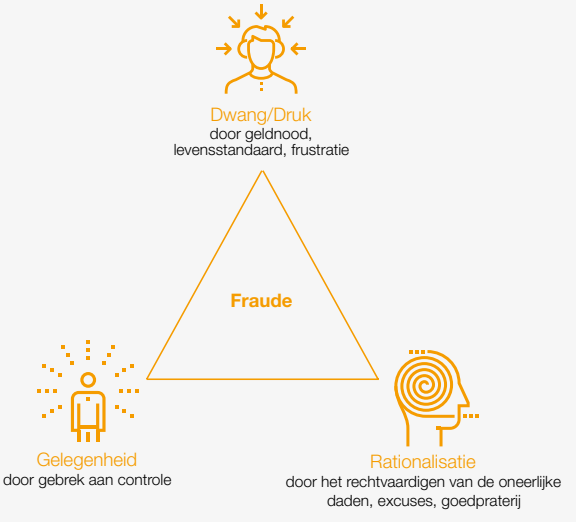
Zowel de externe auditor (commissaris) als de interne auditor zijn generalisten. Zij zijn thuis in alle domeinen van audit en bedrijfsvoering, maar niet gespecialiseerd in een bepaald domein zoals IT, pensioenen of fraude. Binnen deze domeinen zijn specialisaties ontstaan: EDP-auditor, actuaris en fraud auditor (fraud examiner; forensic accountant). Grote bedrijven en grote auditkantoren zetten gespecialiseerde fraude-auditors in bij de jaarlijkse controle. Inmiddels bestaan er onafhankelijke kantoren die zijn gespecialiseerd in fraud risk management (corruptie, terrorisme, criminele organisaties, cybercrime, money laundering).

Ondanks het feit dat interne en externe auditors generalisten zijn, leidt hun methodische aanpak tot ontdekking van zwakke plekken in het antifraudebeleid en van fraude. Interne en externe audit zijn dan ook sterke maatregelen van antifraudebeleid.

2.5 Frauderisico-evaluaties

"Frauderisico-evaluaties zorgen ervoor dat het bedrijf zijn antifraudebeleid kan aanpassen zodra er nieuwe ontwikkelingen zijn of zwakheden worden vastgesteld."

Fraude driehoek



Bron: Donald R. Cressey

Frauderisico-evaluaties (fraud risk assessments) zijn een belangrijk onderdeel van antifraudebeleid. Het betreft een inschatting van het frauderisico die minstens jaarlijks wordt uitgevoerd. Idealiter gebeurt dat wanneer er een reden voor is, bijvoorbeeld: bij het aanboren van een nieuwe markt, het betreden van een nieuw land, het lanceren van een nieuw product, de overname van een ander bedrijf, nieuwe wetgeving (inzake privacy, corruptie, cybercrime, etc.), een nieuw fraudefenomeen (zoals CEO-fraude en wannacry virus), nieuwe richtlijnen voor fraud risk management (zoals COSO en ISO), een nieuwe business partner, een nieuwe benchmarking (zoals de Corruption Perceptions Index[14] en FATF (Financial Action Task Force) blacklists[15]), ...

Frauderisico-evaluaties zijn een sterke maatregel van effectief antifraudebeleid. Ze zorgen ervoor dat het bedrijf zijn antifraudebeleid kan aanpassen zodra er nieuwe ontwikkelingen zijn of zwakheden worden vastgesteld.

Bijzondere aandacht bij de frauderisico-evaluatie vragen de samenstelling van het team dat de evaluatie uitvoert en de interactie met de rest van de organisatie. Zo'n evaluatie doe je niet op een maandagmorgen in een vergaderzaaltje op het hoofdkantoor. Het is absoluut nodig om de managers in het veld te ontmoeten die zich bezighouden met producten, klanten, agenten, leveranciers en transacties. Daarnaast moeten de ondersteunende diensten erbij worden betrokken, zoals IT, HR, Legal, Finance en Accounting.

De Fraud Risk Management Guide[10] bevat een handleiding hoe een frauderisico-evaluatie moet worden uitgevoerd, met bijbehorende checklists en toelichtingen.

2.6 Bewustzijn en training

"A code is nothing, coding is everything."

Voor effectief antifraudebeleid moeten er én duidelijke afspraken worden gemaakt én moeten deze afspraken ook nageleefd worden. De mens is daarbij de cruciale factor en helaas tevens een zwakke schakel. Vaak blijkt hij niet goed op de hoogte te zijn van de afspraken, of legt hij ze anders uit dan bedoeld was. Afspraken zijn dus niet altijd een garantie voor een veilige bescherming tegen fraude.

Bedrijven moeten hun managers en medewerkers voorlichten en bewustmaken van deze afspraken en ze regelmatig trainen om zeker te weten dat de afspraken goed worden geïnterpreteerd. We hebben het vooral over de visie, de kernwaarden en de gedragscode.

Daarnaast gaat het om meer gedetailleerde regels, voor zover van toepassing op de eigen taken, zoals de basisafspraken met de leveranciers (leverancierscode), afspraken over het geven en aannemen van cadeaus (hospitality), voorkennis (beursreglement), omgangsvormen (harassment), ... Voorts moeten managers en medewerkers begrijpen wanneer en hoe ze de vertrouwenspersonen en het meldpunt kunnen benutten.

Er zijn veel oplossingen voor bewustmaking en training: informatie bij indiensttreding, communicatie via het intranet, website en sociale media, informatie en storytelling tijdens management- en afdelingsmeetings, ter sprake brengen tijdens evaluatiegesprekken.

Het bewustzijn wordt ook verhoogd door bepaalde KPI's toe te voegen, zoals het behalen van een compliancetest, het respecteren van de gedragscode of het actief uitdragen van de corporate values. Ook in het beleid rond variabele bezoldiging kan u dit meenemen.

Daarnaast zijn er gespecialiseerde applicaties om het personeel te informeren, het bewustzijn te meten en de kennis en het inzicht te toetsen, zoals het testen van de reactie van personeelsleden op phishing-mails. Mensen leren het beste wanneer ze betrokken raken bij het probleem, niet door ze slechts iets te vertellen of te tonen. Betrokkenheid wordt vooral gecreëerd door de afspraken zeer concreet te maken en te plaatsen in de eigen werkomgeving.

Last but not least is herhaling een belangrijk element: een eenmalige actie is na een paar maanden alweer vergeten.

Bedrijven die hun managers en personeel trainen op het gebied van antifraudebeleid en die desondanks fraude meemaken, hebben 47 procent minder schade dan bedrijven die deze training niet aanbieden.

Het management moet ongewenst gedrag en fraude bespreekbaar maken; het kan immers overal gebeuren. Tijdens management- en personeelsmeetings wordt telkens kort stilgestaan bij gevallen die in de krant stonden of die in de sector gebeuren. "Liever niet bij ons!" Dit kan ook op het eigen intranet, in het personeelsblad, en tijdens werkgesprekken. Ook kunnen cases worden besproken, in spelvorm aangeboden ('serious gaming') of teaser-video's worden gemaakt met levensechte voorbeelden. Ten slotte kan dit alles worden verwerkt in de toelichting op de gedragscode, bij indiensttreding en bij latere updates.

2.7 Data-analyse

"Proactieve transactiemonitoring en reactieve data-analyse vormen samen de nummer één in effectieve fraudebestrijding."

Facturatie, projectbeheer, productie, commerciële activiteiten, communicatie,... alles in het digitale domein ligt vast in data (digitale gegevens). Sommige delen daarvan zijn goed gestructureerd, zoals het financiële systeem of het ERP-systeem; andere minder goed, zoals (e-mail)-correspondentie of documentatiesystemen. Deze overvloed aan data is ook gevoelig voor misbruik zoals fraude.

Tegelijk biedt het talloze mogelijkheden om fraude juist te ontdekken. De handelingen van gebruikers van een geautomatiseerd systeem laten namelijk digitale sporen achter. Door hierop data-analyse toe te passen, ontstaat een van de krachtigste maatregelen van antifraudebeleid: fraud analytics. Hiermee stelt u vooral vast of normale en gewenste patronen worden doorbroken. Fraud analytics helpt vooral met het traceren van frauduleuze transacties maar ook bij het detecteren van valse e-mails, zoals bij CEO-fraude.

Eerst maakt u een inventarisatie van de relevante data in uw organisatie. Niet alleen de data voor de gebruikers, maar tevens verkeersgegevens, logging, metadata en systeemdata. Vervolgens bepaalt u welke van deze data u kunt benutten om signalen op te vangen van de fraudes die u hebt geselecteerd in uw frauderisico-evaluatie (paragraaf 2.5). Voorbeelden van fraud analytics zijn visualisatietechnieken, de monitoring van uw firewall en data mining.

Met data-analyse kan worden zichtbaar gemaakt of een factuur dubbel wordt betaald, of het normale patroon van bestellingen bij een bepaalde leverancier plots wordt doorbroken, of salaris wordt betaald aan een spookwerknemer, etc.

Fraud analytics voegt enkele belangrijke eigenschappen toe aan de bestaande analyses en controles in uw bedrijf. Zo kunnen data van verschillende afdelingen of processen worden gecombineerd, wat nieuwe inzichten oplevert. Fraud analytics objectiveert niet alleen deze inzichten maar ook de manier waarop die worden verkregen. Er bestaan al zelflerende applicaties die patronen herkennen en bijstellen, die traditionele methoden waarschijnlijk niet zouden ontdekken. Fraud analytics biedt toekomst.

TIP VAN DE FEDERALE GERECHTELIJKE POLITIE:

"Zorg dat uw bedrijf een goede firewall heeft. Bewaar logfiles beter 5 weken in plaats van 5 dagen. Doel is om logfiles zo lang mogelijk te bewaren zodat onderzoek naar fraude nog mogelijk is."

Notities:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.8 Verrassingscontroles

"Fraudeurs maken dankbaar gebruik van de voorspelbaarheid van veel controles en audits."

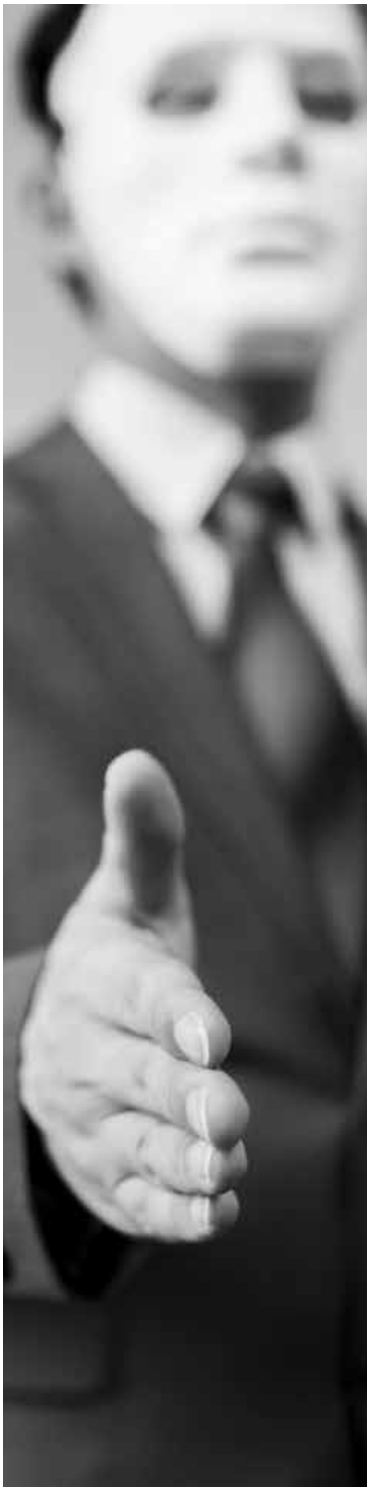
In alle bedrijfsprocessen (aankoop, verkoop, bewaring, betaling, factuurverwerking, ...) vinden dagelijks controles plaats op alle transacties: klopt de ontvangen hoeveelheid met het bestelde volume? Vermeldt de factuur dezelfde bankrekening als onze leveranciersadministratie? Klopt de identiteit van de vrachtwagenchauffeur met de informatie van de klant? Dit zijn eerstelijnscontroles, ook first line of defence genoemd. De personeelsleden uit de eerste lijn voeren deze controles zelf uit. Het zijn bijna altijd voorspelbare controles. Iemand die kwaad wil doen, kan anticiperen op de zwakke plekken in die controleprocedures. Zo is de kwaliteit van deze controles doorgaans zwakker bij grote drukte, indien een functionaris ziek is, op vrijdagmiddag na 16 uur, ...

Daarnaast zijn er tweedelijnscontroles, uitgevoerd door personen die daar speciaal mee belast zijn, zoals onafhankelijke beoordelingen van marges, voorraden en vorderingen en controles op de naleving van interne procedures door afdelingen als kwaliteitscontrole, financiële controlling, risk management en compliance (second line of defence). Ook deze controles zijn vaak voorspelbaar, zowel qua timing als qua omvang. Iemand die kwaad wil doen, kan ook hier anticiperen op zwakke plekken of de controles proberen te manipuleren. Tweedelijnscontroles zijn een belangrijke basis van het antifraudebeleid. Voorwaarde is wel dat de controleur onafhankelijk is (functiescheiding), deskundig op het gecontroleerde gebied (controlekwaliteit) en dat zijn controlebevindingen niet kunnen worden beïnvloed of gemanipuleerd (controleprocedure).

Manipulatie van controles is nagenoeg onmogelijk indien ze onverwacht plaatsvinden, zoals bij verrassingsbezoeken (overvalsbasis) en indien de gecontroleerde zich onbespied waant (camera's). Antifraudebeleid moet voldoende verrassingscontroles bevatten. Deze moeten zowel gericht zijn op de aanwezigheid van de bezittingen (voorraad, bedrijfsmiddelen, vorderingen, schulden, cash, bank, ...) als op de naleving van procedures (kassa, betalingen, magazijn, saldobevestigingen, bank, klanten, leveranciers, ...).

Ten slotte is er de third line of defence: audit. Personeel dat kwaad wil doen, kan auditors vragen om hun controles tijdig aan te kondigen "om ons de kans te geven het goed voor te bereiden", "om u te kunnen helpen", "omdat die controle anders niet mogelijk is", "om ons niet onnodig te belasten". Ze halen hiermee het verrassingselement uit de audit en creëren de gelegenheid om eventuele verschillen weg te werken en tekorten aan te zuiveren, althans op het eerste gezicht. Zo kondigen auditors vaak te vroeg hun selectie aan van bankrekeningen, klanten en leveranciers waarvan een saldobevestiging zal worden gevraagd. Of ze onthullen te vroeg het moment en de plaats van de inventarisaties en kastellingen. Ook zullen de interne procedures perfect worden gevolgd wanneer men weet dat de auditor meekijkt.

Verrassingscontroles en verrassingsaudits zijn een sterk element van effectief antifraudebeleid: bedrijven die verrassingscontroles en verrassingsaudits toepassen, lijden de helft minder schade door fraude dan bedrijven zonder deze maatregelen. Cruciale voorwaarden zijn de onafhankelijkheid en de deskundigheid van de controleur/auditor en de mate waarin de controle/audit is afgeschermd tegen beïnvloeding. De opleiding van controleurs en auditors moet ervoor zorgen dat ze bestand zijn tegen dergelijke beïnvloeding. Een fraudeur die veel te verliezen heeft, zal alles in het werk stellen om te weten te komen wanneer en hoe de controle/audit zal plaatsvinden.



2.9 Personeelsbeleid

"Jobrotatie is een maatregel waardoor er niet langdurig verborgen afspraken kunnen bestaan met klanten en leveranciers of tussen collega's onderling."

Het personeelsbeleid van een bedrijf biedt belangrijke mogelijkheden voor effectieve antifraudemaatregelen. De bekendste is pre-employment screening (PES). Geloof niet meteen wat er in een CV staat: de helft van de CV's is gepimpt. En in geval van fraude blijkt dat in de helft van de gevallen geen PES had plaatsgevonden.

Een PES kan de volgende elementen bevatten: nauwkeurige controle van het aangeleverde CV (data, diploma's, werkgevers), natrekken van referenties, opvragen van bewijs van goed zedelijk gedrag (uittreksel strafregister), verkrijgen van achtergrondinformatie via open bronnen (bestuursmandaten, nevenactiviteiten, media-aandacht) en een gesprek waarin de kandidaat wordt gevraagd om te reageren op situaties die zich op het werk kunnen voordoen (moraliteitsgesprek).

Niet elke PES moet al die elementen bevatten. Vooraf inventariseert u de functies waarvoor een PES moet plaatsvinden en maakt u driedeling: beperkt - gemiddeld - zwaar. Enkele relevante criteria voor die indeling: voorbeeldfunctie; beslissingsbevoegdheid; beschikking over informatie en bedrijfsmiddelen waaronder geld; impact op de reputatie van de organisatie en ervaringen in het verleden.

Verplichte jobrotatie is een maatregel waardoor er niet langdurig verborgen afspraken kunnen bestaan met klanten en leveranciers of tussen collega's onderling. Ook de maatregel van verplichte vakantieopname doorbreekt systematische fraudesystemen. Wanpraktijken op het werk kunnen ook worden blootgelegd door middel van personeelstevredenheidsonderzoeken en exitinterviews.

2.10 Monitoring en respons

"Monitoring en respons zijn de sluitstenen van het antifraudebeleid."

Monitoring

Het is belangrijk dat regelmatig wordt vastgesteld of de ingevoerde antifraudemaatregelen nog bestaan en worden nageleefd. Deze monitoring omvat alle maatregelen die in de vorige paragrafen werden opgesomd.

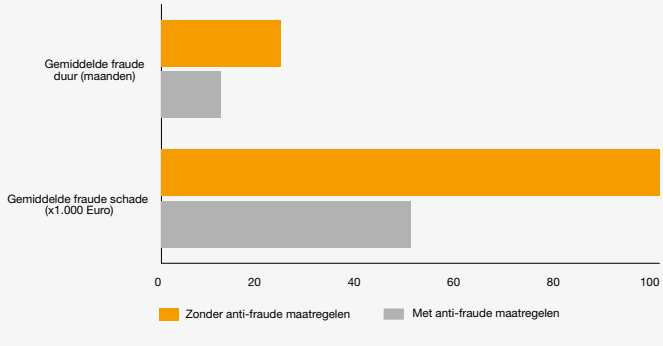
De raad van bestuur belast een directielid met de verantwoordelijkheid voor deze monitoring en verlangt periodiek een update over de verrichte werkzaamheden en de bevindingen. Die worden besproken in het auditcomité en op basis van de resultaten wordt overgegaan tot eventuele aanpassingen van het antifraudebeleid. Tevens worden de bevindingen besproken met de commissaris. Die moet jaarlijks het frauderisico van het bedrijf beoordelen in het kader van zijn auditmandaat en zal willen kennisnemen van de wijzigingen in het antifraudebeleid. De uitwisseling van ervaringen en inzichten tussen het monitoringteam en de auditors is belangrijk voor een goede bijsturing van het antifraudebeleid.

Respons

Het frauderesponsplan is een procedure die het beste lijkt op crisismanagement. Het bevat maatregelen die in de verste verte niet lijken op wat er dagelijks in het bedrijf gebeurt. Gelukkig maar: we hebben het dan ook over de uitzonderlijke omstandigheid van een vermoeden van fraude.

"Het frauderesponsplan is een crisisplan en bevat maatregelen die in de verste verte niet lijken op wat er dagelijks in het bedrijf gebeurt."

Effectiviteit van de antifraudemaatregelen



3. Frauderesponsplan

De gemiddelde manager maakt in zijn hele loopbaan geen enkele of slechts een paar fraudegevallen mee. Hij heeft er dus weinig ervaring mee, en zijn collega's al evenmin. Er worden dan ook veel fouten gemaakt in de eerste dagen nadat er een vermoeden van fraude is gerezen. Door een frauderesponsplan klaar te hebben, kan veel schade voorkomen worden. Het frauderesponsplan toont de do's and don'ts bij een vermoeden van fraude.

"Een cruciaal onderdeel van het frauderesponsplan is de 'Checklist eerste actie bij fraude'."

De eerste stap van een frauderespons is het bijeenroepen van het juiste team. Traditioneel is dit een ontmoeting tussen een directielid, de jurist en het hoofd personeelszaken. In de praktijk blijkt dat zo'n team te licht en onvoldoende gespecialiseerd is en dat u dit best uitbreidt met een auditor en een advocaat, vaak ook een IT-er. Het is belangrijk dat u meteen de juiste profielen inzet:

- Auditor: een fraude-auditor, want een gewone auditor heeft te weinig ervaring met het herkennen en onderzoeken van fraude.
- Advocaat: de huisadvocaat heeft vooral kennis van arbeidsrecht. In geval van fraude zijn ook andere competenties vereist zoals ondernemingsrecht, strafrecht en privacy.
- IT-er: een forensic IT-specialist, want alleen deze heeft voldoende kennis van cybercrime, forensic technology en data-analyse. Hij hanteert een onderzoeksaanpak en software die het bewijsmateriaal niet beschadigen.

Dat team bepaalt hoe het frauderesponsplan wordt uitgevoerd. Als het loos alarm is, dan was de bijeenkomst van het team een nuttige generale repetitie. Het kost vaak maar een paar uur om die eerste analyse te maken, dus voor de kosten hoeft u het niet te laten. Een cruciaal onderdeel van het frauderesponsplan is de 'Checklist eerste actie bij fraude'.

POTENTIËLE FRAUDE-INCIDENTEN

Uw verkoopdirecteur lacht telkens de kritiek van de ondernemingsraad weg dat hij de targets te hoog stelt. Vanochtend stond in de krant dat uw bedrijf een ambtenaar heeft omgekocht bij een openbare aanbesteding.

Uw omzet en marge dalen. Bij een telling van de voorraad treft u meer goederen dan in de boekhouding. Heeft de magazijnier een eigen handel gestart? Hij is vanochtend niet op het werk verschenen.

Een anonieme tip toont aan dat de bouw van uw nieuwe kantoorgebouw werd besteld bij een vriend van uw aankoopmanager. Die laatste ontkent de vriendschap, maar hij overtuigt u niet.

Checklist eerste actie bij fraude

Bijeenroepen frauderesponsteam

Crisismanagement:

- ☐ Roep een crisisteam bijeen: bestuurslid, CFO, HR, legal, audit, advocaat, onderzoeker.
- ☐ Beoordeel hun onafhankelijkheid en deskundigheid ter zake.
- ☐ Stel een woordvoerder aan en maak een concept van persbericht voor het geval er iets uitlekt.
- ☐ Leg anderen spreekverbod op.
- ☐ Beschouw reputatierisico en aansprakelijkheidsrisico.
- ☐ Breng rust: draag uw managers business as usual op.
- ☐ Stel een actieplan op (hierna).

Ruwe analyse:

- ☐ Probeer het vermoedelijke fraudeschema te bepalen.
- ☐ Onderzoek de mogelijkheid dat de fraude omvangrijker is dan op eerste gezicht.
- ☐ Onderzoek de mogelijkheid dat meer partijen betrokken zijn dan de vermoedelijke fraudeur.
- ☐ Onderzoek de noodzaak van schorsing, op non-actief stellen, ontslag, ...
- ☐ Overweeg de beslaglegging bij de vermoedelijke fraudeur; bepaal diens bezittingen.
- ☐ Informeer zo nodig verzekeringsmaatschappijen en captive.
- ☐ Overweeg aangifte te doen.

Veiligstellen van bewijsmateriaal

- ☐ Digitale gegevens: desktop, laptop, tablet, usb-sticks, gsm, printer, fax, vaste telefoon, telefooncentrale, mailserver, back-ups, camera's, toegangsregistratie, urenregistratie, bewakingscamera's, navigatiesysteem, ... Laat dit doen op forensische wijze zodat het bewijsmateriaal wordt geïndexeerd voor onderzoek, en ook bruikbaar is in een eventuele gerechtelijke procedure.
- ☐ Documenten: arbeidsovereenkomst, gedragscode, boekhouding, contracten, correspondentie, agenda, notities, prullenbak, dvd's, cd's, ...
- ☐ Interview personen die wellicht in een later stadium niet meer voor het onderzoek beschikbaar zullen zijn (ontslag, verlof, onder druk gezet, ...).

Beperk schade en voorkom herhaling

- ☐ Beperk bevoegdheden en toegang van de betrokkene:
  - Informeer interne partijen over beperking toegang: system administrator, receptie, bewaking en beveiliging, magazijn, relevante andere afdelingen, ...
  - Informeer interne partijen over beperking bevoegdheden: bestuur, interne audit, security, risk management, relevante lijnfuncties, ondernemingsraad, ...
  - Informeer externe partijen over beperking bevoegdheden: groepsmaatschappijen, banken, leveranciers, klanten, toezichthouder, kamer van koophandel, staatsblad, vakbonden, ...

- ☐ Draag de taken van betrokkene over aan ander(en).
- ☐ Stop betalingen aan personen/organisaties die mogelijk betrokken zijn.
- ☐ Blokkeer toegang tot de systemen (dataserver, mailserver, paswoord, mailaccount, inbellen, ...) en gebouwen (sleutels, badges, ...).
- ☐ Blokkeer en laat inleveren: bankkaart, kredietkaarten, tankkaarten, gebruik van firmawagen/autosleutels, lidmaatschappen, abonnementen, kortingkaarten, ...

Fraude-audit

- ☐ Opdrachtaanvaarding:
  - Bepaal vereiste deskundigheid.
  - Bepaal vereiste onafhankelijkheid.
  - Bepaal haalbaarheid van het bewijs.
- ☐ Opdrachtuitvoering:
  - Leg overeenkomst schriftelijk vast.
  - Stappenplan en kostenraming.
  - Regelmatig overleg over voortgang, bevindingen en kosten.
  - Interviewen; verzamelen van documenten; analyseren.
  - Documenteren bewijsmateriaal.
  - Bevindingen schriftelijk rapporteren aan crisisteam.
  - Mondelinge toelichting aan crisisteam.
- ☐ Stappen:
  - Ontslag; beslag; aangifte; persbericht; ...

Leren van ervaringen

- ☐ Deel de ervaringen met de rest van de organisatie.
- ☐ Verbeter het frauderesponsplan op basis van de ervaringen.

4. Zelftest

A. Algemeen		Ja	Nee	Weet niet
1.	Wij hebben een antifraudebeleid ontwikkeld en formeel ingevoerd.	☐	☐	☐
2.	Ons bedrijf heeft een gedragscode ontwikkeld en formeel ingevoerd.	☐	☐	☐
3.	Onze raad van bestuur tekent formeel de financiële rapportages af.	☐	☐	☐
4.	Onze directie controleert regelmatig zelf transacties, posities en overeenkomsten.	☐	☐	☐
5.	Wij hebben een speak-up cultuur, met toegankelijke vertrouwenspersonen.	☐	☐	☐
6.	Ons bedrijf heeft een ethics hotline opgezet.	☐	☐	☐
7.	Wij hebben een interne auditdienst of -verantwoordelijke.	☐	☐	☐
8.	Onze commissaris beoordeelt de interne controle rond het opstellen van de jaarrekening.	☐	☐	☐
9.	Wij hebben een zelfstandige ethics/fraud officer of huren deze expertise in.	☐	☐	☐
10.	Wij voeren periodiek frauderisico-assessments uit.	☐	☐	☐
11.	Ons personeel krijgt regelmatig training over fraude en preventie.	☐	☐	☐
12.	Ons bedrijf beschermt en beloont klokkenluiders.	☐	☐	☐
13.	Wij gebruiken reactieve data-analyse om fraude op te sporen.	☐	☐	☐
14.	Wij gebruiken proactieve transactiemonitoring om fraude op te sporen.	☐	☐	☐
15.	Ons bedrijf doet aan pre-employment screening.	☐	☐	☐
16.	Wij hanteren verrassingscontroles zoals mystery shopping en onverwachte tellingen.	☐	☐	☐
17.	Wij werken met jobrotatie en verplichte vakantieopname.	☐	☐	☐
18.	Wij hebben een steunprogramma voor personeel in financiële moeilijkheden.	☐	☐	☐
19.	Ons bedrijf monitort regelmatig zijn antifraudebeleid.	☐	☐	☐
20.	Wij hebben een procedure voor respons en communicatie bij fraudeincidenten.	☐	☐	☐

Deze vragen betreffende antifraudebeleid in het algemeen dienen ter illustratie van deze gids. Ze hebben niet allemaal hetzelfde gewicht in de scoring. Nadere informatie over scoring en diagramweergave zijn verkrijgbaar bij de auteurs.

B. Juridisch		Ja	Nee	Weet niet
1.	De RvB komt frequent samen met een goede voorbereiding en houden een echte beraadslaging over meer dan alleen financiële resultaten; er zetelen niet-operationele of onafhankelijke bestuurders.	☐	☐	☐
2.	De RvB volgt periodiek de uitvoering van haar beslissingen door (senior) management op.	☐	☐	☐
3.	De delegatie van kernbevoegdheden is schriftelijk uitgewerkt met afbakening van interne bevoegdheid en externevertegenwoordigingsbevoegdheid; de gedelegeerden zijn competent, hebben gezag en krijgen voldoende budget.	☐	☐	☐
4.	Een interne sign-off (vier ogen principe) geldt voorafgaandelijk het stellen van risicovolle handelingen door de handtekeningsbevoegde personen; meer dan één handtekening is dan nodig.	☐	☐	☐
5.	'Getrouw beeld' heeft altijd voorrang op 'creatief boekhouden'.	☐	☐	☐
6.	Financiële rapportering gebeurt op basis van tools/software met automatische detectie van fouten & anomaliën, volgens een vastgesteld stramien, direct na afsluiting van het boekjaar, met voldoende controletijd.	☐	☐	☐
7.	De externe accountant of commissaris is echt onafhankelijk van het management. Hij rapporteert aan de RvB over bedreigingen van zijn onafhankelijkheid.	☐	☐	☐
8.	De commissaris of externe accountant weet waar materiële afwijkingen van de jaarrekening door fraude kunnen voorkomen en meldt vastgestelde anomaliën of fraude aan de Raad van Bestuur.	☐	☐	☐
9.	Een interne auditor werd aangesteld, met duidelijke taken en verantwoordelijkheden en passend budget en competentie.	☐	☐	☐
10.	De interne auditor waakt over de identificatie van bedrijfseigen frauderisico's en hun evolutie.	☐	☐	☐
11.	Sollicitanten worden grondig gescreend bij aanwerving. Werknemers krijgen een opleiding met documentatie over de bedrijfsnormen en waarden en politiek ter vermijding van fraude.	☐	☐	☐
12.	Medewerkers worden (steekproefsgewijs) gecontroleerd op fraudegevoelige handelingen.	☐	☐	☐

Zelftest

B. Juridisch (vervolg)		Ja	Nee	Weet niet
13.	De onderneming heeft een externe of interne 'data privacy officer' (DPO).	☐	☐	☐
14.	De onderneming heeft een gedocumenteerd beleid inzake bescherming van privacy en data alsook voor IT Security, én controleert periodiek de naleving ervan.	☐	☐	☐
15.	De activiteiten zijn vergund en de vergunningen worden nageleefd; ook bij latere wijzigingen van activiteiten.	☐	☐	☐
16.	De COO of een door hem aangestelde persoon stuurt en controleert de naleving van de vergunningen. Een plan van aanpak en remediëring bij overtreding is voorhanden.	☐	☐	☐
17.	Bij detectie van fraude treedt een gedetailleerd op voorhand uitgewerkt actieplan in werking met rapportering aan de RvB en senior management.	☐	☐	☐
18.	De onderneming is zich bewust dat bewijsgaring aan bepaalde voorwaarden moet voldoen en laat zich bijstaan door advocaten met beroepsgeheim voor de bepaling van de rechtspositie.	☐	☐	☐
19.	Kent u als bedrijfsleiding volgende misdrijven:	☐	☐	☐
19.1	Een bestuurder maakt systematisch gebruik van goederen die de vennootschap toebehoren (misbruik van vennootschapsgoederen)?	☐	☐	☐
19.2	Een werknemer ontvangt geld om een aanbesteding toe te kennen (passieve private omkoping)?	☐	☐	☐
19.2	Een uitgevoerd contract wordt achteraf schriftelijk opgemaakt en geantidateerd; (valsheid in geschrifte)?	☐	☐	☐

Deze vragen betreffen specifieke juridische aspecten inzake antifraudebeleid. Ze hebben niet allemaal hetzelfde gewicht in de scoring. Nadere informatie over scoring is verkrijgbaar bij de auteurs.

5. Welke maatregelen voor welke fraude?

In hoofdstuk 1 bespraken we de belangrijkste fraudevarianten. In hoofdstuk 2 overliepen we de meest effectieve antifraudemaatregelen. Welke antifraudemaatregelen zijn nu het belangrijkst voor welke soort fraude? De nummering in onderstaande tabel verwijst naar de paragrafen in deze gids. De gele vlakken geven aan dat de betreffende antifraudemaatregel belangrijk is voor de bescherming tegen de betreffende soort fraude. De witte vakken geven aan dat de maatregel eerder een beperkte bescherming zal bieden tegen dit soort fraude. Dit is echter geen exacte wetenschap. De tabel is dan ook bedoeld als hulpmiddel bij frauderisico-evaluaties. Daarbij moet ook het individuele risicoprofiel van het bedrijf betrokken worden: al dan niet import/export, risicogevoeligheid van de sector, organisatiestructuur, ...

Categorieën maatregelen		Fraude varianten									
		Cybercrime		Aankopen en verkopen			Misbruik en diefstal		Verslaggevingsfraude		
		1.1 Lekken en hacken	1.2 Identitetsfraude	1.3 Conflicterende belangen	1.4 Manipulatie offerteprocedures	1.5 Omkoping in het buitenland	1.6 Bedrijfsmiddelen, voorraden	1.7 Financiële middelen	1.8 Financiële rapportages	1.9 Werving en selectie	1.10 Niet-financiële rapportages
Organisatie en leiding	2.1 Leadership			■	■	■	■	■			
	2.2 Toezicht					■	■	■	■		■
	2.3 Cultuur			■	■	■	■		■	■	■
	2.4 Audit	■	■		■	■	■	■	■		■
Frauderisico-evaluaties	2.5 Benchmarking				■	■	■	■			
Preventie en detectie	2.6 Bewustzijn	■	■	■	■	■	■	■			
	2.7 Data-analyse				■	■	■	■	■	■	■
	2.8 Controles	■	■				■	■	■	■	■
	2.9 Personeelsbeleid						■	■		■	
Monitoring, Respons	2.10 Monitoring	■	■	■	■	■	■	■	■		■

6. Een selectie van juridische topics

Een toelichting over fraude en de preventie van fraude kan niet los gezien worden van het wetgevend kader waarin ondernemingen, bestuur, management, personeel en alle andere stakeholders zich bewegen. Deze regelgeving bepaalt de inhoudelijke invulling van misdrijven die onder de noemer fraude aan bod kunnen komen en legt ook de grenzen vast waarbinnen antifraudemaatregelen uitgewerkt worden.

6.1 Goed uitgewerkt corporate governance charter

Ondernemingen met een goed uitgewerkt 'Fraud Risk Management Plan' zijn minder vatbaar voor fraude en lijden in geval van fraude minder schade. Een 'corporate governance charter' draagt niet alleen bij tot 'deugdelijk bestuur' maar ook tot 'deugdelijk ondernemen' naar zowel interne als externe actoren.

Het eerste en wellicht belangrijkste niveau om corporate governance toe te passen is het bestuurs- en senior managementniveau. Fraude krijgt immers de meeste kansen bij afwezigheid van structuur, normering, toezicht en controle.

In België onderscheiden we de 'Corporate Governance Code 2009' (ook wel de 'Code Lippens' genoemd) voor beursgenoteerde ondernemingen en de zogenaamde 'Code Buysse' voor de niet-beursgenoteerde ondernemingen. De implementatie en naleving van de Code Buysse is vrijwillig en opgebouwd rond tien basisprincipes en drie pijlers.

Een actieve en toezichthoudende raad van bestuur

Rechtbanken wijzen vandaag op het belang van een actieve invulling van een bestuursmandaat. Een bestuurder kan zich niet van zijn aansprakelijkheid ontdoen door te beweren dat hij niet actief deelnam aan het bestuur en daarom niet op de hoogte was. We onthouden hierbij:

1. Stel bestuurders aan met competentie en voldoende tijd, die oog hebben voor het belang van de vennootschap. Externe bestuurders zijn een absolute meerwaarde om tunnelvisie en belangenvermenging te voorkomen en om objectiviteit te introduceren. In crisissituaties zijn zij beter geplaatst om controle uit te oefenen op management en personeel. Betaal ook een degelijke vergoeding, want ook hier geldt het principe: 'if you pay peanuts, you get monkeys'.

2. Het bestuur waakt over de uitwerking en de opvolging van een degelijk antifraudebeleid door het (senior) management. Een structurele, open en directe communicatielijn tussen bestuur en management is onontbeerlijk. De voorzitter van de raad van bestuur kan hierin als voortrekker een actieve rol spelen.

3. Een bestuur dat actief sturend optreedt, vermindert het risico op misdrijven, zoals bijvoorbeeld private omkoping, misbruik van vennootschapsgoederen of valsheid in de financiële rapportering.

Een performant (senior) management

Een goed managementteam om fraude te vermijden, is cruciaal. Als operationele leiding staat het management dicht bij de medewerkers en straalt het zijn gezag af op de organisatie. Het (senior) management bestaat uit de uitvoerende bestuurders of de leden van het directiecomité, met als spilfiguur de gedelegeerd bestuurder of de algemeen directeur. Deze laatste heeft een enorme impact op de organisatie en bepaalt mee het ethisch niveau van de organisatie in zijn geheel en in elk onderdeel.

Performantie houdt ook een jaarlijkse evaluatie in door de raad van bestuur. Om frustratie te vermijden, is het belangrijk duidelijke afspraken te maken over gehanteerde parameters en beoordelingscriteria. Een correcte vergoeding is belangrijk. Variabele vergoedingen zijn weliswaar motiverend en sturend, maar ze moeten ook niet de pan uitswingen. Vergoedingssystemen die teveel of nodeloze risico's aanmoedigen, zijn uit den boze, net zoals systemen die valsheid in de financiële rapportering aanmoedigen.

Het 'audit en financieel comité'

We stipten eerder al het belang aan van audit als antifraudemaatregel. Het auditcomité is verplicht voor beursgenoteerde bedrijven. Ook voor een niet beursgenoteerd bedrijf dat een zekere omvang heeft bereikt, is de inrichting van een audit- en financieel comité aangeraden. Het is een adviserend comité in de schoot van de raad van bestuur.

1. Het auditcomité bepaalt de politiek inzake risicobeheer op basis van door het management in kaart gebrachte risico's. Deze risico's situeren zich op alle domeinen in de onderneming (operationeel, financiële rapportering, allerhande regelgeving zoals milieu, fiscaliteit, sociaal, stedenbouw, vergunningen,…) en doorkruisen de diverse hiërarchische niveaus (werkvloer, middenkader, executive management, bestuur,…).

2. Het auditcomité houdt toezicht op de integriteit van de financiële informatieverstrekking door de vennootschap, het onderzoek en de evaluatie van de systemen van interne controle en risicobeheer, alsook op de doeltreffendheid van de interne auditprocessen, op het financiële beleid en de onafhankelijkheid van de commissaris. Het fungeert als aanspreekpunt voor de interne auditor en commissaris. De leden moeten beschikken over voldoende relevante deskundigheid in financiële, boekhoudkundige en auditaangelegenheden.

"Elke bestuurder is contractueel aansprakelijk ten aanzien van de vennootschap wanneer hij zijn mandaat niet naar behoren uitvoert."

De Code Buysse is 'soft law' en haar toepassing is – ondanks het onmiskenbare belang ervan – gebaseerd op vrijwilligheid. De bestuurder heeft beleidsvrijheid en hoeft de aanbevelingen van de code dus niet te volgen. Maar elke bestuurder is contractueel aansprakelijk ten aanzien van de vennootschap wanneer hij zijn mandaat niet naar behoren uitvoert. Een bestuurder moet bijgevolg rekening houden met de beste gebruiken. De Corporate Governance Code hoort daar zonder twijfel bij.

6.2 Delegatie van bevoegdheden

Kan een bedrijfsleider zijn mogelijke strafrechtelijke aansprakelijkheid inperken door een deel van zijn bevoegdheden te delegeren aan een medewerker?
Delegatie van bevoegdheden of verantwoordelijkheden wordt algemeen aanvaard. Delegatie biedt voor leidinggevenden de mogelijkheid om de tussenkomende kaderleden verantwoordelijk te maken en taken en verantwoordelijkheden door te schuiven waardoor er meer tijd vrijkomt voor toezicht en controle. De gedelegeerden krijgen de nodige middelen om normconformiteit binnen hun bevoegdheidsdomein te stimuleren en te handhaven. Het bestuur en het management oefenen hierop toezicht uit. Aldus is delegatie een belangrijk instrument voor risicobeheersing, waaronder ook het voorkomen van fraude.

Delegatie is slechts rechtsgeldig indien aan een reeks voorwaarden is voldaan. Deze voorwaarden zien erop toe dat de gedelegeerden competent zijn en de nodige middelen en het nodige gezag hebben om hun bevoegdheden binnen een duidelijk afgebakend kader uit te oefenen.

Bij een rechtsgeldige delegatie verschuift de verantwoordelijkheid naar de gedelegeerde, maar dat sluit niet automatisch uit dat de delegerende ook zelf (strafrechtelijk) aansprakelijk kan zijn op grond van een eigen fout. Klassiek zal dit het geval zijn wanneer de delegerende te kort schiet aan zijn plicht tot toezicht en de zaken heeft laten aanmodderen terwijl voldoende duidelijk was dat de gedelegeerde niet in staat bleek de gedelegeerde taak naar behoren te vervullen.

6.3 Aansprakelijkheid van bestuurders en leidinggevenden

Er is een belangrijk onderscheid tussen strafrechtelijke en burgerrechtelijke aansprakelijkheid. Hetgeen hieronder uiteen gezet wordt voor een bestuurder geldt ook voor elk directielid (in de zin van het Wetboek van vennootschappen).

Burgerrechtelijke aansprakelijkheid

Een bestuurder is een mandataris van de vennootschap en dus ten aanzien van de vennootschap contractueel gehouden om zijn mandaat op professionele en actieve wijze naar best vermogen uit te oefenen. De aandeelhouders kunnen de bestuurder aansprakelijk stellen bij een foutieve uitvoering van zijn mandaat. Een bestuurder die geen passende structuur en organisatie op poten zet om fraude te vermijden en op die manier fraude faciliteert, handelt niet op professionele wijze en zou hiervoor ten aanzien van de vennootschap aansprakelijk kunnen zijn.

Derden die schade geleden hebben, kunnen een bestuurder alleen aanspreken indien zij bewijzen dat hij een onrechtmatige daad pleegde, dus tekort kwam aan de algemene zorgvuldigheidsplicht. In de praktijk zal een derde dit vaak enkel kunnen bewijzen indien de bestuurder een strafrechtelijke inbreuk pleegde, waardoor die derde schade leed.

Strafrechtelijke aansprakelijkheid

Bestuurders kunnen misdrijven plegen en strafrechtelijk aansprakelijk zijn ten opzichte van de vennootschap, diens aandeelhouders, werknemers, leveranciers en financiers. Misdrijven specifiek voor bestuurders zijn onder meer misbruik van vennootschapsgoederen, valsheid in de jaarrekening, niet-tijdige voorlegging van de jaarrekening aan de algemene vergadering, uitkering van dividenden in strijd met de regels inzake winstuitkering, ... Slachtoffers van strafrechtelijke inbreuken, waaronder bijvoorbeeld de vennootschap, kunnen schade vorderen door zich burgerlijke partij te stellen.

6.4 Strafrechtelijke aansprakelijkheid van de onderneming

Ook privaatrechtelijke en publiekrechtelijke rechtspersonen kunnen zelf strafrechtelijk verantwoordelijk worden gesteld voor hun daden, los van de handelingen van de natuurlijke personen die voor hun rekening handelen. Een strafrechtelijke veroordeling van de rechtspersoon kan leiden tot een gedwongen liquidatie van de onderneming.

Eigen corporatieve schuld

Een rechtspersoon kan strafrechtelijk aansprakelijk zijn wanneer een intrinsieke band bestaat tussen het misdrijf en de rechtspersoon. De rechtspersoon moet dus een 'eigen corporatieve schuld' treffen die niet zuiver afgeleid wordt van de fout begaan door de natuurlijke persoon die het misdrijf pleegde.

In het ondernemingsleven situeren de meeste misdrijven zich in de sfeer van nalatigheid of nonchalance en gaat het over misdrijven die geen bijzonder opzet vereisen. Bijvoorbeeld strafrechtelijk gesanctioneerde overtredingen van de welzijnswet, de loonbeschermingswet, milieuwetgeving, stedenbouwkundige en/of vergunningsregelgeving. Voor dit type misdrijven is de rechtspraak glashelder: een gebrekkige interne organisatie, geen toewijzing van taken en bevoegdheden aan de juiste personen met de juiste bekwaamheden, afwezigheid van toezicht en controle, zijn bepalend voor de eigen corporatieve schuld van de rechtspersoon. Vermits fraudemisdrijven heel vaak voortvloeien uit een gebrek aan leiding, organisatie, structuur en toezicht, kan het ontbreken daarvan door de rechter worden aangewend om de eigen corporatieve schuld van de onderneming vast te stellen.

Voor opzettelijke misdrijven, zoals bijvoorbeeld fiscale fraude, witwassen, valsheid in de jaarrekening,... moet worden aangetoond dat de rechtspersoon zelf doelbewust en intentioneel deze misdrijven pleegde. Het opzet van de geïdentificeerde natuurlijke persoon die het misdrijf pleegde, moet in dat geval samenvallen met het opzet in hoofde van de rechtspersoon.

6.5 Handel met voorkennis

"Misbruik van voorkennis is streng verboden bij beursgenoteerde vennootschappen en vennootschappen die financiële instrumenten emitteren."

Misbruik van voorkennis is streng verboden bij beursgenoteerde vennootschappen en vennootschappen die financiële instrumenten emitteren. Dit verbod treft niet alleen de leidinggevenden, werknemers en aangestelden van de emittent, maar ook sommige toeleveranciers en externe dienstverleners. Ook deze laatste doen er daarom goed aan specifieke gedragsregels te voorzien voor hun medewerkers.

Met de wet van 31 juli 2017 worden strengere strafsancties voorzien voor marktmisbruik. Daarenboven moeten alle personen en instellingen met een vergunning van of een inschrijving bij de FSMA of de Nationale Bank van België een passende interne meldingsprocedure invoeren (een zogenaamde 'klokkenluidersregeling') om dergelijke inbreuken te melden.

6.6 Fraudebewijs vergaren

"Het bewijsmateriaal moet rechtmatig zijn en ook rechtmatig verkregen zijn."

Notities:

Bij een fraudeonderzoek is het uiteraard de bedoeling om bewijs in handen te krijgen dat – indien nodig – als rechtmatig bewijs kan worden gebruikt. Het bewijsmateriaal moet rechtmatig zijn en ook rechtmatig verkregen zijn.

Een voorbeeld van onrechtmatig bewijs is onder andere het bewijs dat tot stand komt met miskenning van het beroepsgeheim of de discretieplicht (bijvoorbeeld van de advocaat, revisor, accountant) of door valsheid in geschrifte. Dergelijk bewijs kan nooit worden gebruikt voor het bestraffen van fraude.

Bij onrechtmatig verkregen bewijs is het bewijs op zich niet onrechtmatig, maar wordt het mogelijk onbruikbaar door de manier waarop het werd verkregen. Hierbij denken we aan bewijzen verkregen door uitlokking, met miskenning van de wettelijke vereisten voor de privédetective (bijvoorbeeld zonder toestemming gemaakte beeldopnames, in niet voor het publiek toegankelijke plaatsen), door een schending van het recht op privacy van de werknemer bij een ontslag om dringende redenen,... In een aantal gevallen kan onrechtmatig verkregen bewijs toch worden gebruikt.

Een rechter mag evenwel nooit rekening houden met onregelmatig verkregen bewijs wanneer:

- vormvoorwaarden voorgeschreven op straffe van nietigheid niet werden gerespecteerd;
- de begane onrechtmatigheid de betrouwbaarheid van het bewijs heeft aangetast;
- het gebruik van het bewijs in strijd is met het recht op een eerlijk proces.

Rechtbanken behouden dus een grote appreciatiebevoegdheid voor bewijzen die op een 'onregelmatige wijze' werden verkregen. Een goed voorbereide onderneming zal bij de opsporing en het bewijs van fraude dan ook aandacht hebben voor het gebruik van rechtmatig én regelmatig verkregen bewijsmiddelen.

Onrechtmatig verkregen bewijs (bijvoorbeeld via een bewakingscamera die niet bij de Privacycommissie is aangegeven) kan in een aantal gevallen toch nog worden gebruikt in rechte op basis van de door het Hof van Cassatie uitgewerkte Antigoon-criteria.[17]

6.7 Privacy

Bij het uitwerken van een fraudebeleid en bij het uitvoeren van een fraudeonderzoek komt privacy geregeld aan bod, omdat alle gegevens (data, beelden, digitale gegevens, e-mails,...) aan de hand waarvan een persoon kan worden geïdentificeerd, persoonsgegevens zijn en onder de privacyreglementering vallen.

GDPR is op komst

De privacyreglementering is streng en het grootste risico is dat de onderneming het verkregen bewijs niet in rechte kan gebruiken. De recente Europese Privacyverordening (GDPR, General Data Protection Regulation) die vanaf 25 mei 2018 wordt toegepast, voorziet een gevoelige verstrenging van de privacyreglementering. Een onderneming zal door deze wetgeving bijkomend waakzaam moeten zijn, omdat de Privacycommissie in de toekomst bijkomende slagkracht krijgt en er voor inbreuken op deze Europese Verordening aanzienlijke boetes (tot 20 miljoen euro) kunnen geheven worden.

Vuistregels

Bij iedere 'verwerking' van persoonsgegevens (bijvoorbeeld een data-analyse, of het monitoren van internetverkeer) moeten de algemene privacybeginselen maximaal gerespecteerd worden:

1. Transparantie: de personen van wie de gegevens verwerkt worden, moeten dit weten en hierover afdoende geïnformeerd zijn.
2. Finaliteit: een verwerking kan enkel voor rechtmatige doeleinden, bijvoorbeeld uitvoering van een overeenkomst, gerechtvaardigd belang of wettelijke verplichting.
3. Proportionaliteit: is de inbreuk op de privacy wel evenredig met het beoogde doel?

"De personen van wie de gegevens verwerkt worden, moeten dit weten en hierover afdoende geïnformeerd zijn."

Vanaf 25 mei 2018 zal iedere onderneming een dataregister moeten bijhouden en voor nieuwe procedures/producten een privacy assessment moeten verrichten (effectenbeoordeling) waarbij de privacytoets wordt verricht alsook wordt gecontroleerd of er geen alternatieven beschikbaar zijn die de privacy niet of minder schaden.

1. Voorzie een privacyreglement en een privacybeleid. Grotere bedrijven en bedrijven die veel persoonsgegevens verwerken, zullen daarenboven een Data Privacy Officer (DPO) moeten aanstellen.
2. Kies voor het minst privacygevoelige alternatief, wetende dat bij camerabewaking of controle op e-mail- of internetgebruik u in ieder geval rekening moet houden met het recht op privacy en de toepasselijke regelgeving.

Bronnen

[1] Report to the Nations 2016, Association of Certified Fraud Examiners, Houston, Texas, US, 2016
www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf
[2] Fortune-500, US, 2015
http://beta.fortune.com/global500/list
[3] Institute of Fraud Auditors (IFA) Belgium, 2017
www.ifabelgium.be
[4] Association of Certified Fraud Examiners (ACFE) Belgium, 2017
www.acfebelgium.be
[5] EBBEN Partners, 2017
www.ebbenpartners.be/advieslijn
[6] Internationale antifraudestandaarden, een selectie:
- Fraud Risk Management Guide, COSO, US, 2016.
- Basistechnieken van de bedrijfsrevisor in het kader van fraude, ICCI (red.), Maklu, Antwerpen, 2012.
- Internal Auditing and Fraud, Practice Guide, Institute of Internal Auditors, US, 2009.

[7] UK Bribery Act (VK, 2012) en Foreign Corrupt Practices Act (VS, 1977)
[8] Belgische Gids voor Cyberveiligheid, International Chamber of Commerce (ICC) Belgium, Brussel, 2014
www.vbo-feb.be/publicaties/belgische-gids-voor-cyberveiligheid_2014-05-26/.
[9] Anticorruptiegids voor Belgische ondernemingen in het buitenland, FOD Economie, Brussel, 2016
http://economie.fgov.be/nl/binaries/Anticorruptiegids_tcm325-281523.pdf
[10] Fraud Risk Management Guide, Committee of Sponsoring Organizations of the Treadway Commission (COSO), US, 2016
www.coso.org/Pages/Purchase-Guide.aspx
[11] Waeterinckx P., Deruyck F., Van Volsem F. (red.), Strafrecht in de onderneming - Praktsche gids voor bestuurders en zaakvoerders, 3e editie, Intersentia, Mortsel, 2016
http://intersentia.be/nl/shop/academisch/strafrecht-in-de-onderneming-3e-editie.html
[12] Lammers E.J., Forensic auditing in België, Kluwer, Mechelen, 2013
http://shop.wolterskluwer.be/shop/nl_BE/Actiesites/expertise-in-de-kijker-audit/Forensic-auditing-in-Belgi-;pgid=NexqqvHSeedSR05Msvx90MoW0000Ad-UU2AK;sid=fGrNS31rDgfJSyWEPhgZsNWrzzE2Rc4wh2Q=?p=BPFORAUDIBI13001
[13] Olislaegers & De Creus, 2017
www.odc.be
[14] Corruption Perceptions Index (CPI) van Transparency International
www.transparency.org/research/cpi/overview
[15] Financial Action Task Force (FATF)
www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-february-2017.html
[16] Samenspanning bij overheidsopdrachten - Een gids voor inkopers bij overheden, Belgische Mededingingsautoriteit, 2017
www.bma-abc.be/sites/default/files/content/download/files/20170131_overheidsopdrachten.pdf
[17] Van der Sype, Y., Antigoon gesust. Het privédetective verslag als bewijs in (on)rechte, Or. 2015, afl. 8

Disclaimer

De in deze gids vermelde informatie is louter algemeen van aard en is niet gericht op de specifieke situatie van een individu of een rechtspersoon; ze is niet noodzakelijk volledig, accuraat of bijgewerkt; dit is geen professioneel of juridisch advies; ze vervangt het advies van een expert niet; en ze geeft geen garanties voor een veilige bescherming. Voor specifieke situaties kan u contact opnemen met de auteurs van wie u de contactgegevens kan terugvinden op www.ebbenpartners.be en www.odc.law.

Over de auteurs

Deze gids is geschreven onder de verantwoordelijkheid van EBBEN Partners[5], een onafhankelijke dienstverlener op het gebied van governance, risk & compliance, gespecialiseerd in integriteit- en fraudezaken. De juridische aspecten zijn geschreven onder de verantwoordelijkheid van Olislaegers & De Creus[13], een nichekantoor gespecialiseerd en actief in de zakenadvocatuur.

Evert-Jan Lammers is Registered Fraud Auditor en partner bij EBBEN. Hij is erevoorzitter van het Institute of Fraud Auditors (IFA) Belgium, bestuurslid van Transparency International Belgium, voorzitter van het platform International Cooperation van het Institute for Financial Crime, voorzitter van European Rating House, voormalig leider van KPMG Forensic Belgium, en executive professor fraud auditing aan de Antwerp Management School.

Sonny Luypaert is Certified Fraud Examiner en partner bij EBBEN. Tevens is zij voorzitter van de Association of Certified Fraud Examiners (ACFE) Belgium. Zij startte haar carrière als boekhoudster bij een Belgische kmo en was later onder meer CFO Benelux van Accenture, Controller ECEMEA van Baxter Healthcare en CFO/COO van The Boston Consulting Group Belgium.

Dylan Casaer is lid van de balie te Brussel en vennoot bij het advocatenkantoor Olislaegers & De Creus. Hij heeft 20 jaar expertise in arbeidsrecht & privacy als advocaat voor zowel kmo's als multinationaal actieve ondernemingen en hij heeft 12 jaar bestuurservaring als schepen van de stad Aalst bevoegd voor personeelszaken.

Kristof De Creus is lid van de balie te Brussel en samen met Michael Olislaegers stichtend vennoot van het advocatenkantoor Olislaegers & De Creus. De voorbije 25 jaar was hij juridisch adviseur en advocaat van zowel kmo's als multinationaal actieve ondernemingen.

colofon

D/2017/0369/02
Deze Voka Wijzer werd geschreven door Evert-Jan Lammers, Sonny Luypaert, Dylan Casaer en Kristof De Creus i.s.m.:

Voka-kenniscentrum
Niko Demeester | Secretaris-generaal
Stijn Decock | Hoofdeconoom
Sonja Teughels | Arbeidsmarkt
Veronique Leroy | Arbeidsmarkt en arbeidsverhouding
Jonas De Raeve | Onderwijs
Vincent Thoen | Innovatie en economie
Goedele Sannen | Mobiliteit en logistiek
Ellen Vanassche | Milieu en klimaat
Klaas Nijs | Energie en klimaat
Steven Betz | Ruimtelijke ordening en milieu
Karl Collaerts | Fiscaliteit en begroting
Pieter Van Herck | Welzijns- en gezondheidsbeleid
Gilles Suply | EU en internationaal ondernemen

Eindredactie
Erik Durnez, Sandy Panis

Foto's
Shutterstock, Chak López

Concept en vormgeving
Propaganda, Zaventem

Druk
INNI Group, Heule

Structurele partner:

Voka Wijzer 'Fraudepreventie in uw onderneming' is een brochure van Voka – Vlaams netwerk van ondernemingen.

Verantwoordelijke uitgever
Hans Maertens i.o.v. Voka vzw - Burgemeester
Callewaertlaan 6 - 8810 Lichtervelde
info@voka.be - www.voka.be

Notities:

EBBEN
PARTNERS

WWW.EBBENPARTNERS.BE

Olislaegers & De Creus
advocaten - avocats

WWW.ODC.LAW

voka