ONDERZOEK

Non-compliance-risico's: voorkom schade en schande

Inhoud

Over het onderzoek

Fraude, corruptie en non-compliance. Het blijven actuele thema's binnen Nederland. Als sprake is van bewuste overtredingen van wet- en regelgeving, keurt de maatschappij dat af. Niet alleen vanwege de economische schade, maar ook omdat sprake is van morele afkeuring en schande. Bestuurders, toezichthouders en vaak ook de externe accountant hebben dan wat uit te leggen. Daarom is het van belang dat organisaties hun zaken op orde hebben en zich regelmatig afvragen of gedragingen passend zijn. Van een externe accountant wordt verwacht dat daarop wordt toegezien.

Dit onderzoek is voor het tweede jaar op rij uitgevoerd door de afdelingen Audit & Assurance en Forensics & Technology van BDO. De resultaten van dit jaar worden afgezet tegen die van het vorige rapport en geven mogelijke veranderingen in non-compliancerisico's weer. Dit biedt waardevolle inzichten voor bedrijven om hun aanpak ten aanzien van fraude-, corruptie- en non-compliancerisico's te verbeteren en zich beter voor te bereiden op toekomstige uitdagingen.

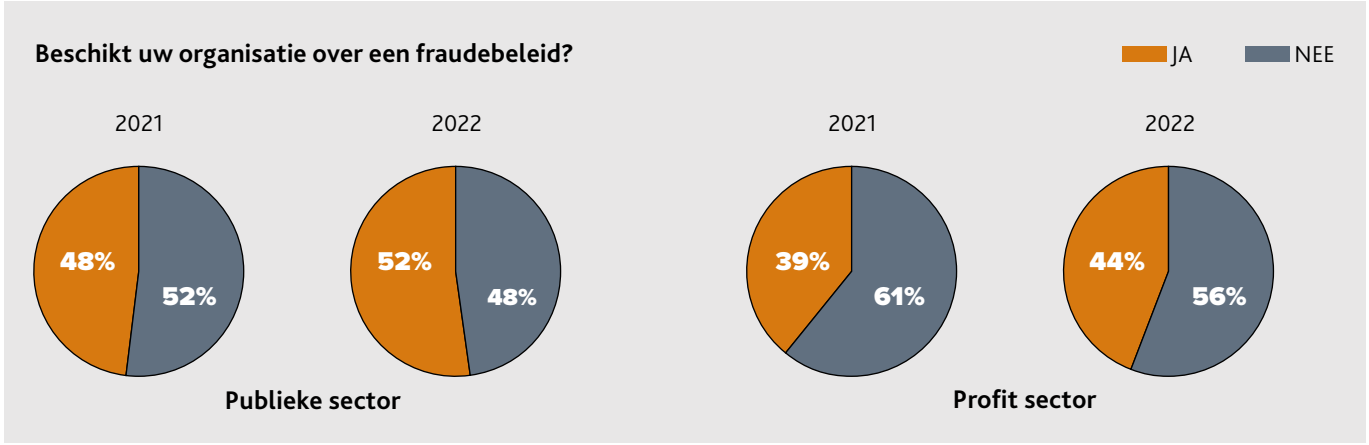
Ons onderzoek is gebaseerd op een uitgebreide enquête onder bijna 1000 organisaties, bestaande uit ongeveer 750 profitorganisaties en 250 nonprofitorganisaties (hierna: 'publieke sector'). We vroegen deze organisaties naar de stand van zaken rondom compliance, de risico's met betrekking tot zowel fraude en corruptie als overtredingen van wet- en regelgeving. Hoe gaan organisaties om met hun eigen fraudebeleid en frauderisicoanalyse? Werken ze samen met tussenpersonen (agenten)? En, zijn ze voorbereid op een fraude-incident? Dit onderzoek levert een aantal interessante inzichten op, die wij graag met u delen. Niet in de laatste plaats het besef dat er mogelijkheden liggen voor organisaties om hun compliance framework te verbeteren.

1. Fraudebeleid en incident-responsplan liggen niet op de plank

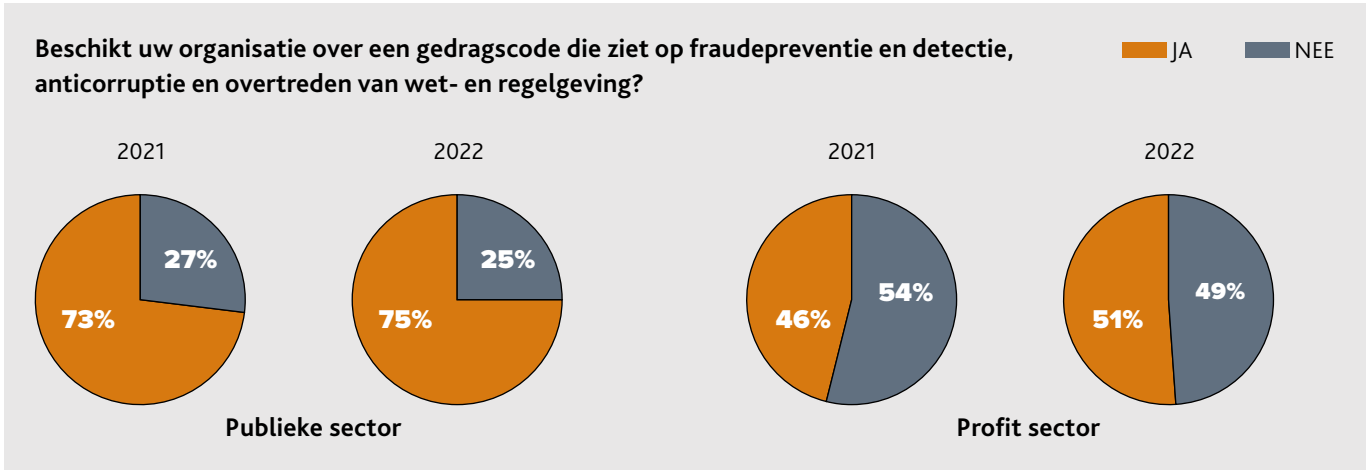
Publieke sector een stap verder dan profitsector

Ondernemen is risico nemen. Een raamwerk van maatregelen zorgt er voor dat deze risico's aanvaardbaar zijn én voorkomt dat schade ontstaat. De organisatiestructuur, governance en intern toezicht, beleid en strategie, interne beheersing en processen dragen - naast de bedrijfscultuur - bij aan het beheersen van de belangrijkste (bedrijfs)risico's. Risico's op fraude, corruptie en andere non-compliance lijken moeilijker te beheersen dan de meeste andere risico's. Met name omdat sprake is van bewuste overtredingen van wet- en regelgeving, waarbij de mens vaak een belangrijke rol speelt. De mens is immers een denkende en calculerende risicofactor. Dit neemt echter niet weg dat entiteiten ook hier maatregelen kunnen nemen om non-compliance zo veel als mogelijk te voorkomen en te beheersen.

Een fraudebeleid speelt hierin een belangrijke rol. In zo'n beleid staan de belangrijkste uitgangspunten over 'eerlijk zakendoen'. Het geeft de kaders weer van integer handelen in en door een organisatie en spreekt werknemers en andere (zaken)partners als het ware direct aan. Uit ons onderzoek blijkt echter dat veel entiteiten niet over een dergelijk beleid beschikken:

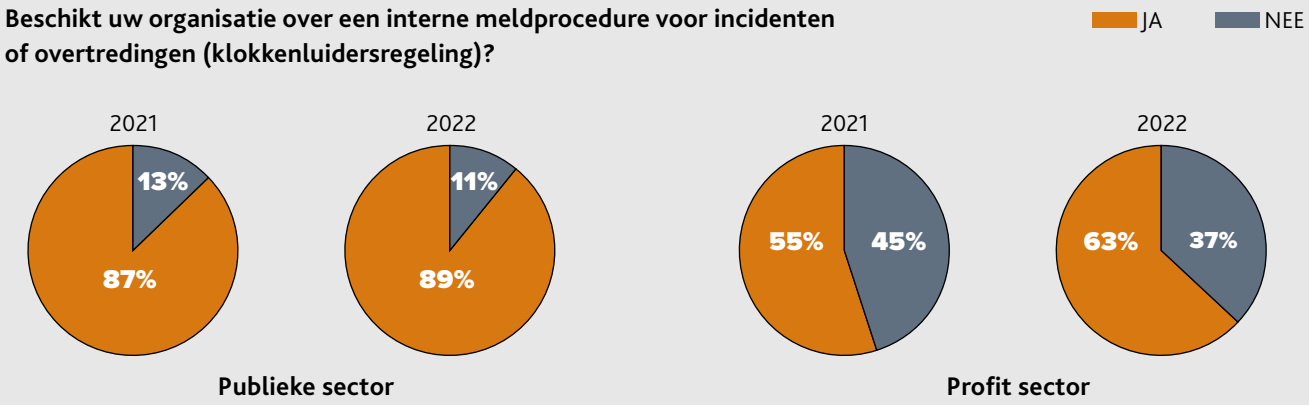


Ten opzichte van het vorige onderzoek is er een licht positieve ontwikkeling in het percentage respondenten dat over een fraude-beleid beschikt. Dat geldt zowel in de profit- als in de publieke sector. Het is nog steeds zo dat in de profitsector minder dan de helft van de bedrijven zegt te beschikken over een (formeel) fraudebeleid. In de publieke sector is de verdeling ongeveer fiftyfifty. Dit schuurt te meer omdat een deel van de organisaties (ook) niet beschikt over een gedragscode, waarin de gedragsregels rondom fraudepreventie en -detectie, anticorruptie en het voorkomen van overtredingen van wet- en regelgeving zijn vastgelegd. Organisaties uit de publieke sector scoren hier aanmerkelijk beter dan profitbedrijven: 75% van de publieke sector tegen 51% van de profit heeft een dergelijke gedragscode. Positief is dat in beide sectoren sprake is van een lichte toename ten opzichte van vorig jaar.



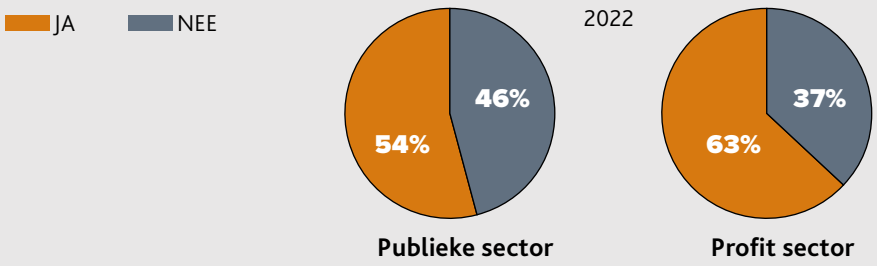
Organisaties werden ook bevraagd of zij beschikken over een (formele) interne meldprocedure voor incidenten of overtredingen, anders gezegd een (interne) klokkenluidersregeling. Ook hier valt op dat organisaties in de publieke sector beter scoren dan de profitsector. Bijna 90% van de respondenten uit de publieke sector tegen ruim 60% van de profitsector zegt over zo'n interne procedure te beschikken. Ook hier geldt dat in beide sectoren sprake is van een stijging ten opzichte van het vorige onderzoek. Hoewel de profit nog achterblijft is daar dit jaar wel een mooie inhaalslag te zien (+8%).

Beschikt uw organisatie over een interne meldprocedure voor incidenten of overtredingen (klokkenluidersregeling)?



Naast Nederlandse wet- en regelgeving speelt ook internationale regelgeving een belangrijke rol in het zakendoen. Denk aan de Amerikaanse Foreign Corrupt Practices Act (FCPA), de Engelse UK Bribery Act en de Franse Sapin 2, die veelal een extraterritoriale werking hebben. Wij hebben daarom nagevraagd of organisaties beleidslijnen en procedures hebben omtrent de naleving van wet- en regelgeving:

Beschikt uw organisatie over beleidslijnen en procedures inzake naleven van wet- en regelgeving?
Beleidslijnen en procedures

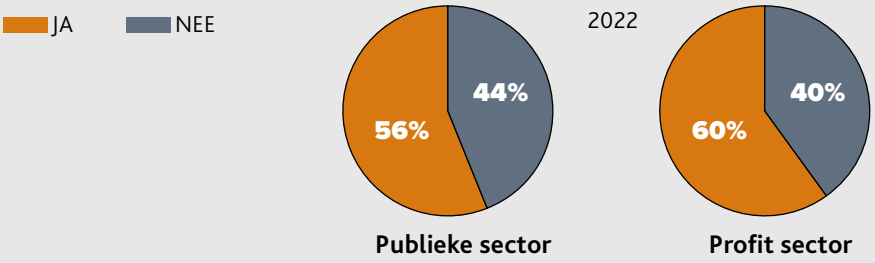


Zowel in de publieke sector (46%) als in de profitsector (37%) geven respondenten aan dat er geen processen en procedures zijn die zien op het naleven van wet- en regelgeving. Dat is een opmerkelijke uitkomst, omdat wet- en regelgeving veelal de *licence to operate* voor een organisatie betreft. Dit geldt in de profit-, maar zeker ook voor de publieke sector. Naast het feit dat overtredingen kunnen leiden tot financiële schade, is er ook een belangrijk risico op reputatieschade. Denk hierbij ook aan schendingen van bijvoorbeeld milieuregels, iets waarvoor in het kader van de aankomende CSRD-verplichtingen steeds meer aandacht nodig is.

Voor iedere organisatie is het belangrijk om te beschikken over beleidslijnen en procedures om op die manier risico's te identificeren, te beoordelen en passende maatregelen te nemen om deze risico's te beperken. Die beleidslijnen en procedures bieden een kader voor de verantwoordelijkheden voor medewerkers en hoe zij dienen om te gaan met mogelijke fraude en andere compliance-inbreuken. Deze medewerkers zijn immers de 'oren en ogen' van de organisatie om non-compliancerisico's te voorkomen en te beheersen.

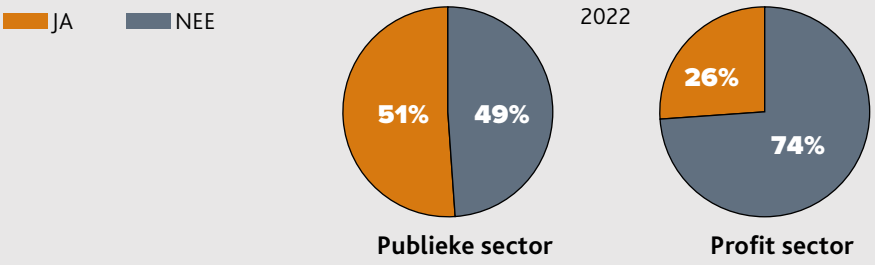
Eerder schreven we over het al dan niet beschikbaar zijn van een fraudebeleid en/of een gedragscode. In het verlengde van bovenstaande zijn dit jaar twee nieuwe vragen gesteld. De eerste vraag betreft het besluitvormingsproces, de tweede ziet op het al dan niet hebben van een eigen frauderisicoanalyse. Ten aanzien van de eerste vraag wordt zowel in de publieke als in de profitsector door respondenten relatief vaak (56% resp. 60%) aangegeven dat besluitvorming in handen is van slechts één of enkele personen. Dit kan - zeker in het mkb - logisch zijn, aangezien er maar één of enkele beslissingsbevoegden zijn. Er kan echter ook sprake zijn van kwetsbaarheid en een gevoeligheid, doordat individuen (ook) persoonlijk gewin nastreven.

Is de besluitvorming omtrent transacties in handen van een beperkt aantal personen? Denk bijvoorbeeld aan leveranciersselectie en investeringsbeslissingen.
Besluitvorming omtrent transacties



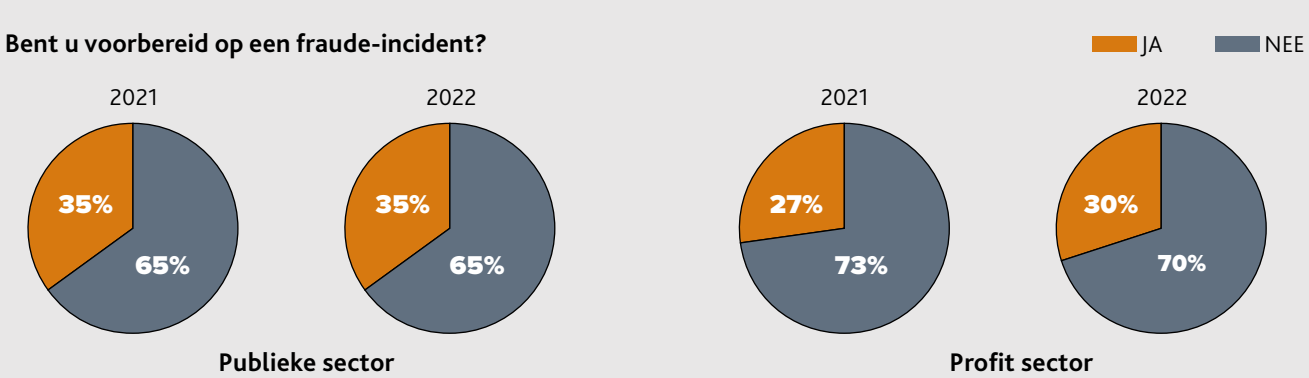
Als het gaat om de eigen frauderisicoanalyse, geeft ruim 50% van de respondenten uit de publieke sector aan dat binnen hun organisatie (periodiek) een frauderisicoanalyse wordt uitgevoerd. In de profitsector is dit net iets meer dan 25%. In beide sectoren is dus nog heel wat te winnen en wij bevelen dan ook van harte aan dat organisaties werk maken van het in kaart brengen van hun belangrijkste fraude-, corruptie- en andere non-compliancerisico's. Niet alleen omdat de accountant dit vraagt, maar ook en vooral voor de organisatie zelf.

Heeft u een frauderisicoanalyse uitgevoerd?
Frauderisicoanalyse

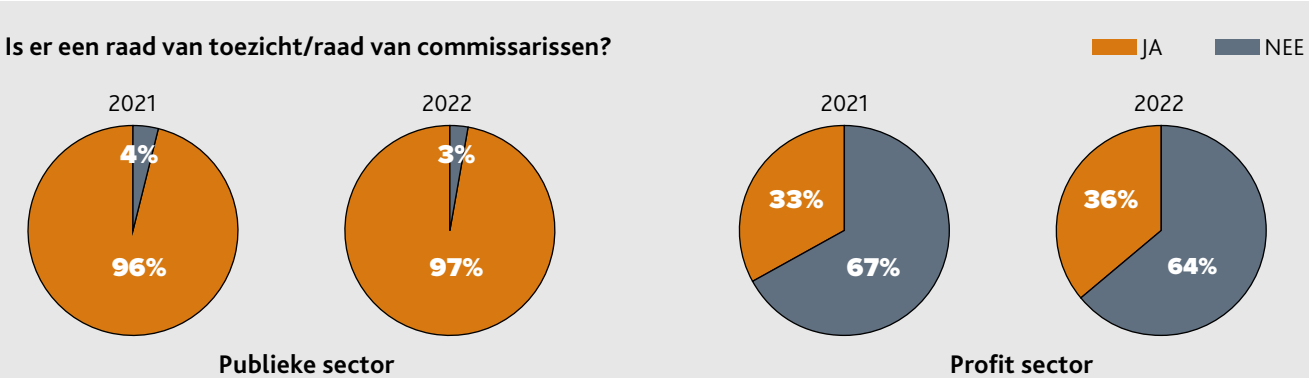


'EHBO-doos' bij weinig organisaties aanwezig

Tot slot de hamvraag: zijn organisaties voorbereid op een fraude-incident? Want het hebben van een fraudebeleid, een gedragscode en een klokkenluidersregeling is één ding. Maar wat als er écht iets aan de hand is en er snel geschakeld moet worden? Is er een spreekwoordelijke EHBO-doos aanwezig? Hebben organisaties een noodplan voorhanden, een fraude- of incidentresponsplan, waarin bijvoorbeeld de belangrijkste contactpersonen zijn vastgelegd of wie de leiding en coördinatie op zich neemt? En waarin staat welke maatregelen moeten worden genomen, zoals het veiligstellen van data, het instellen van nader onderzoek - en door wie - en de interne en externe communicatiestrategie. Het antwoord is ten opzichte van het vorige onderzoek nauwelijks verbeterd:



Hoewel incidenten nooit helemaal te voorkomen zijn, spelen tone at the top en (bedrijfs)cultuur een belangrijke rol in de vatbaarheid van organisaties voor non-compliancerisico's. Een open cultuur, waarin mensen elkaar durven aan te spreken, draagt bij aan voorkomen en beheersen van incidenten. Het is aan het bestuur en management van organisaties om deze cultuur te bevorderen. Dat gebeurt door een combinatie van meer 'formele' uitingen (zoals een gedragscode, processen en procedures) en het bevorderen en bewaken van een goede bedrijfscultuur. Het is aan de interne toezichthouders (raad van commissarissen) om daarop toezicht te houden. Nagenoeg alle organisaties uit de publieke sector beschikken over een raad van toezicht/raad van commissarissen. In de profitsector beschikt (slechts) een derde van de organisaties over zo'n toezichthouder. Hier is dus ruimte voor verbetering, met name omdat een goede raad van commissarissen een bestuur ook uitdaagt en prikkelt op onderwerpen die van nature minder prettig zijn, zoals fraudebeheersing en tone at the top.

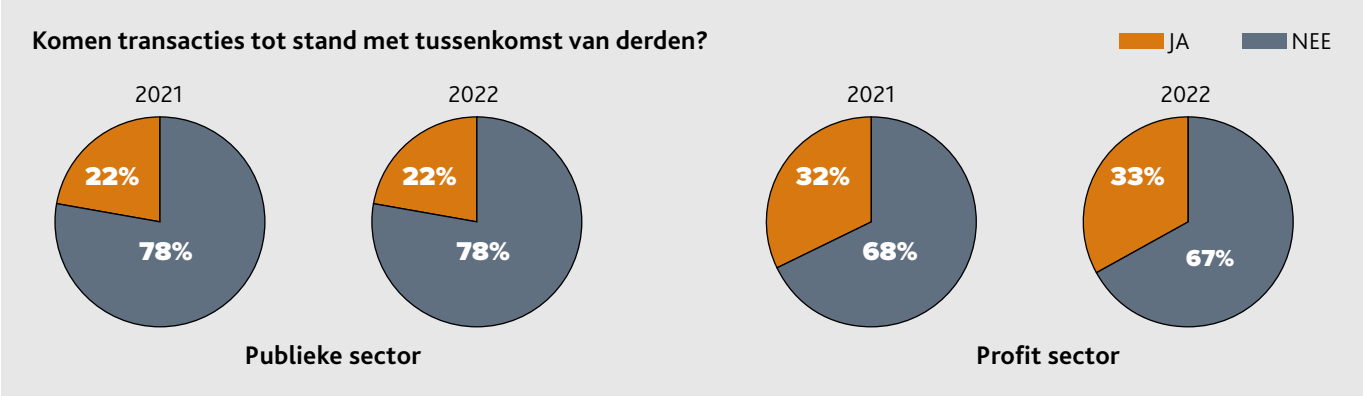


2. Zakendoen via tussenpersonen of agenten

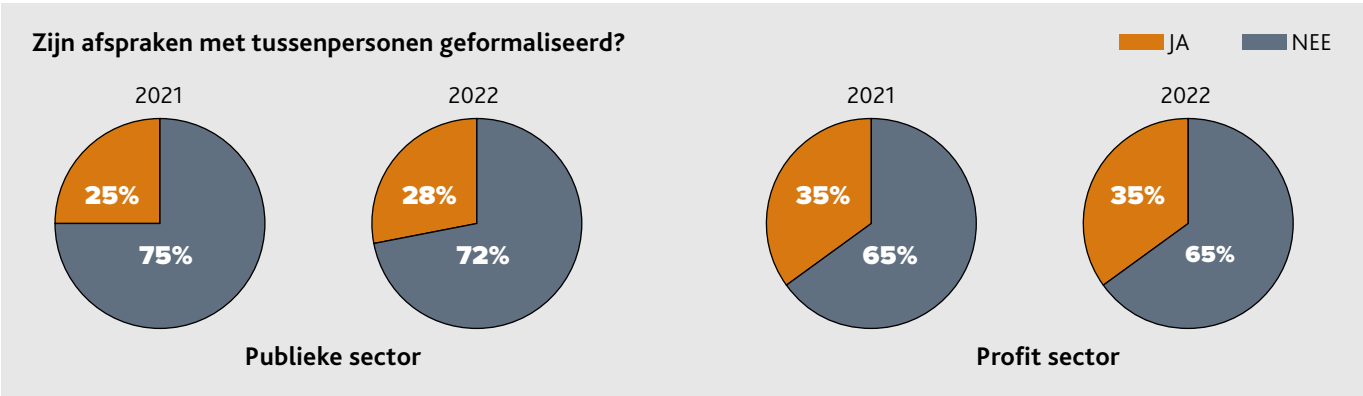
Onbekend, maar zeker niet onbemind

Organisaties maken, bij het doen van inkopen of verkopen, soms gebruik van tussenpersonen. Denk aan transacties via assuradeurs, makelaars of andere intermediairs. Hiermee is op zich niets mis. Maar, er kan ook sprake zijn van agenten of tussenpersonen die, tegen betaling van een - soms resultaatafhankelijke - vergoeding, diensten verrichten die niet helemaal transparant zijn. Hierdoor is niet altijd duidelijk wat de agent of tussenpersoon precies doet, waarop de vergoeding is gebaseerd en hoe betaling plaatsvindt. Daardoor bestaat het risico dat een deel van de vergoeding wordt gebruikt om transacties oneigenlijk te beïnvloeden. Het kan daardoor zelfs voorkomen dat tussenpersonen - namens de onderneming - ambtenaren of anderen omkopen. Van belang is te realiseren dat (het bestuur van) de onderneming verantwoordelijk is voor het handelen van de ingeschakelde tussenpersoon.

Wij onderzochten of en in hoeverre organisaties gebruikmaken van tussenpersonen. Volgens de respondenten uit de profitsector is dat in ongeveer een derde van de gevallen zo, in de publieke sector ligt dat rond een vijfde.

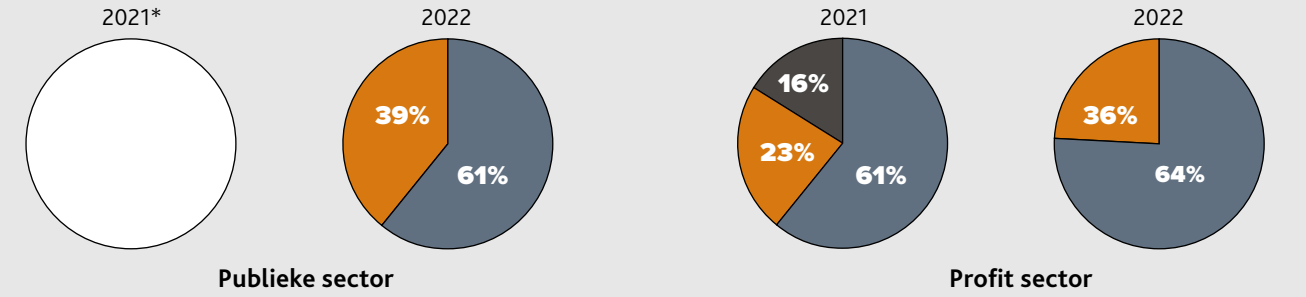


Áls sprake is van tussenpersonen, is het onze verwachting dat afspraken zijn geformaliseerd en (daardoor) meetbaar en controleerbaar zijn, bijvoorbeeld via een zogeheten *right to audit-clausule*. Dat blijkt echter niet het geval. Onderstaande percentages hebben betrekking op organisaties die aangaven soms gebruik te maken van tussenpersonen. Hieruit blijkt dat in de publieke sector slechts in ongeveer 25% van de gevallen sprake is van geformaliseerde afspraken, bijvoorbeeld in de vorm van een contract. In de profitsector ligt dat iets hoger (35%). Er is dus ook nog een overgroot deel waarbij afspraken niet zijn vastgelegd. Hierdoor neemt de kans toe dat tussenpersonen niet doen wat is beoogd en is sprake van een hoger non-compliancerisico.



Ook komt de vraag op of organisaties de tussenpersoon waarmee ze in zee gaan, wel goed kennen. Dit is met name van belang indien sprake is van een agent of tussenpersoon in het buitenland. Via een due diligence-onderzoek kan inzicht worden verkregen in de achtergronden van de tussenpersoon en kan onder andere een financieel, juridisch en/of integriteitsonderzoek betreffen. Respondenten geven echter aan dat zo'n onderzoek vaak niet wordt uitgevoerd:

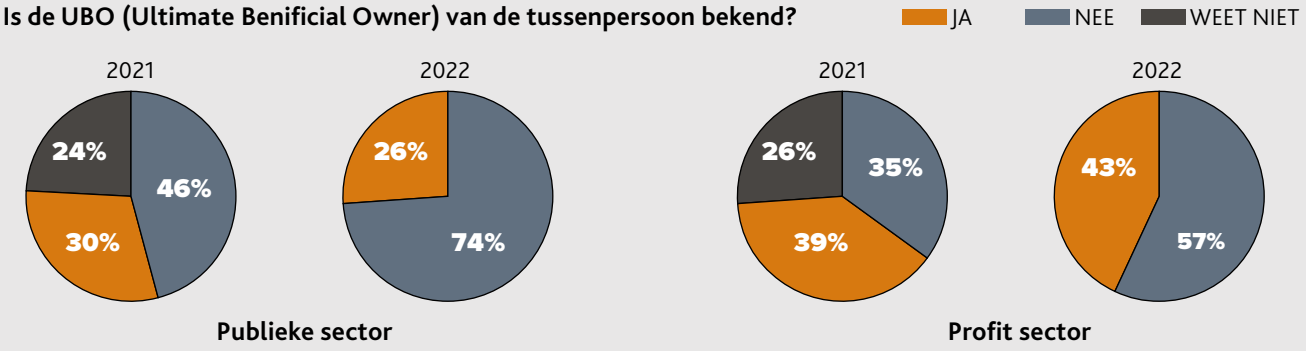
Heeft u een due diligence-onderzoek uitgevoerd naar de tussenpersoon?



** Deze vraag is in 2021 niet gesteld aan respondenten uit de publieke sector.*

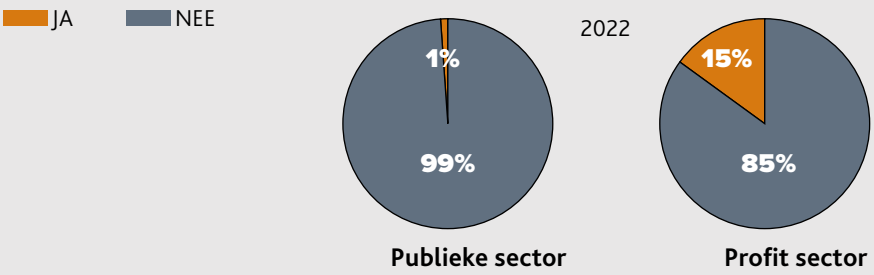
Ook blijkt, bij de organisaties die gebruikmaken van tussenpersonen, de uiteindelijke eigenaar - ofwel de Ultimate Benificial Owner (UBO) - lang niet altijd bekend. Hoewel de profitsector hier beter scoort dan de publieke sector, is er een hoog percentage respondenten dat aangeeft de UBO('s) van een ingeschakelde agent of tussenpersoon niet te kennen:

Is de UBO (Ultimate Benificial Owner) van de tussenpersoon bekend?



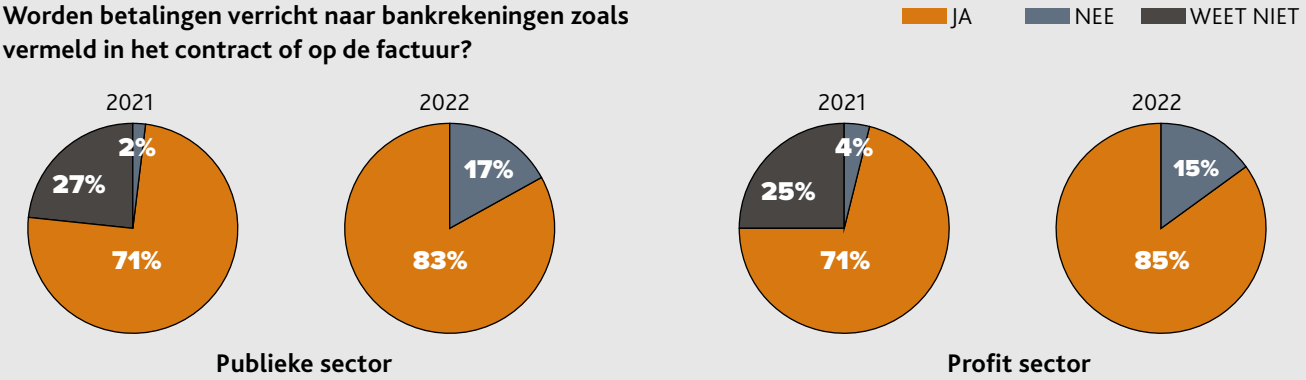
Aanvullend is dit jaar gevraagd of ook zaken wordt gedaan in landen met een hoger corruptierisico. In de publieke sector blijkt dat, passend bij de aard van hun activiteiten, nauwelijks het geval. In de profitsector komt dit wel voor, namelijk in ongeveer 15% van de gevallen. In die gevallen kan sprake zijn van een verhoogde risico-indicatie, een zogeheten *red flag*.

Werkt u in landen met een hoog corruptierisico?



Er is positief nieuws te melden als het gaat om het doen van betalingen. Zowel in de profit- als de publieke sector geeft ongeveer 85% van de respondenten aan dat betalingen aan tussenpersonen plaatsvindt via het bankrekeningnummer dat vooraf in het contract met of op de factuur van de tussenpersoon is vermeld. Aan de andere kant: in nog steeds zo'n 15% van de gevallen wordt daarvan afgeweken. Ook dat kan een indicator zijn van een corruptierisico, met name als sprake is van betalingen aan of via hoogrisicolanden.

Worden betalingen verricht naar bankrekeningen zoals vermeld in het contract of op de factuur?



Organisaties die aangeven gebruik te maken van tussenpersonen of agenten werd ook gevraagd of er vergoedingen worden betaald in de vorm van een resultaatafhankelijke vergoeding (succesfee). Het slagen van een transactie heeft dan direct impact op (de hoogte van) de vergoeding die de tussenpersoon ontvangt. Daardoor kan sprake zijn van een hoger corruptierisico. Slechts een beperkt deel van de respondenten (19% uit de profitsector en 8% uit de publieke sector) geeft aan dat transacties tot stand komen op basis van een succesfee. In die gevallen is extra alertheid geboden omdat ook dan weer sprake kan zijn van een corruptierisicofactor.

Over BDO

BDO Forensics & Technology ondersteunt organisaties bij geschilbeslechting, maar ook bij het voorkomen, detecteren en adequaat reageren op fraude, corruptie en non-compliance.

Een manier om incidenten te voorkomen is inzicht creëren in waar uw organisatie risico's loopt op niet-naleving van wet- en regelgeving. Onze specialisten helpen organisaties met het creëren van inzicht in deze risico's en het mitigeren hiervan, bijvoorbeeld door het opstellen van een fraudebeleid en het verder verbeteren van frauderisicomanagement.

BDO Audit & Assurance controleert uw jaarrekening of andere financiële verantwoording. Daarbij wordt niet alleen naar 'het boekje' gekeken, maar ook naar zaken als privacy, ICT, strategie en bedrijfsvoering, bedrijfscontinuïteit en fraude-, corruptie- en overige non-compliancerisico's. BDO Audit & Assurance vindt het belangrijk dat zaken niet alleen kloppen (binnen de regels zijn), maar ook deugen. Daaraan besteden wij, samen met de gecontroleerde organisaties, veel tijd en aandacht.

Heeft u vragen over frauderisicopreventie en -beheersing óf audit? Neem dan voor een vrijblijvende kennismaking contact met ons op.

Wilt u meer informatie?
Neem dan contact op met:

DICK VAN ONZENOORT
Partner BDO Forensics & Technology
E dick.van.onzenoort@bdo.nl
T 06 - 41 15 01 95

COEN MATEIJSEN
Partner BDO Audit & Assurance
E coen.mateijsen@bdo.nl
T 040 - 269 81 24

MEER INFORMATIE
Wil je meer weten over
BDO Forensics & Technology?
Kijk dan op onze website.

www.bdo.nl

02/2024 – BM2412