

ONDERZOEK

Fraude- en andere risico's in beeld: van beleid naar praktijk

Analyse non-compliancerisico's 2024

Inhoud

Over het onderzoek	02
Heeft u al wél een fraudebeleid?	03
Frauderresponsplan	05
Cyber	06
Het risico van het ongebruikelijke	08
Sanctiewet	09
Over BDO	11

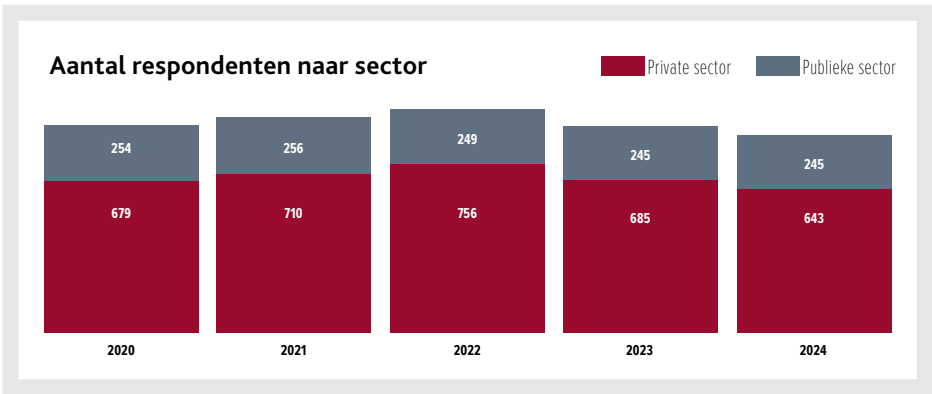
Over het onderzoek

In een snel veranderende wereld, waar regelgeving voortdurend in beweging is en maatschappelijke verwachtingen blijven toenemen, hoort het thema non-compliance hoog op de agenda van organisaties te staan. Het voorkomen en beheersen van fraude, corruptie en andere integriteitsschendingen vormt immers een wezenlijk onderdeel van goed bestuur en verantwoord ondernemerschap. Toch blijkt uit onderzoek dat geen enkele sector immuun is voor deze uitdagingen. De praktijk leert dat bewuste aandacht voor compliance, risicobeheersing en ethisch handelen niet alleen een wettelijke en maatschappelijke plicht is, maar ook bijdraagt aan het behoud van vertrouwen van stakeholders en de reputatie van een organisatie.

Alweer voor het vijfde jaar op rij brengt BDO Forensics & Technology, in samenwerking met BDO Audit & Assurance, de belangrijkste trends, inzichten en ontwikkelingen op het gebied van non-compliance in kaart. Hiermee ondersteunen we organisaties bij het versterken van hun weerbaarheid en het realiseren van duurzame verbeteringen. Daarvoor hebben wij onderzoek uitgevoerd naar fraude-, corruptie en andere non-compliancerisico's¹.

Ons onderzoek is gebaseerd op een uitgebreide enquête onder honderden organisaties in zowel de private als de publieke sector. In de publieke sector konden wij een nadere verdeling maken naar woningcorporaties, zorginstellingen, lagere overheden en maatschappelijke organisaties. De private sector is nader verdeeld in financiële dienstverlening, food & flowers, TMT (techniek, media & telecommunicatie), bouw & vastgoed en een grote groep 'overige'.

De resultaten bieden inzicht in de ontwikkelingen op het gebied van bewustwording, beleidsvorming en risico-inschattingen van organisaties in verschillende sectoren. Als organisatie in één van de sectoren kunt u nagaan hoe u scoort ten opzichte van de benchmark en kunt u bepalen welke stappen nog ondernomen moeten worden om non-compliancerisico's te mitigeren.



¹ Hierna, ten behoeve van de leesbaarheid van deze publicatie, veelal gezamenlijk aangeduid als 'fraude(risico's)'

Heeft u al wél een fraudebeleid?

Wij komen het vaak tegen: organisaties hebben bijvoorbeeld wel een gedragscode of een klokkenluidersregeling en soms ook zelf een frauderisicoanalyse uitgevoerd, maar missen een overkoepelend fraudebeleid. Daarmee zijn de eerder genoemde documenten vaak onsamenvattende delen, die elk op zich waardevol kunnen zijn, maar als geheel onvoldoende richting en houvast bieden. Dit gebrek aan integratie leidt ertoe dat verantwoordelijkheden onduidelijk zijn, processen niet op elkaar aansluiten en cruciale lessen uit incidenten niet worden geborgd in het beleid.

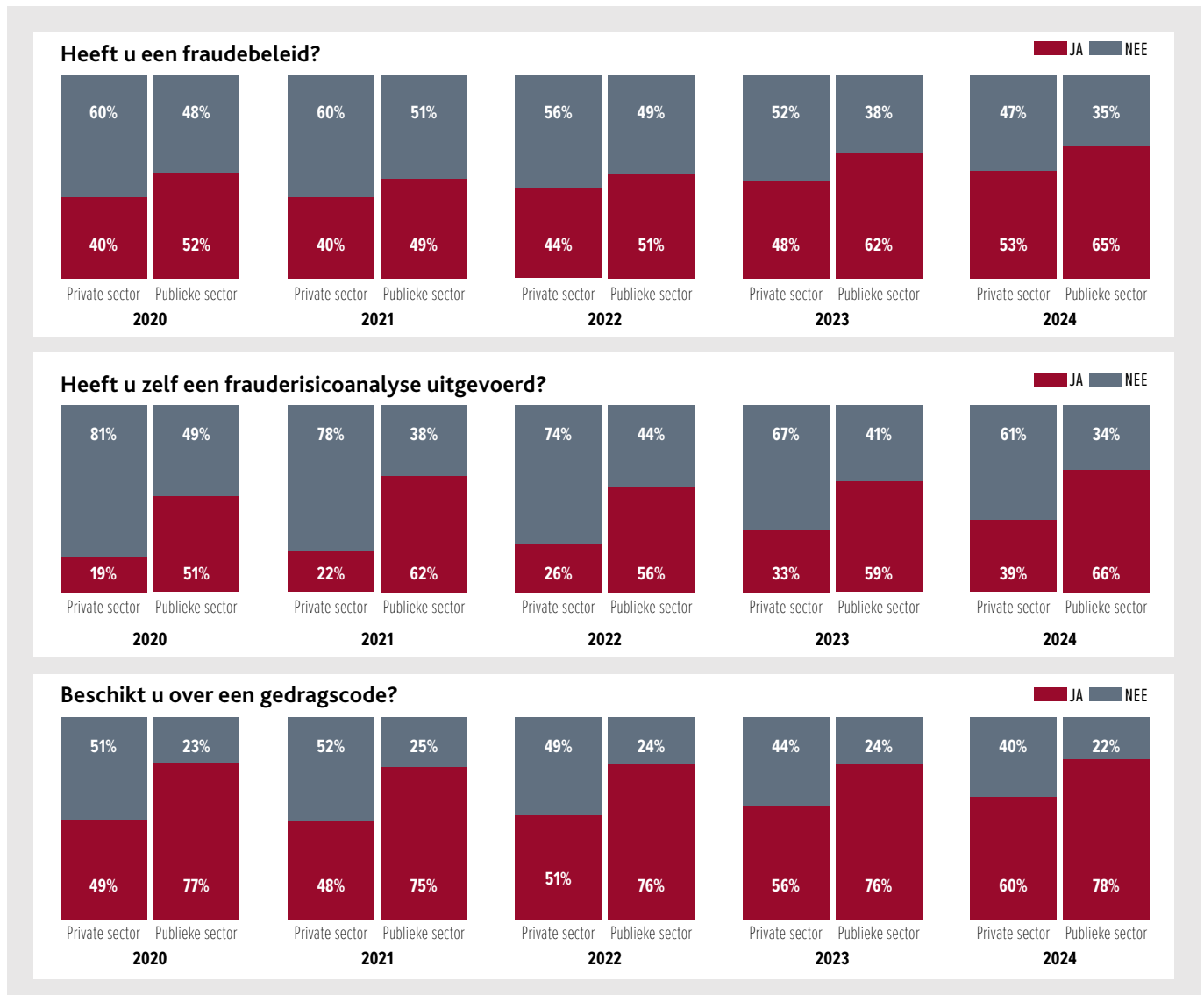
Een overkoepelend fraudebeleid vormt het fundament waarop andere regelingen steunen en zorgt voor een structurele en consistente aanpak waarbij preventie, detectie en opvolging van fraude helder zijn vastgelegd en breed worden gedragen binnen de organisatie. Bijkomend voordeel: er ontstaat een cultuur waarin integriteit vanzelfsprekend is en risico's beheersbaar blijven.

Een belangrijk element van een overkoepelend fraudebeleid is dat het zich niet beperkt tot alleen de technische kant van risico's en maatregelen. Belangrijk is juist ook de bereidheid van de organisatie om een bepaalde mate van risico te accepteren uit hoofde van haar ondernemerschap en/of maatschappelijk doel. Ook bevat het de organisatiestandpunten omtrent eventuele 'grijze gebieden' waarmee een organisatie vanuit de aard van haar activiteiten te maken heeft. Het fraudebeleid is daarmee onderdeel van de visie en identiteit van de organisatie.

Een eigen frauderisicoanalyse geeft organisaties inzicht in de specifieke risico's die binnen hun processen en organisatiecultuur spelen. Door niet alleen te vertrouwen op algemene richtlijnen, maar zelf risico's in kaart te brengen, kunnen kwetsbaarheden en mogelijke fraudevormen tijdig in beeld komen. Dit helpt om gerichte maatregelen te nemen en daarbij te focussen op die onderdelen die het meest effectief zijn.



Ook dit jaar vroegen wij aan onze respondenten of zij beschikten over een integraal fraudebeleid, of zij zelf (jaarlijks) een frauderisicoanalyse uitvoeren en of zij beschikken over een gedragscode. In onderstaande grafieken geven wij de ontwikkelingen aan.



De trend van de afgelopen jaren heeft zich gelukkig voortgezet, wat onder andere betekent dat intussen meer dan 50% van de organisaties uit de private sector beschikt over een integraal fraudebeleid. Ook in de publieke sector zet die stijgende lijn zich voort. Hetzelfde geldt voor het hebben van eigen frauderisicoanalyse en het bezit van een gedragscode.

Wat opvalt is dat de publieke sector doorgaans verder is in de implementatie van deze instrumenten dan de private sector. In de publieke sector zijn integriteitsvraagstukken en transparantie al langere tijd een vast onderdeel van de organisatiecultuur, mede door wettelijke kaders en maatschappelijke verwachtingen. Hierdoor is het hebben van een integraal fraudebeleid, een eigen frauderisicoanalyse en een breed gedragen gedragscode vaker de norm; organisaties worden er ook scherper op beoordeeld en afgerekend.

In de private sector is wel een inhaalslag zichtbaar: steeds meer bedrijven onderkennen het belang van een structurele aanpak en investeren in het uitwerken en implementeren van fraudebeleid en gedragscodes. Toch blijft het percentage organisaties met een volledig uitgewerkt en geïntegreerd beleid nog altijd fors achter bij de publieke sector. Dit verschil laat zien dat er winst te behalen valt, vooral bij bedrijven waar integriteit en frauderisicomanagement nog niet vanzelfsprekend zijn verankerd. Door te investeren in een integraal beleid, een eigen analyse en een duidelijke gedragscode, maar óók in trainingen om het bewustzijn op fraude- en corruptierisico's te verhogen, vergroten organisaties hun weerbaarheid en dragen zij bij aan een transparante en integere bedrijfsvoering. En ja, dit soort maatregelen kosten geld, maar wegen niet op tegen de schade als een organisatie écht wordt geraakt door een fraudegeval.

Frauderresponsplan

Een alarmerende constatering

Hoewel steeds meer organisaties investeren in een integraal fraudebeleid, risicoanalyses en gedragscodes, blijkt uit ons onderzoek dat de daadwerkelijke voorbereiding op een fraude-incident in zowel de private als de publieke sector achterblijft. Slechts ongeveer 35% van de organisaties in de private sector en 47% in de publieke sector geeft aan daadwerkelijk voorbereid te zijn als zich een fraude-incident voordoet. Dit betekent dat een ruime meerderheid van de organisaties geen adequaat frauderresponsplan heeft.

Zonder een vooraf vastgesteld en geoefend stappenplan ontbreekt het aan heldere procedures, eenduidige verantwoordelijkheden en een gestructureerde aanpak wanneer een incident zich voordoet. Dit leidt ertoe dat organisaties vaak reactief handelen, waardoor kostbare tijd verloren gaat, bewijsstukken verloren kunnen raken en de impact van de schade groter uitvalt dan nodig is.

Daarnaast kan het gebrek aan voorbereiding leiden tot onzekerheid binnen de organisatie, onduidelijkheid richting externe partijen en reputatieschade. In het ergste geval kan dit het vertrouwen van medewerkers, klanten en andere stakeholders ernstig aantasten. Wij adviseren daarom om voorbereid te zijn op een incident en een draaiboek klaar te hebben. Want juist in een tijd waarin fraude steeds complexer wordt en meer en meer digitaliseert, is het van essentieel belang om als organisatie voorbereid te zijn. Een frauderresponsplan is niet alleen een papieren document, maar een praktisch instrument waarmee organisaties adequaat, snel en effectief kunnen reageren op incidenten. Het vastleggen van procedures, verantwoordelijkheden en communicatielijnen zorgt ervoor dat de schade wordt beperkt, de juiste lessen worden getrokken en het vertrouwen behouden blijft.

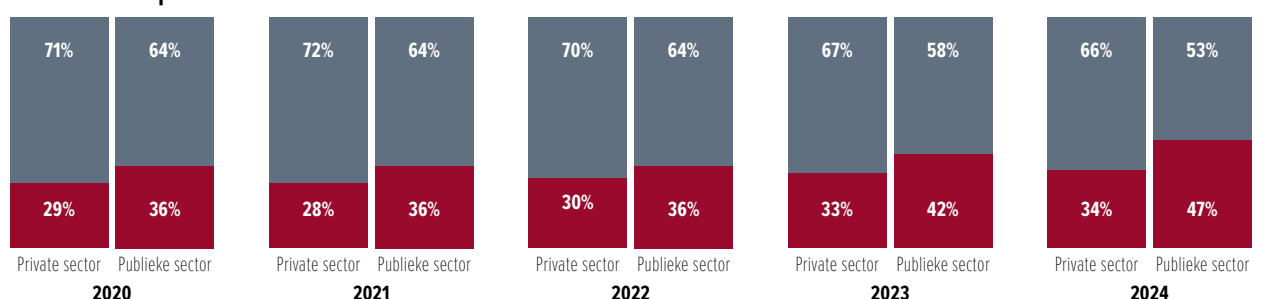
Een goed frauderresponsplan is geen *stand alone* document, maar een onderdeel van het fraudebeleid en sluit hierop dus aan. Dat betekent bijvoorbeeld dat kaders en verantwoordelijkheden duidelijk zijn. Maar het gaat ook nog een stap verder. Door zaken concreet te maken, voor het geval zich een incident voordoet. Bijvoorbeeld:

- ▶ Wie beoordeelt de eerste melding?
- ▶ Wie heeft de leiding?
- ▶ Wie moeten wel en niet worden geïnformeerd?
- ▶ Hoe wordt data veiliggesteld en door wie?
- ▶ Welke advocaat wordt -indien nodig- geraadpleegd?
- ▶ Wie kan worden ingezet voor (forensisch) onderzoek?
- ▶ Welke arbeidsrechtelijke maatregelen kunnen worden genomen?
- ▶ Hoe wordt omgegaan met externe communicatie of vragen uit de pers?

Oproep tot verbetering

De constatering dat slechts 35% van de organisaties in de private sector beschikt over een frauderresponsplan vraagt om gerichte actie. Organisaties doen er verstandig aan niet alleen te investeren in preventie en detectie, maar ook in concrete voorbereiding op het onvermijdelijke moment dat er iets misgaat. Door het ontwikkelen, testen en onderhouden van een frauderresponsplan verhogen organisaties hun weerbaarheid, minimaliseren ze schade en dragen ze bij aan een integere en toekomstbestendige bedrijfsvoering.

Voorbereid op fraude incident 2020-2024

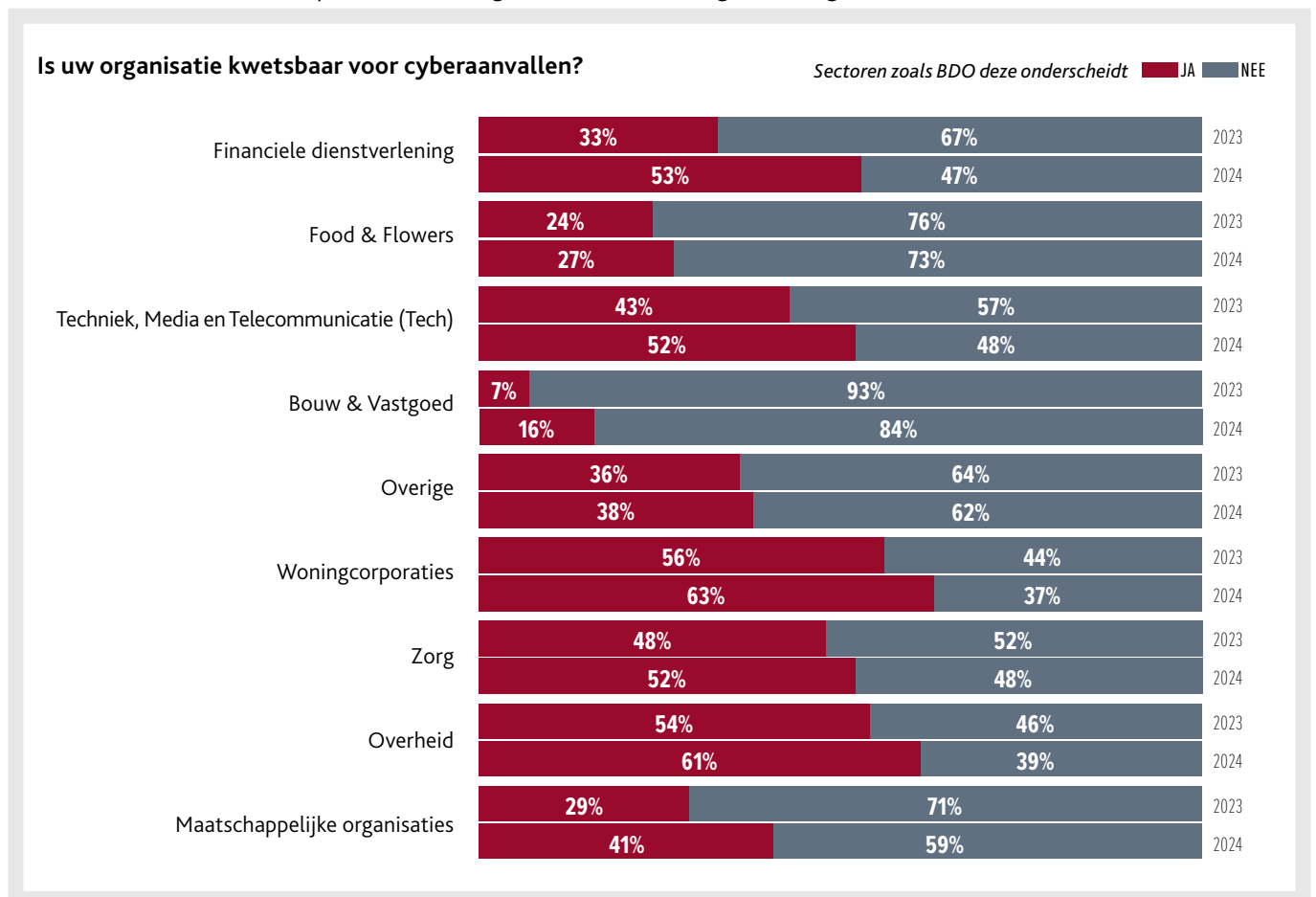


Cyber

Gezien de actualiteit van het onderwerp hebben wij vorig jaar voor het eerst specifiek onderzoek gedaan naar de kwetsbaarheid voor cyberaanvallen in relatie tot de afhankelijkheid van digitale gegevensverwerking. Dat onderzoek hebben wij dit jaar herhaald. Hieruit blijkt dat organisaties hun eigen kwetsbaarheid voor cyberaanvallen hoger inschatten dan een jaar geleden. Dit geldt zowel voor de private als de publieke sector, waarbij die inschatting in beide gevallen zo'n 5% hoger ligt. In die zin lijken alle investeringen in cyberbeveiliging, technische maatregelen maar vooral bewustwordingscampagnes hun vruchten af te werpen: mensen lijken zich méér bewust van de risico's. Daarbij blijft de afhankelijkheid van digitale gegevensverwerking logischerwijs onverminderd groot, zo niet groter dan vorig jaar: vrijwel alle kernprocessen binnen organisaties zijn digitaal verweven, van klantcommunicatie en logistiek tot personeelsadministratie en financiële afhandeling.

De groeiende complexiteit van cyberdreigingen vraagt om voortdurende alertheid. Het blijft daarom cruciaal om niet alleen te blijven investeren in technologische oplossingen, maar ook in actuele kennis en helder beleid rondom digitale weerbaarheid. Het is van belang dat organisaties niet alleen vertrouwen op hun beveiligingssystemen, maar zich ook realiseren dat de afhankelijkheid van digitale systemen de potentiële schade bij incidenten vergroot. Daarom verdienen ook de gedrags- en menselijke risico's rond cyber bijzondere aandacht. Menselijk handelen blijft immers een van de zwakste schakels in de digitale beveiliging. Denk hierbij aan het onbewust klikken op phishinglinks, het delen van wachtwoorden of het onvoldoende herkennen van verdachte situaties. Zelfs met de beste technische beveiliging kan een onoplettende medewerker grote gevolgen hebben voor de organisatie.

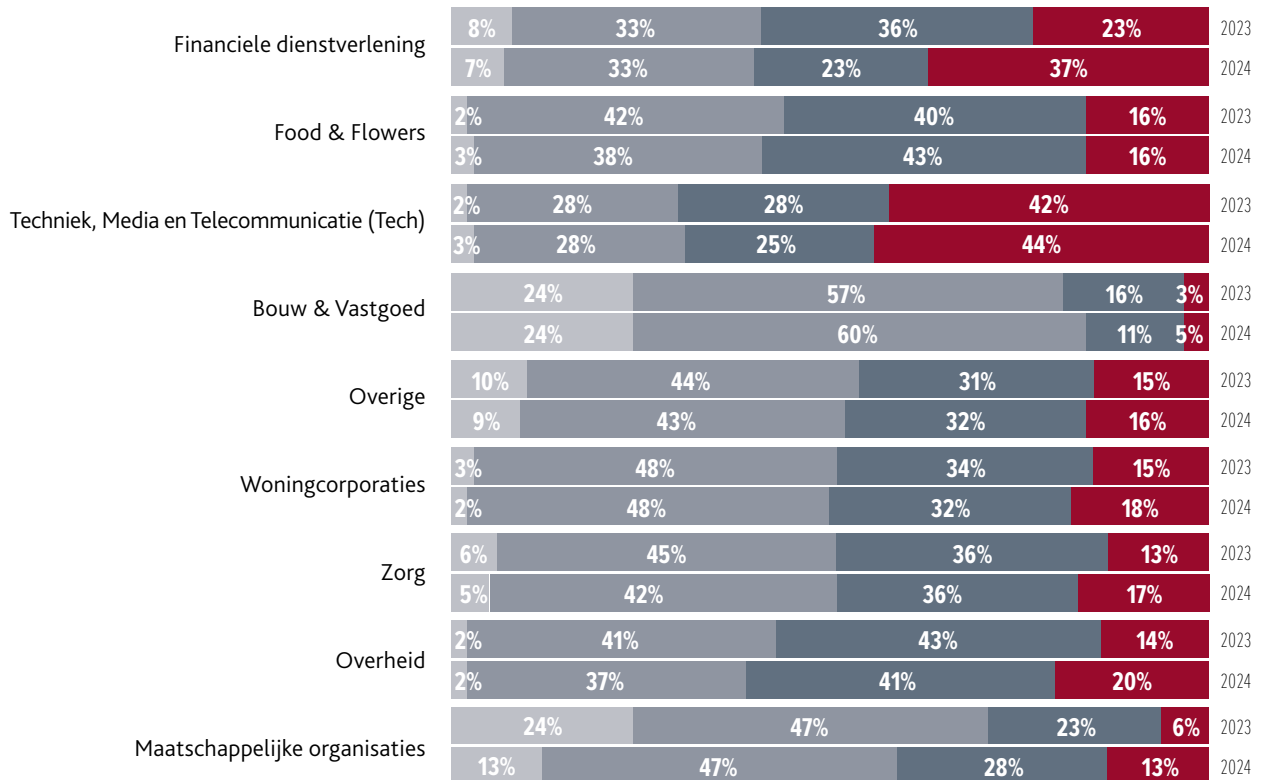
Het is daarom essentieel om te investeren in regelmatige bewustwordingscampagnes, trainingen en het stimuleren van een open meldcultuur, zodat medewerkers alert blijven en zich verantwoordelijk voelen voor de digitale veiligheid van de organisatie. Wij adviseren daarom structureel aandacht te besteden aan cyberweerbaarheid en aan het oefenen van responsplannen, waardoor zowel de continuïteit als de reputatie van de organisatie kan worden gewaarborgd.



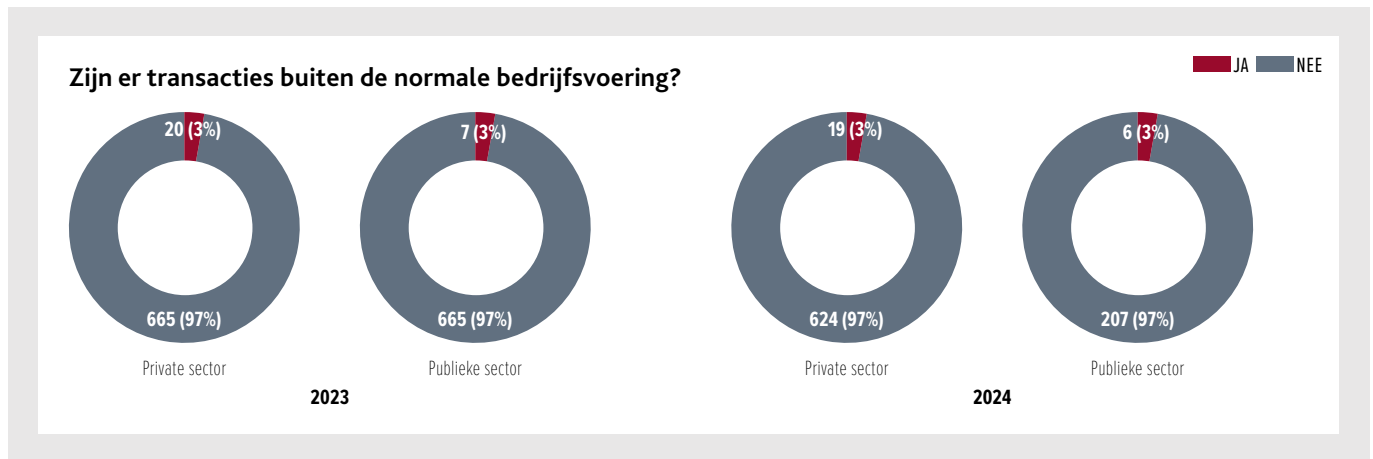
Hoe afhankelijk van digitale gegevensverwerking bent u voor de continuïteit van uw organisatie?

Sectoren zoals BDO deze onderscheidt

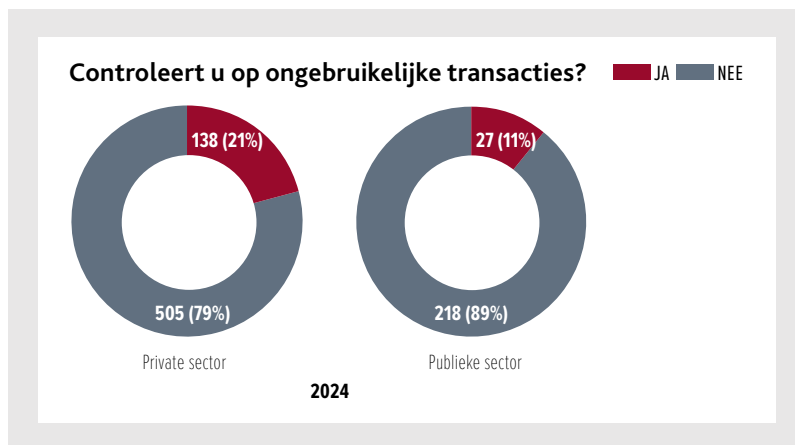
NIET GEMIDDELD GROOT ZEER GROOT



Het risico van het ongebruikelijke



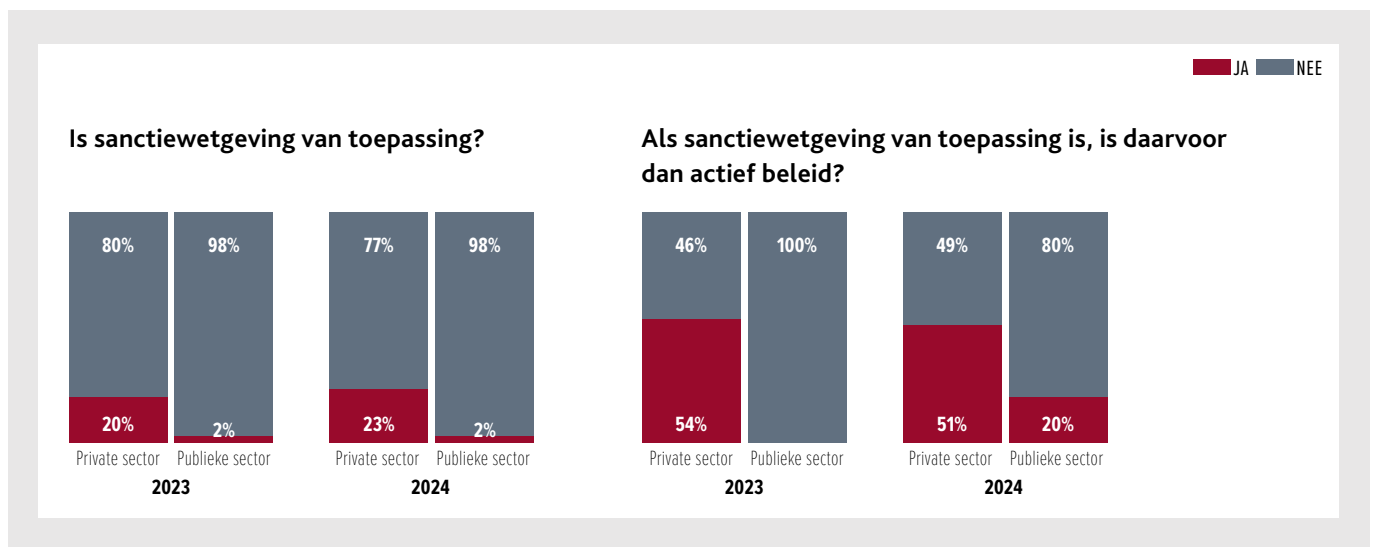
Net zoals vorig jaar vroegen wij of er weleens transacties plaatsvinden die buiten de normale bedrijfsvoering vallen. Dat percentage blijft, over het geheel bezien, onverminderd laag (3%). Dit jaar vroegen wij voor het eerst of organisaties ook daadwerkelijk controleren op ongebruikelijke transacties. De reactie hierop viel ons tegen: slechts 21% van de respondenten uit de private sector en 11% uit de publieke sector gaat actief na of sprake is van mogelijke ongebruikelijke transacties. Dat verklaart ons inziens ook waarom er maar 3% niet -reguliere zaken wordt gesignaleerd... Wij adviseren organisaties dan ook meer focus aan te brengen en scherpere controles aan te brengen die helpen om bijzonder zaken proactief te signaleren en vervolgens gerichte acties te ondernemen.



Stel: je verkoopt goederen of diensten aan bedrijf A, maar de betaling komt van een bankrekening van bedrijf B. Dat kán heel legitiem zijn. Bijvoorbeeld als dit van tevoren bekend is en bedrijf B behoort tot de groep van A en voor die groep alle financiële afwikkelingen verzorgt. Maar het kan ook anders: bedrijf B is onbekend, de relatie met A is onduidelijk, B zit in een heel andere bedrijfstak of is sowieso moeilijk traceerbaar. In dat geval is alertheid geboden, want het risico bestaat dat bedrijf B een tussenpersoon is voor ondergronds bankieren. In 2023 kwam daarvan een [grote casus](#) aan het licht, waarbij ruim 100 Nederlandse bedrijven betalingen ontvingen van bedrijfjes uit Denemarken, die niet hun directe klant waren. De Deense bedrijven werden gebruikt om geld uit Syrië, Libië en Irak wit te wassen.

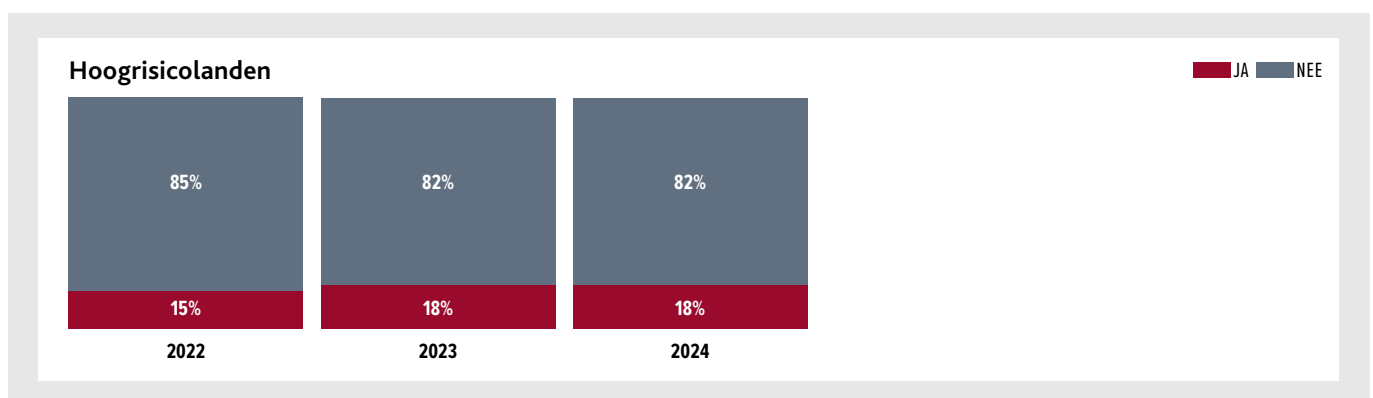
Sanctiewet

Het naleven van sanctiewetgeving is voor bedrijven van groot belang, ten eerste om te zorgen dat een organisatie niet (onbedoeld) betrokken raakt bij leveringen van gesanctioneerde goederen of *dual use*-goederen of bij leveringen aan gesanctioneerde partijen. Hierdoor worden juridische risico's beperkt en kan reputatieschade worden voorkomen. Om die reden hebben wij vorig jaar voor het eerst navraag gedaan of sanctiewetgeving van toepassing is en zo ja, of daarvoor actief een beleid wordt gevolgd. De antwoorden van dit jaar zijn vrijwel gelijk aan die van vorig jaar:



De internationale en nationale regels rondom sancties veranderen regelmatig en vragen om een proactieve houding van organisaties. Mede door de complexiteit van handelsrelaties, uiteenlopende regelgeving per land en de noodzaak tot strikte klant- en transactiecontroles, is het voor bedrijven vaak een hele uitdaging om volledig compliant te blijven. Het risico op onbewuste overtredingen is reëel, zeker wanneer interne kennis of systemen niet up-to-date zijn. Daarom is het essentieel om te investeren in actuele kennis, duidelijke processen en regelmatige controles, zodat bedrijven niet alleen aan de letter maar ook aan de geest van de sanctiewetgeving voldoen.

Dit is vooral van belang voor bedrijven die zaken doen met zogeheten *hoogrisicolanden*. Dat zijn landen die bijvoorbeeld laag scoren op de Corruption Perception Index, en veelal gaat het dan ook om landen waarop sancties van toepassing zijn.



Het aantal respondenten dat aangeeft zaken te doen met hoogrisicolanden stijgt gestaag: van ruim 15% over 2022 tot ruim 18% over 2024. Dat kan aan de ene kant zorgwekkend worden genoemd, maar wij hopen dat bedrijven hierbij een hogere mate van bewustwording laten zien. Bijna de helft van de respondenten geeft in ieder geval aan dat zij zich bewust zijn dat ook sanctiewetgeving van toepassing is, terwijl het overall percentage op 22,5% ligt, zoals hiervoor al bleek.

Wanneer we nader kijken naar het -door private organisaties- zakendoen met hoogrisicolanden geven organisaties daarbij het volgende aan in de uitvraag:

- ▶ 58% van die organisaties maakt hierbij gebruik van één of meer tussenpersonen;
- ▶ daarvan:
 - heeft ruim de helft (56%) een formeel beleid opgesteld voor het zakendoen via tussenpersonen;
 - heeft 41% goed onderzoek (due diligence) gedaan naar de tussenpersoon;
 - weet slechts 43% wie de UBO is van de tussenpersoon;
 - is in 40% van de gevallen een anticorruptieclausule opgenomen in het contract met de tussenpersoon;
 - heeft 32% een right to audit opgenomen in het contract met de tussenpersoon;
 - geeft 27% aan dat de te leveren prestatie en vergoeding niet klip en klaar is verwoord in het contract.

De inzet van agenten of tussenpersonen bij het zakendoen met hoogrisicolanden is vaak onvermijdelijk, maar kan ook risico's meebrengen. Enerzijds kunnen deze tussenpersonen waardevolle lokale kennis en netwerken bieden, waardoor toegang tot complexe en soms onbekende markten wordt vergemakkelijkt. De inzet van een (lokaal) handelsagent of -vertegenwoordiger is ook niet verboden. Anderzijds vergroot het gebruik van agenten de kans op ondoorzichtigheid en mogelijke betrokkenheid bij corruptieve praktijken. Het is dan ook cruciaal dat bedrijven niet alleen formeel beleid opstellen, maar dit ook daadwerkelijk naleven door vooraf onderzoek uit te voeren en duidelijke contractuele afspraken te maken, inclusief het opnemen van anticorruptieclausules en een right to audit. Ook het periodiek, transparant verantwoording afleggen door de agent aan de opdrachtgever is van belang zodat duidelijk is welke activiteiten de agent uitvoert en wat hiervoor een passende vergoeding is. Op die manier kunnen organisaties grip houden op de integriteit van hun internationale handelsrelaties.

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.mateijssen@bdo.nl

T 06 - 31 67 05 09

MEER INFORMATIE

Wil je meer weten over
BDO Forensics & Technology?
[Kijk dan op onze website.](#)

Deze publicatie is zorgvuldig voorbereid en tot stand gekomen, maar is in algemene bewoordingen gesteld en bevat alleen informatie van algemene aard. Deze publicatie bevat geen advies voor concrete situaties, zodat uitdrukkelijk wordt afgeraden om zonder advies van een deskundige op basis van de informatie in deze publicatie te handelen, na te laten of besluiten te nemen. Voor het verkrijgen van een advies dat is toegesneden op uw concrete situatie, kunt u zich wenden tot BDO Accountants & Adviseurs of een van haar adviseurs. BDO Accountants & Adviseurs, de met haar gelieerde partijen en haar adviseurs aanvaarden geen aansprakelijkheid voor schade die het gevolg is van handelen, nalaten of het nemen van besluiten op basis van de informatie in deze publicatie.

BDO is een op naam van Stichting BDO te Amsterdam geregistreerd merk.

In deze publicatie wordt **BDO** gebruikt ter aanduiding van de organisatie die onder de merknaam 'BDO' actief is op het gebied van de professionele dienstverlening (accountancy, belastingadvies en advisory).

BDO Accountants & Adviseurs is een op naam van BDO Holding B.V. te Eindhoven geregistreerde handelsnaam en wordt gebruikt ter aanduiding van een aantal met elkaar in een groep verbonden rechtspersonen, die ieder afzonderlijk onder de merknaam 'BDO' actief zijn op een bepaald terrein van de professionele dienstverlening (accountancy, belastingadvies en advisory).

BDO Holding B.V. is lid van BDO International Ltd, een rechtspersoon naar Engels recht met beperkte aansprakelijkheid, en maakt deel uit van het wereldwijde netwerk van juridisch zelfstandige organisaties die onder de naam 'BDO' optreden.

BDO is de merknaam die wordt gebruikt ter aanduiding van het BDO-netwerk en van elk van de BDO Member Firms.

www.bdo.nl