Uw frauderisico-programma

pwc

Uw frauderisicoprogramma

Fraude is een veelvoorkomend probleem. Stakeholders besteden daarom meer en meer aandacht aan dit onderwerp. Het is belangrijk dat organisaties zich wapenen tegen fraude. Voor het voorkomen en/of detecteren van fraude bestaat helaas geen one-size-fits-all oplossing; het risico op fraude wordt bijvoorbeeld beïnvloed door de sector waarin de organisatie actief is maar ook door de organisatiecultuur en de van toepassing zijnde wet- en regelgeving. Een van de hulpmiddelen die een organisatie kan gebruiken om meer inzicht te verkrijgen in mogelijke frauderisico's is het COSO-raamwerk dat is opgesteld door COSO en ACFE en is vastgelegd in de 'Fraud Risk Management Guide' (hierna: COSO-raamwerk). Dit is een handig hulpmiddel voor de bestuurders en met governance belaste personen om het frauderisicoprogramma te ontwerpen en te blijven toetsen. De forensische afdeling van PwC kan u helpen dit programma vorm te geven.

1. Waarom een frauderisicoprogramma?

Veel organisaties hebben helaas te maken met fraude, of hebben hier in het verleden mee te maken gehad. Het spreekt voor zich dat organisaties niets liever willen dan fraude voorkomen, maar door de veranderende wereld worden zij steeds geconfronteerd met nieuwe frauderisico's. De wereldwijde pandemie is een voorbeeld van zo'n verandering. Veel organisaties zijn onder financiële druk komen te staan door het wegvallen van omzet, terwijl andere organisaties in korte tijd hard zijn gegroeid. In sommige gevallen zelfs zo hard dat naast een toename van de omzet ook een sterke toename van het aantal werknemers nodig is. Het is belangrijk om te leren omgaan met de frauderisico's die zulke veranderingen met zich meebrengen. Daarnaast moeten organisaties beoordelen hoe zij kunnen voldoen aan de eisen met betrekking tot de jaarrekening. Maar waar begin je?

Organisaties hebben net als accountants een belangrijke maatschappelijke rol bij de preventie en bestrijding van fraude. Financieel-economische criminaliteit is een maatschappelijk probleem dat burgers en organisaties financieel kan benadelen. Het is daarom belangrijk om als organisatie goed in kaart te brengen welke risico's bestaan en vervolgens te beoordelen of deze risico's voldoende gemitigeerd worden met de bestaande beheersingsmaatregelen of dat daar juist wijzigingen in moeten worden aangebracht.

2. Raamwerk voor frauderisicoprogramma

Organisaties ervaren het zetten van de eerste stap op weg naar het in kaart brengen van frauderisico's als lastig. Om op een gestructureerde wijze inzichtelijk te maken waar in de organisatie de mogelijke leemtes of frauderisico's zich bevinden, kan gebruik worden gemaakt van de vijf onderdelen van het COSO-raamwerk, weergegeven in het overzicht hieronder.

	Onderdeel	Frauderisicomanagement principe	Aandachtspunten en voorbeelden
	Controleomgeving	De organisatie ontwikkelt en communiceert een frauderisicomanagement-programma dat de verwachtingen van de bestuurders en toezichthouders laat zien, net als haar toewijding op het gebied van integriteit en ethiek met betrekking tot het frauderisico.	• Tone at the top via nieuwsbrieven, blogs etc. • Gedragscode voor zowel medewerkers als business partners. • Gedragscodes jaarlijks laten confirmeren. • Communiceren over opvolging van (vermoedens) van fraude. • In beeld brengen welke wet- en regelgeving van toepassing is op het gebied van fraude (bijvoorbeeld UK Bribery Act en de Wwft).

	Onderdeel	Frauderisicomanagement principe	Aandachtspunten en voorbeelden
	Risicobeoordeling	De organisatie voert een alomvattende frauderisicobeoordeling uit om specifieke frauderisico's of -schema's te identificeren, weegt de kans en impact af, evalueert bestaande beheersingsactiviteiten en neemt actie om resterende frauderisico's af te dekken.	• Jaarlijkse update van de geïdentificeerde risico's. • Neem ook externe risico's mee in de risicobeoordeling. • Betrek de gehele organisatie bij het identificeren van frauderisico's • Neem bekende fraudezaken uit de eigen organisatie en uit uw branche mee. • Schenk aandacht aan mogelijke frauderisico's bij activiteiten buiten de reguliere processen. • Veelvoorkomende onderwerpen zijn: steekpenningen, omkoping, declaraties, cybercrime, doorbreking van functiescheiding, personeelsleden met schuld, greenwashing.
	Beheersings-activiteiten	De organisatie selecteert, ontwikkelt en voert preventieve en detectieve controlemaatregelen uit om het risico dat fraude niet (tijdig) wordt ontdekt te mitigeren.	• Screening van werknemers, leveranciers of klanten. • Dagelijkse aansluiting van bankafschriften. • Fraudetrainingen. • Functiescheiding. Gebruik van data-analyse: • Continuousmonitoringsoftware die direct een waarschuwing afgeeft zodra bepaalde foutieve handelingen zijn verricht. • Internetonderzoek naar de frauderisico's in het land waar een nieuwe vestiging wordt geopend. • Businessintelligencesoftware om benchmarkanalyses tussen vestigingen uit te voeren. • Process mining voor het in beeld brengen van de standaard transacties en om het mogelijk te maken om te focussen op de uitzonderingen.
	Informatie en communicatie	De organisatie ontwikkelt een communicatieproces om informatie over indicatie(s) van fraude te ontvangen en voert een gecoördineerde aanpak uit ten aanzien van het onderzoeken van vermoedens van fraude, alsook om passende corrigerende acties tijdig uit te voeren.	• Stel een klokkenluidersregeling in. • Stel een informatieprotocol op in het geval van fraude; wie moet wanneer geïnformeerd worden? • Maak gebruik van anonieme vragenlijsten. • Stel een protocol op voor het uitvoeren van fraudeonderzoeken: wie is daarvoor verantwoordelijk en hoe geschiedt dit (intern/extern)?

	Onderdeel	Frauderisicomanagement principe	Aandachtspunten en voorbeelden
	Bewaking	De organisatie selecteert, ontwikkelt en evalueert voortdurend om te toetsen of alle vijf de punten uit het raamwerk aanwezig zijn en werken, en communiceert tekortkomingen op een tijdige wijze naar partijen die verantwoordelijk zijn voor het opvolgen van die tekortkomingen, alsook naar bestuurders en toezichthouders.	• Monitor relevante fraude-metrics, zoals bijvoorbeeld het aantal klokkenluidersmeldingen • Bespreek het raamwerk periodiek en breid het uit of kort het in waar nodig. • Bespreek niet alleen de opzet van het raamwerk, maar ook de werking daarvan (bijvoorbeeld effectiviteit van de beheersingsactiviteiten). • Neem hierin ook de cultuur van de organisatie mee. • Vraag de accountant om zijn visie op het raamwerk.

3. Frauderisicobeoordeling:

Door een frauderisicobeoordeling op te stellen kunt u risico's in de bedrijfsvoering en zwakke punten in de interne beheersing die een frauderisico voor de organisatie inhouden, per proces identificeren en begrijpen. Voor de geïdentificeerde risico's kan een plan worden ontwikkeld om ze te beperken. De frauderisicobeoordeling betreft het tweede en derde component van het COSO-model (risicobeoordeling en beheersingsactiviteiten).

De frauderisicobeoordeling bestaat uit de volgende vier stappen:

1. Voor de relevante processen in uw organisatie worden de 'rode vlaggen' c.q. de mogelijke fraudescenario's in kaart gebracht. Hierbij gaat het om de vraag: Welke fraudes kunnen er worden gepleegd en hoe kunnen die plaatsvinden?
2. Per scenario wordt de kans bepaald dat de fraude zich voordoet evenals de impact die de fraude heeft als deze zich voordoet; op deze wijze heeft u een indruk van de bruto frauderisico's in uw organisatie.
3. Per scenario wordt vastgesteld of het risico wordt afgedekt door maatregelen van interne beheersing. Het resultaat hiervan bestaat uit de (resterende) netto frauderisico's.
4. Indien er sprake is van netto frauderisico's die u niet gewenst acht c.q. die niet in uw '**risk appetite**' vallen weet u waar u aanvullende beheersmaatregelen moet implementeren.

Het is raadzaam om bij het opstellen van een frauderisico beoordeling rekening te houden met de volgende aandachtspunten:

- Betrek de gehele organisatie bij het identificeren van frauderisico's. Hoe completer het risicoregister, hoe beter de organisatie heeft kunnen nadenken over welk risico acceptabel is en welk niet. Beheersingsactiviteiten kunnen pas worden ontworpen wanneer de risico's bekend zijn. Maar hoe zorgt een organisatie ervoor dat het risicoregister zo volledig mogelijk is? Dit vraagt om creativiteit en kennis van de organisatie. Daarom is het belangrijk de risicobeoordeling uit te voeren met een brede groep aan disciplines binnen de organisatie (bijvoorbeeld de afdelingen inkoop, verkoop en de directie).
- Hanteer de fraudedriehoek (Gelegenheid, druk en rationalisatie) bij het identificeren van frauderisico's en neem hiaten in de interne beheersingsmaatregelen, zoals gerapporteerd door de interne- of externe accountant mee in de frauderisico-analyse.
- Leer van fraudegevallen uit het verleden. Fraudegevallen die geconstateerd zijn in de branche zijn aanwijzingen dat het risico ook op de eigen organisatie van toepassing is.
- Bekijk risico's altijd als inherente risico's: het risico zonder rekening te houden met beheersingsmaatregelen.
- Bekijk risico's vanuit verschillende perspectieven: wat zijn de risico's met betrekking tot veiligheid, commercie, fraude en/of cyber.
- Kijk naar de impact van ontwikkelingen op de risicobeoordeling: corona leidt tot meer thuiswerken en daarom nemen wellicht cyberrisico's toe.
- Er zijn veel onderzoeken beschikbaar die kijken naar frauderisico's van een specifieke branche. Die kunnen gebruikt worden als inspiratie.

De uitkomst van een frauderisicobeoordeling kan worden gedocumenteerd in een risicoregister, een dergelijk risicoregister kan er als volgt uitzien:

Risico	Verschijningsvorm (hoe het risico zich kan manifesteren)	Proces	Impact	Kans	Risico	Reeds aanwezige beheersings-maatregelen	Dekt risico af	Resterend netto risico	Aanvullende maatregel
Frauduleuze betalingen	Medewerker verandert IBAN-crediteur in betaalbatch in eigen IBAN	Inkoop en betalingen	1	10	10	Autorisatie van betaalrun door CEO, zonder IBAN-controle	Deels	6	4 ogenprincipe op IBAN-wijzigingen
	Medewerker verstuurt nepfacturen		4	3	12	..	Geheel	1	n.v.t.
	Medewerker verhoogt bestaande facturen		Inkoop en betalingen	..	..	..	..	..	..
	..		..	..	..	..	..	..	..

4. Hoe kunnen wij u helpen?

Wij gaan graag met u in gesprek over hoe u fraude binnen uw organisatie voorkomt en tijdig detecteert. Hieronder treft u enkele voorbeelden van ondersteuning die wij u kunnen bieden:

4.1. Quickscan van uw frauderisicoprogramma

Het doel van de quickscan is om inzichtelijk te maken welke elementen al aanwezig zijn in een eventueel frauderisicoprogramma en welke factoren aandacht behoeven.

Aanpak:

Voor het uitvoeren van deze quickscan maken wij gebruik van het hiervoor beschreven COSO-raamwerk voor fraudebeheersing. Per component van het COSO-raamwerk brengen wij voor u in kaart welke elementen reeds geïmplementeerd zijn door uw organisatie en welke elementen missen. Hierbij zullen wij uiteraard rekening houden met wat verwacht mag worden van uw organisatie gelet op de omvang van de organisatie en uw sector. De quickscan wordt uitgevoerd doormiddel van het houden van interviews en door het opvragen en analyseren van relevante documenten (bijvoorbeeld de integriteitscode en klokkenluidersregeling van uw organisatie).

Output:

De uitkomst van de quickscan wordt gerapporteerd in een rapportage waarbij per COSO-component terugkoppeling wordt gegeven over geïmplementeerde maatregelen en mogelijke verbeterpunten.

4.2. Ondersteuning bij het opstellen van de frauderisicobeoordeling

Wij kunnen u ondersteunen bij het opstellen van de frauderisicobeoordeling, een mogelijke aanpak die hierbij gehanteerd kan worden is als volgt:

- Wij bieden u een format aan dat u kunt gebruiken voor het opstellen van de frauderisicobeoordeling.
- Wij evalueren aan ons ter beschikking gestelde procesbeschrijvingen en andere relevante informatie.
- Samen met uw medewerker die verantwoordelijk is voor het opstellen van de frauderisicobeoordeling, interviewen wij relevante proceseigenaren om inzicht te vergaren in mogelijke frauderisico's en in reeds geïmplementeerde beheersingsmaatregelen. Uw medewerker stelt op basis van de verkregen informatie en met onze hulp de frauderisicobeoordeling op.
- Wij evalueren de opgestelde analyse en koppelen onze observaties aan u terug, in een gesprek.

Output:

Voor deze vorm van ondersteuning bieden wij u een format dat u kan gebruiken voor de frauderisicobeoordeling en voorzien wij u tijdens het proces van input om tot een goede frauderisicobeoordeling te komen.

4.3. Workshop fraudebewustwording

Een andere manier waarop wij u kunnen ondersteunen is het geven van een workshop fraudebewustwording. De doelstelling van deze workshop is om de deelnemers meer bewust te maken van frauderisico's. Dit doen wij door de deelnemers mee te nemen in de theorie rondom fraude, recente ontwikkelingen en vooral door het delen van veel voorbeelden uit onze eigen praktijk. Ook dagen wij de deelnemers uit om zelf eens in de schoenen van een fraudeur te gaan staan en de 'perfecte fraude' te verzinnen. Uiteraard met als doelstelling om daarbij passende beheersmaatregelen te bedenken. Tenslotte bespreken wij verschillende dillema's en stellingen met betrekking tot fraude, cultuur en gedrag binnen de eigen organisatie van de deelnemers.

De workshop fraudebewustwording levert niet alleen medewerkers op die zich bewust zijn van de verschillende manieren waarop uw organisatie slachtoffer kan worden van fraude, maar levert ook input voor het opstellen van een frauderisicobeoordeling.

Uiteraard zullen wij van tevoren met u van gedachten wisselen over uw wensen voor de workshop en de onderwerpen die wij zullen behandelen. De opzet van de workshop is flexibel en wij kunnen deze aanpassen naar uw voorkeuren. Het is uiteraard mogelijk om de workshop digitaal te faciliteren.

Sander Kranenburg
Partner

T: +31 (0)88 792 53 09
E: dander.kranenburg@pwc.com
LinkedIn

Rian Mes
Senior Manager

T: +31 (0)88 792 35 68
E: rian.mes@pwc.com
LinkedIn

pwc.com