ONDERZOEK

Bewustwording rond frauderisico's neemt toe, nu de andere non-compliancerisico's nog

Analyse non-compliancerisico's in 2023

Inhoud

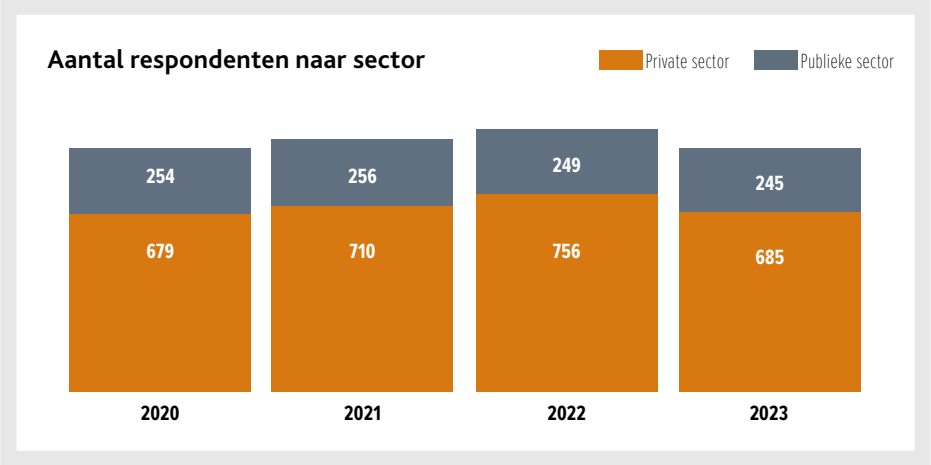
Over het onderzoek

Met regelmaat berichten media over fraude-, corruptie- en witwaszaken. Of het nu gaat om geschonden vertrouwen, brutaal bedrog of een geraffineerde methode met meerdere betrokkenen: de verhalen van individuen en bedrijven die zich verrijken ten koste van werkgevers, klanten, afnemers of overheid leiden nagenoeg altijd tot maatschappelijke verontwaardiging. Niet zelden worden ook de bestuurders, toezichthouders en externe accountants onder wiens oog dit kon gebeuren hierop aangesproken. Ondanks dat alles staat het onderwerp fraude in veel organisaties niet hoog op de agenda. Kenmerken die in de gepubliceerde zaken als 'red flags' worden aangemerkt komen echter in veel organisaties voor.

BDO Forensics & Technology voert jaarlijks, in samenwerking met BDO Audit & Assurance, onderzoek uit om de bewustwording met betrekking tot fraude-, corruptie- en non-compliancerisico's[1] te peilen. Het onderzoek is gebaseerd op een uitgebreide enquête onder organisaties in de private en publieke sector. De resultaten bieden inzicht in de ontwikkelingen op het gebied van bewustwording, beleidsvorming en risico-inschatting van honderden organisaties in uiteenlopende sectoren. Hiermee kunnen organisaties en accountants bepalen welke stappen nog ondernomen moeten worden om de betreffende risico's effectief te bestrijden.

Sectoren

De respondenten zijn verdeeld over diverse sectoren, waarbij woningcorporaties, zorginstellingen, lagere overheden en maatschappelijke organisaties gezamenlijk worden aangeduid als publieke sector. De private sector is nader verdeeld in financiële dienstverlening, food & flowers, techniek, media & telecommunicatie (tech), bouw & vastgoed en een grote groep 'overige'.



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

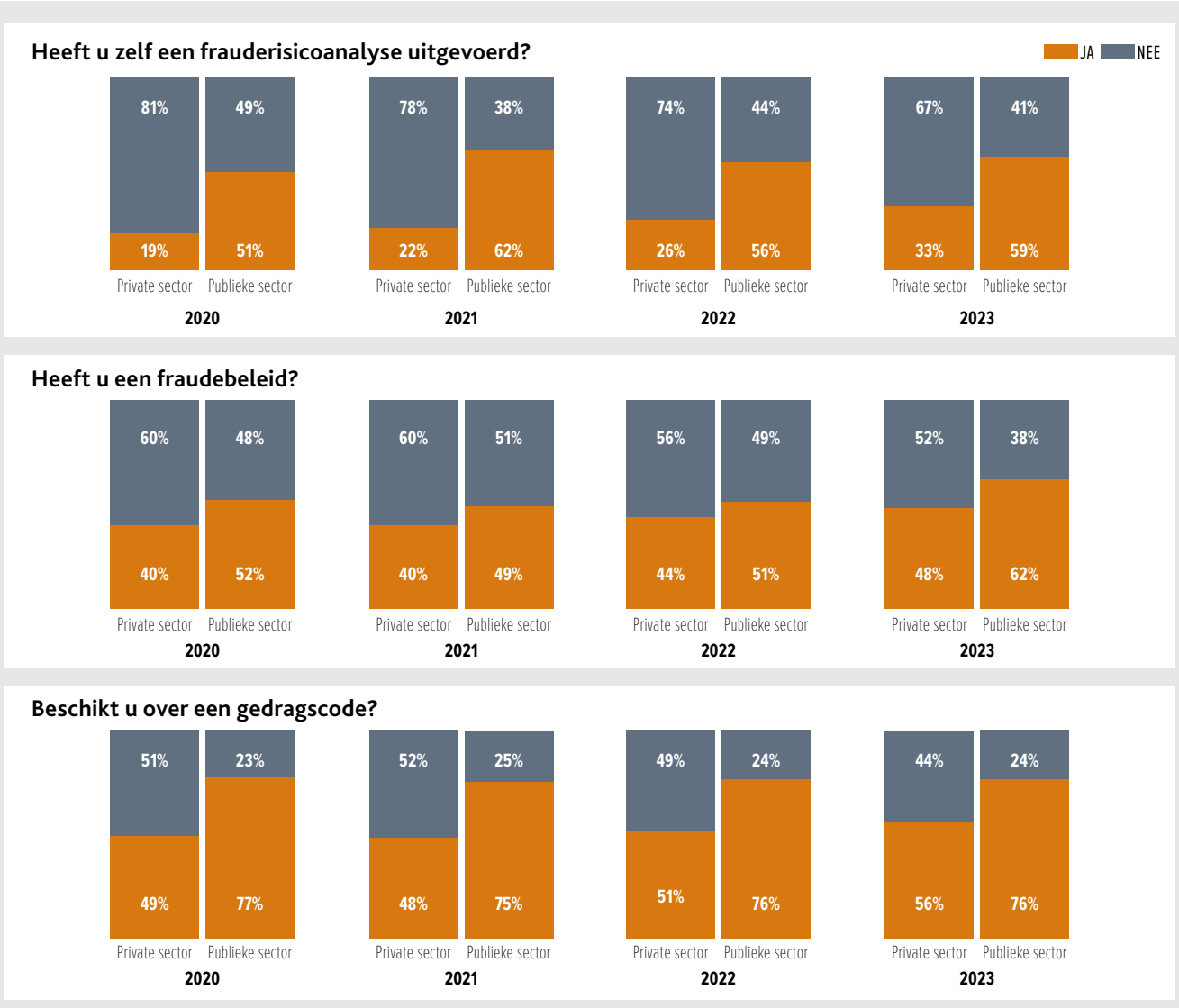
Mondjesmaat meer aandacht voor fraudebeleid

Private sector bezig aan een voorzichtige inhaalslag

Het begint met bewustwording

Fraude, corruptie of non-compliance zijn voor de meeste organisaties gelukkig niet dagelijks aan de orde. Dit kan er voor zorgen dat deze onderwerpen weinig prioriteit krijgen bij het inrichten van bedrijfsprocessen en richtlijnen. Ten onrechte. Uit internationale schattingen blijkt dat de jaarlijkse schade door fraude voor organisaties oploopt tot 5% van de omzet[2]. Hoe voorkomt u dat uw organisatie geraakt wordt door of zelfs medeplichtig wordt aan fraude? En hoe zorgt u dat de maatregelen hiervoor niet onnodig beslag leggen op de beschikbare tijd en middelen. Een gedegen frauderisicoanalyse en -beleid zijn hiervoor onmisbaar

Via een frauderisicoanalyse inventariseert u wat er allemaal mis kan gaan in uw organisatie. Dit stelt u in staat om vooral die maatregelen te treffen die het meest effectief zijn, in tegenstelling tot een '*one size fits all*'-benadering. Een frauderisicobeleid is breder en bevat de belangrijkste uitgangspunten over eerlijk zakendoen. Het geeft de kaders weer van integer handelen in en door een organisatie en spreekt werknemers en (zaken)partners als het ware direct aan. In ons onderzoek vroegen wij onze respondenten of zij beschikten over een frauderisicoanalyse, fraudebeleid, gedragscode en beleidslijnen omtrent witwassen en sanctiebepalingen. Tussen de publieke en private sector bestaan verschillen in ontwikkeling hiervan, zo blijkt uit onderstaande grafiek.



2 *Bron: Occupational Fraud 2024: A Report to the Nations - Association of Certified Fraud Examiners, Inc. (2024)*

Steeds vaker een vastgelegd fraudebeleid in de private sector

In voorgaande jaren constateerden we in ons onderzoek dat organisaties in de publieke sector over het algemeen vaker een fraudebeleid en gedragscode hebben dan organisaties in de private sector. Het werken met publiek geld en de verantwoording die daarover moet worden afgelegd, kan hiervoor een reden zijn. Ook kan een oorzaak zijn dat deze organisaties vaker aan (intern) toezicht zijn onderworpen, waardoor fraudepreventie nadrukkelijker op de agenda staat. Publieke organisaties hebben immers (al dan niet wettelijk verplicht) vaker een toezichthoudend orgaan.

Uit ons onderzoek blijkt dat er in de publieke sector in 2023 een toename van 10% is op de aanwezigheid van een fraudebeleid, ten opzichte van het jaar 2022. De aanwezigheid van een frauderisicoanalyse en gedragscode blijkt ten opzichte van 2022 min of meer op een gelijk niveau. In de private sector is over de afgelopen jaren een gestage toename zichtbaar in de aanwezigheid van alle drie de genoemde beleidsstukken. Dit wijst erop dat ook in de private sector de bewustwording op dit onderwerp geleidelijk toeneemt. De doelstelling van de accountancysector om fraude en corruptie onder de aandacht te brengen in de bestuurskamers lijkt daarmee op de goede weg. We zien bovenstaande resultaten als een positieve ontwikkeling, die in de komende jaren navolging verdient bij organisaties die nog niet over dergelijke beleidsstukken beschikken.

Weinig risicobewustzijn in cyberdomein

Meer dan de helft van de organisaties acht zich niet kwetsbaar

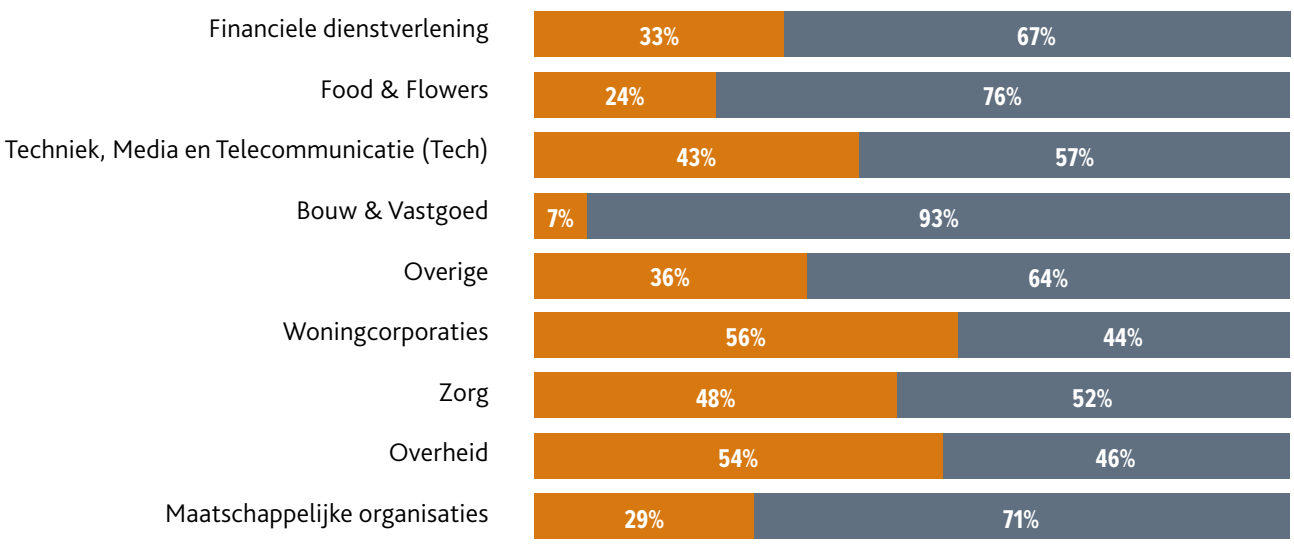
Cyberaanval: die zag u niet aankomen?

Dat kwaadwillenden in toenemende mate voor de digitale route kiezen is geen geheim. Cyberincidenten zijn niet alleen een gevaar voor de (nationale) overheid, maar komen voor bij elk type organisatie. Bijvoorbeeld in de vorm van phishing of ransomwareaanvallen waarbij geprobeerd wordt in te breken en/of gegevens te versleutelen. Of bij zogeheten CEO-fraude, waarbij derden zich – al dan niet met behulp van AI[3] – voordoen als een bestuurder of hogere manager van een bedrijf en zo betaalmiddelen loskrijgen. Sowieso zorgen de ontwikkelingen rond AI voor een toename van fraude.

Met deze ontwikkelingen in het achterhoofd voegden wij twee specifieke vragen toe aan ons onderzoek, namelijk:

1. Bent u van mening dat uw organisatie kwetsbaar is voor cyberaanvallen door kwaadwillenden?
2. Hoe afhankelijk is uw organisatie van digitale gegevensverwerking, zodanig dat de ontoegankelijkheid van ICT kan leiden tot bedrijfsdiscontinuïteit?

Is uw organisatie kwetsbaar voor cyberaanvallen?



Sectoren zoals BDO deze onderscheidt

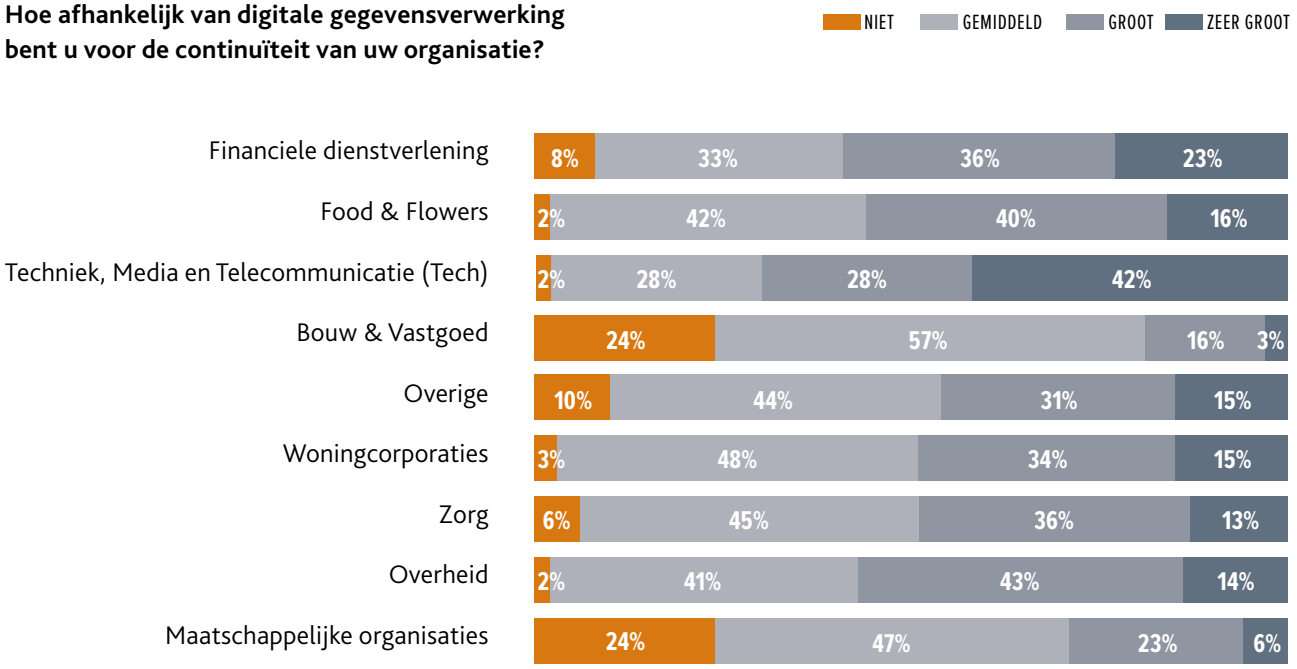
Gemiddeld genomen vindt 49% van de publieke sectororganisaties zich kwetsbaar voor cyberaanvallen, tegenover 33% van de private sector als geheel. Er zijn relatief grote verschillen in de onderliggende sectoren. De sectoren die zichzelf het meest kwetsbaar achten zijn de sectoren waar over het algemeen grote hoeveelheden persoonsgegevens worden verwerkt, zoals overheid, zorg en woningcorporaties. Uit onderzoek van de Autoriteit Persoonsgegevens[4] blijkt dat de meeste cyber-aanvallen ook daadwerkelijk voorkomen in die sectoren. Het is daarom in alle, maar vooral in díe sectoren, van belang dat passende maatregelen worden genomen om de risico's op cybercrime tegen te gaan.

3 AI = Artificial Intelligence
4 Bron: Rapportage Datalekken 2023 – Autoriteit Persoonsgegevens (2024)

Grote afhankelijkheid van digitale gegevensverwerking

Het beeld dat ontstaat uit de vorige vraag klemt, te meer omdat organisaties steeds afhankelijker worden van digitale gegevensverwerking. Een dag 'plat liggen' kost handenvol geld. Op onze vraag over de afhankelijkheid van digitale gegevensverwerking ontlopen de publieke en private sector elkaar weinig. Voor beide sectoren geldt dat net minder dan de helft (respectievelijk 47% en 49%) hun afhankelijkheid van digitale gegevensverwerking inschat als 'groot' of 'zeer groot'.

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



Sectoren zoals BDO deze onderscheidt

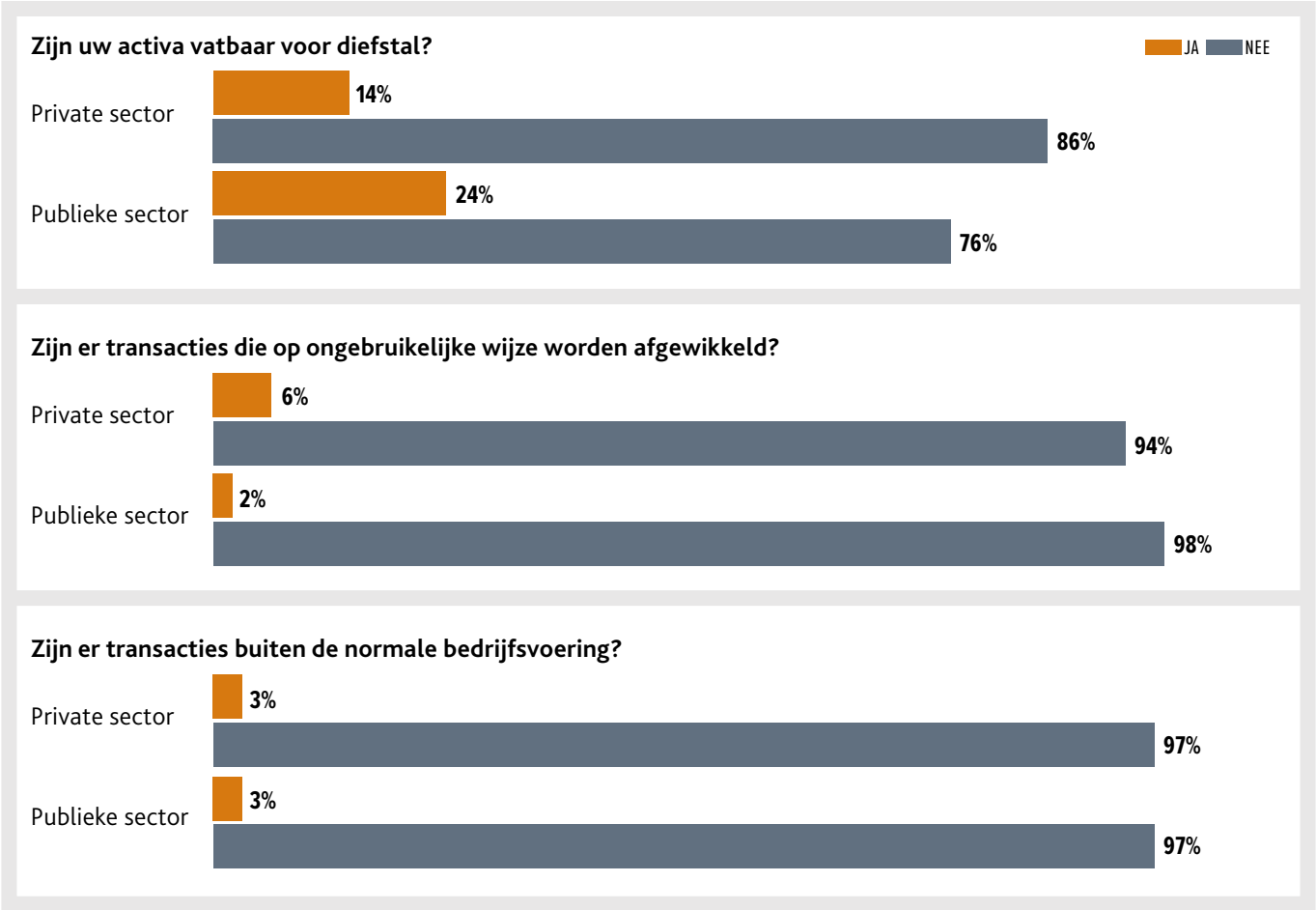
In de publieke sector gaat het aandeel respondenten dat hun afhankelijkheid minimaal 'groot' noemt gelijk op met het aandeel dat zich kwetsbaar acht. In de private sector valt op dat een aanzienlijk deel van de respondenten zich ondanks een grote afhankelijkheid van digitale gegevensverwerking, niet kwetsbaar acht voor cyberaanvallen. Ook in dit domein zijn dus nog verdere stappen noodzakelijk om tot een niveau van bewustwording te komen dat kan leiden tot effectieve maatregelen tegen cyberrisico's.

Oog voor de uitzondering

Rode vlaggen en wetgeving niet overal duidelijk in beeld

Onbekend maakt onbeschermd?

Wij begrijpen dat het lastig is effectieve monitoring toe te passen op onregelmatigheden die zich maar zelden uiten en bovendien veelal worden verhuld. In het eerste hoofdstuk 'Mondjesmaat meer aandacht voor fraudebeleid' wezen wij al op het belang van fraudebeleid en risicoanalyse. Met risicoanalyse kan ook in beeld worden gebracht welke transacties onduidelijk of ongebruikelijk zijn. In ons onderzoek vroegen wij hier ook naar, waarbij tevens werd gevraagd naar de aard van de transacties. De uitkomsten bevestigen onze theorie: ongebruikelijke zaken komen (gelukkig) niet vaak voor, maar als het voorkomt is verhoogde alertheid geboden.



Allereerst valt op dat organisaties in de publieke sector hun activa meer vatbaar achten voor diefstal dan organisaties in de private sector. Op basis van de aard van de sectoren ligt dit niet direct in de lijn der verwachting, omdat de publieke sector vaak vooral een dienstverlenend karakter heeft en activa (dan) een meer ondersteunende rol spelen. Aan de andere kant is de private sector zich mogelijk bewuster van risico's op diefstal en zijn er al meer maatregelen genomen.

Er worden door de respondenten weinig transacties als 'ongebruikelijk' of 'buiten de normale bedrijfsvoering' aangeduid. Toch is het percentage organisaties in de private sector die aangeven met 'ongebruikelijke transacties' te maken te hebben (bijna 6%) opvallend. Uit de toelichting blijkt dat het vooral gaat om zogeheten 'derdenbetalingen': betalingen aan, of ontvangsten van een andere partij dan de directe handelspartner. Voorkomende verklaringen zijn:

- Er wordt geleverd aan, of ontvangen van, een lokale vestiging terwijl de financiële transactie wordt afgewikkeld met het internationale hoofdkantoor;
- Er zijn landen betrokken waarop sancties van toepassing zijn of waarvan het banksysteem, volgens de betreffende respondent, niet goed functioneert.

Daarnaast signaleren wij in praktijksituaties dat er wordt betaald aan of door een derde, die an sich niets met de transactie te maken heeft.

In diverse gevallen geven respondenten ook aan deze transacties in overleg met hun bank te evalueren. Dat is ook sterk aan te bevelen, aangezien banken in hun rol als poortwachter in het financiële systeem goed kunnen beoordelen of er sprake is van witwasrisico's. Zo kan worden voorkomen dat organisaties onbewust meewerken aan het witwassen van criminele gelden, wat vooral bij betalingen door een derde een risico kan zijn. Ons advies is dan ook dat organisaties altijd verifiëren of ontvangen of betaalde gelden naar een bekend, geverifieerd, bankrekeningnummer gaan.

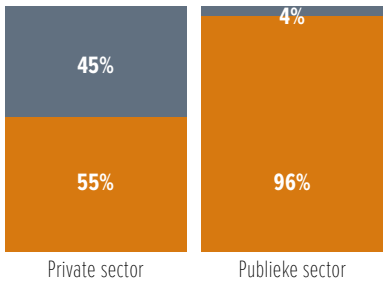
Als de klokkenluider niet weet waar de klepel hangt

Voor sommige aspecten van fraude en corruptie zijn de effecten dermate groot dat in wetgeving is vastgelegd hoe organisaties in Nederland daarmee moeten omgaan. Wij stelden in ons onderzoek daarom onder andere vragen over klokkenluiders- en sanctiewetgeving. Dat leidde tot enkele opvallende resultaten.

Een klokkenluidersregeling is een effectief middel om fraude tijdig te detecteren. Bekend is dat ruim 50% van de fraudes wordt ontdekt door een tip van een medewerker en nog eens ruim 30% door tips van klanten of leveranciers[5]. Klokkenluiders dus, die daarmee veruit de belangrijkste bron van fraudedetectie zijn en een organisatie dus veel geld kunnen besparen. Veel organisaties in de private sector lijken daar echter nog niet van doordrongen.

In de publieke sector heeft een overgrote meerderheid (ruim 95%) van de organisaties een klokkenluidersregeling. In de private sector is dat slechts 55% van de organisaties. Een dergelijke regeling is op basis van de Wet bescherming klokkenluiders verplicht voor bedrijven vanaf 50 medewerkers. Van de organisaties zonder klokkenluidersregeling geeft 41% aan dat zij qua werknemersaantal in die categorie vallen en dus niet aan de wet voldoen.

Heeft u een klokkenluidersregeling?



41%

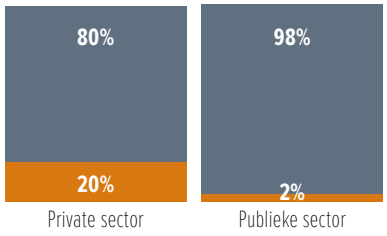
van de bedrijven met meer dan 50 medewerkers heeft **geen** klokkenluidersregeling. Vanaf dit aantal is een interne meldprocedure verplicht op basis van de Wet bescherming klokkenluiders.

5 *Bron: Occupational Fraud 2024: A Report to the Nations - Association of Certified Fraud Examiners, Inc. (2024)*

De Sanctiewet geldt voor iedereen, maar (bijna) niemand weet het

Daarnaast is, zeker sinds de oorlog in Oekraïne, sanctiewetgeving de afgelopen jaren prominenter in het nieuws geweest. Toch zijn er maar weinig organisaties die aangeven dat de wetgeving hieromtrent van toepassing is op hun sector, producten of diensten. Sanctiewetgeving staat nog het meest op het netvlies in de private sector en dan voornamelijk in de financiële dienstverlening:

Is sanctiewetgeving van toepassing?



46%

van de bedrijven die aangeeft dat sanctiewetgeving van toepassing is, geeft ook aan geen beleid daarop te hebben.

Toch geeft slechts 49% van de respondenten uit de sector financiële dienstverlening aan dat deze wetgeving voor hen relevant is. Van alle bedrijven die de sanctiewetgeving wel relevant achten, geeft slechts 54% aan dat zij ook beleid hebben wat gericht is op het voldoen aan die wetgeving. Er is dus nog werk aan de winkel. Sanctieregelgeving is complex en verandert ook regelmatig doordat er weer nieuwe (sanctie)pakketten van toepassing worden. Zowel voor organisaties die zich realiseren dat sanctiewetgeving van toepassing is als organisaties die aangeven dat dat niet het geval is, is het daarom van belang zich hierover periodiek te laten informeren en alert te zijn. Een overtreding is zo gemaakt en met alle gevolgen van dien. Uiteindelijk geldt de sanctiewet immers voor iedereen.

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 06 - 31 67 05 09

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

www.bdo.nl

10/2024 – BM2448

Een andere kijk op waarde