

Fraude risico analyse 2022 Diamant-groep

Aanleiding

Najaar 2021 hebben we, ter voorbereiding op de rechtmatigheidsverantwoording, met het bestuur afgesproken inzicht te geven in de eigen inschatting van het risico dat de jaarrekening een materiële afwijking zou kunnen bevatten als gevolg van fraude. Ook is afgesproken dat we de risico analyse jaarlijks gaan actualiseren. De frauderisicoanalyse die voor u ligt bevat een overzicht van de relevante beheersmaatregelen en een overzicht van de processen met de grootste fraude restrisico's waarvoor nog aanvullende maatregelen nodig zijn.

Doel

Nagaan of onze processen fraudeproof zijn en die waar nodig te verbeteren. D.m.v. risico inventarisatie als basis voor de planning-en-control cyclus zorgen voor een duidelijke grondslag voor de rechtmatigheidsverantwoording. Het opstellen van aanvullend integriteitsbeleid / gedragsregels en de medewerkers hiermee bekend maken. Leidinggevend en vragen om dit beleid uit te dragen en alert te zijn op fraude signalen.

Integriteit en fraude

Er zijn tal van definities van integriteit en fraude. Wij zien integriteit als begrip ruimer dan fraude. Integriteit kan beperkt worden uitgelegd als de afwezigheid van fraude en corruptie. Integriteit wordt veelal echter breder uitgelegd en vallen er ook waarden onder zoals collegialiteit, betrouwbaarheid, klantgerichtheid, objectiviteit, fatsoenlijkheid, effectiviteit en efficiëntie. Ook voor fraude zijn er verschillende definities.

Een voorbeeld hiervan is afkomstig uit COS 240: wanneer spreek je van fraude?

- Een opzettelijke handeling
- Door een of meer leden van het management, met governance belaste personen, werknemers of derden
- Ter verkrijging van onrechtmatig of onwettig voordeel
- Ten laste van de Diamant-groep
- Door misbruik te maken van vertrouwen (misleiding, verhullen van feiten)

Rechtmatigheidsverantwoording

Vanaf boekjaar 2022 moet het bestuur een rechtmatigheidsverantwoording opnemen in de jaarrekening.

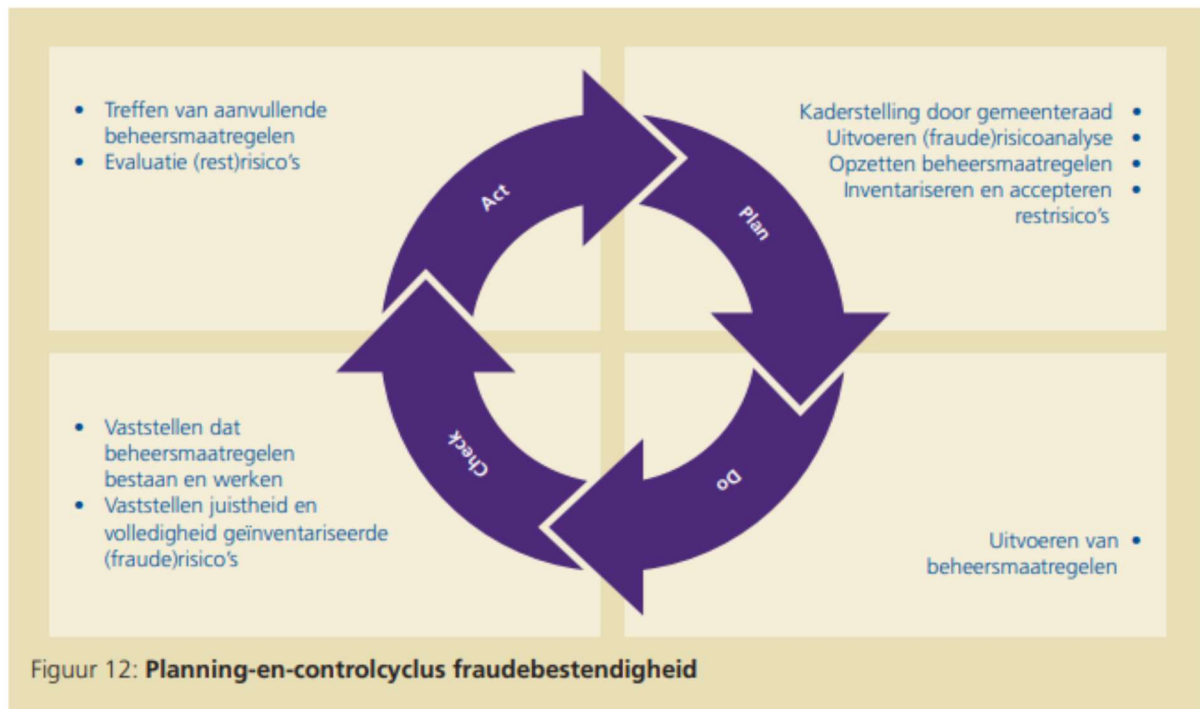
Er zijn 3 rechtmatigheidscriteria:

- Voorwaardencriterium
- Begrotingscriterium
- Misbruik & Oneigenlijk gebruik criterium

In het kader van het Misbruik & Oneigenlijk gebruik criterium dient verantwoording te worden afgelegd over fraudebeheersing. Een belangrijke bouwsteen hiervoor is de frauderisico analyse.

Proces versterking fraudebestendigheid

De volgende figuur toont het proces dat de Diamant-groep vanaf 2022 periodiek zal gaan doorlopen ter versterking van de fraudebestendigheid. Het is gestructureerd volgens de "plan, do, check, act"-cyclus (PDCA).



Het proces start met de uitvoering van een risicoanalyse, waarna beheersmaatregelen in het proces worden vastgesteld. Vervolgens wordt beoordeeld of de getroffen beheersmaatregelen ook in de praktijk zijn ingevoerd en daadwerkelijk functioneren. De laatste stap betreft het rapporteren over risico's, beheersmaatregelen en bevindingen. In het kader van de frauderisicoanalyse is het een belangrijke constatering dat het periodiek analyseren van kwetsbare processen daadwerkelijk plaatsvindt.

Uitgevoerd stappenplan frauderisicoanalyse (zei bijlagen 1 tm 4)

1. Inventarisatie potentiële (bruto) risico's (zie aparte bijlage bruto risico's en risicoschaal)
2. Inventarisatie aanwezige beheersmaatregelen (blz. 4-7 frauderisico's en beheersmaatregelen)
3. Bepalen resterende (netto) frauderisico (zie aparte bijlage netto risico's)
4. Aanbeveling aanvullende maatregelen voor gebieden met een verhoogd restrisico (blz. 8 restrisico's)

Nog uit te voeren stappen Frauderisico analyse

- Voorleggen aan management ter meningsvorming en besluitvorming
- Voorleggen aan accountant ter beoordeling
- Samen met aanvullend integriteitsbeleid voorleggen aan het bestuur ter vaststelling
- Aanvullende maatregelen vaststellen voor gebieden met een verhoogd restrisico
- Diamant-groep breed medewerkers informeren over integriteitsbeleid en trainen in fraude awareness

Fraudegevoeligheid en (functioneren van) beheersmaatregelen

Als het om fraude en frauderen gaat, kunnen we stellen dat de volgende zaken de fraudegevoeligheid van een organisatie beïnvloeden:

1. Gelegenheid: biedt de fraudeur de mogelijkheid om fraude te plegen of zoals het spreekwoord zegt: "gelegenheid maakt de dief".
2. Druk: zorgt ervoor dat de noodzaak voor het plegen van fraude bij de fraudeur tot stand komt. Dit kan bijvoorbeeld ingegeven zijn door financiële problemen bij een potentiële fraudeur.
3. Rationalisatie: zorgt ervoor dat het geweten uitgeschakeld wordt. Mensen die wel druk voelen of gelegenheid hebben te frauderen, doen dit niet, omdat hun geweten hen tegenhoudt. Dit kan echter omslaan indien medewerkers zich bijvoorbeeld achtergesteld of benadeeld voelen. Dan zijn er mogelijke redenen om het plegen van fraude te rechtvaardigen. Ook verkeerd voorbeeldgedrag kan hiertoe leiden.

Deze zaken zijn als leidraad gebruikt bij de verdere uitwerking van de risico analyse per proces. Per proces is aangegeven welke beheersmaatregelen bij de Diamant-groep bestaan waarvan we de werking toetsen en hierover gaan rapporteren.

1. Gelegenheid

In de opzet van de processen zijn de noodzakelijke beheersmaatregelen, waaronder functiescheidingen, opgenomen. Met de inventarisatie van de belangrijkste risico's en daaraan gekoppelde beheersmaatregelen in de materiële processen is dit expliciet inzichtelijk gemaakt. Het lijnmanagement is verantwoordelijk voor de uitvoering van de beheersmaatregelen in het proces. Steekproefsgewijs worden lijncontroles uitgevoerd door medewerkers van bedrijfsvoering/bedrijfsbureaus. De voortgang van de uitvoering van de lijncontroles en van de controles op de werking van de beheersmaatregelen in de processen wordt bewaakt door de afdeling Planning & Control, die ook de voortgang van het verbeterplan voor processen met een verhoogd restrisico bewaakt en rapporteert aan management en bestuur.

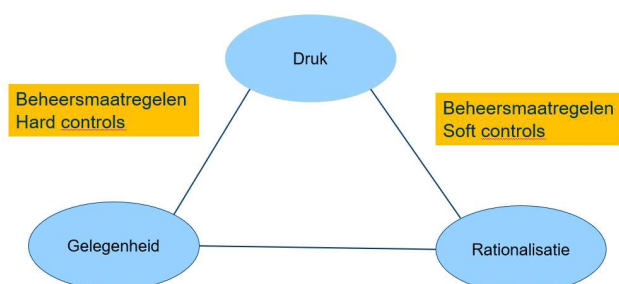
2. Druk

Dit is niet altijd te voorkomen, omdat dit zich ook in de privésfeer van medewerkers afspeelt. Druk kan ook zijn intimidatie of sociale/-groepsdruk van buiten, i.v.m. het externe belang van die groep of persoon. Leidinggevend en dienen alert te zijn op signalen vanuit de werkvloer en de bedrijfsarts en vertrouwenspersoon kunnen ondersteuning bieden aan medewerkers.

3. Rationalisatie

Beleidskaders integriteit zijn niet uitgewerkt, M&O beleid ontbreekt. Er is een klokkenluidersregeling vastgesteld, maar in het jaarverslag van de ombudsvrouw wordt niet ingegaan op integriteit. Er hebben geen Diamant-groep brede trainingen plaatsgevonden. Medewerkers leggen geen ambtseed/-belofte af. Bij introductie van nieuwe medewerkers worden algemene gedragsregels overhandigd, maar wordt er geen expliciete aandacht besteed aan integriteit. Na vaststelling van het beleid zal er een verbeterplan gemaakt worden voor deze softcontrols.

Frauderisicoanalyse Diamant-groep beschrijving risico's met aanwezige beheersmaatregelen



FRAUDERISICO

Gelegenheid (hardcontrols)

Proces	Beheersmaatregel	Risico H/G/L
Cybercrime (diefstal van bedrijfsgegevens, platleggen computernetwerk)	Monitoring netwerken, controle toegangsrechten, wachtwoordbeheer, controle loggings gebruikers, controle loggings beheerders, patch management, uitvoeren pen test, controle back-ups en recovery , cybercrimeverzekering.	H (complex)
Aanbesteding (Borgen van economisch meest voordelige inkoop cf. aanbestedingsregels)	Vanuit management en bedrijfsvoering wordt gestuurd op voortgang en volledigheid aanbestedingskalender. Voorlopige gunningsbeslissing door de algemeen directeur. Ook beneden de grens van Europese aanbesteding werken we met Tendered ivm transparantie naar buiten. Intern leggen we de processtappen transparant vast op inkoopformulieren (bepalen aanbestedingsprocedure, voorlopige gunning) en in proces verbaal van aanbesteding.	L
Inkoop (Borgen dat de inkopen voor jezelf zijn en niet voor een andere partij)	Bezig met optimalisatie inkoopproces : onderscheid maken tussen specifieke stromen van inkopen en hiervan het risicoprofiel bepalen en beheersmaatregelen vast stellen : wanneer bewijs prestatielevering verplicht? Autorisatiematrix in goedkeuren en ontvangstmelden in financieel systeem	M
Wijzigen betaalrekening Personeel (Borgen dat	Controle door personeelsadministratie wordt afgedwongen in de workflow (op basis van	L?

salarisbetalingen op het juiste bankrekeningnummer worden overgemaakt)	foto van bankpas op naam die door werknemer wordt aangeleverd). Mogelijkheid tot mutaties betaalrekeningen buiten de workflow om nog nagaan in nieuwe HRM/salarissysteem, en indien mogelijk hier een aanvullende verbijzonderde controle op zetten.	
Wijzigen betaalrekening crediteuren (Borgen dat crediteurenbetalingen op het juiste bankrekeningnummer worden overgemaakt)	Slechts 2 medewerkers hebben rechten om een bankrekening van een leverancier in te geven/te wijzigen (ook superuser kan dit niet). Deze 2 medewerkers kunnen geen inkoopfactuur opvoeren/goedkeuren en hebben ook geen rechten om facturen te betalen. In het werkproces van het CRM proces is opgenomen dat de gelogde bankrekeningmutaties worden gecontroleerd aan de hand van de brongegevens door iemand anders als deze 2 medewerkers.	L
Treasury	Nota treasurystatuut is gedateerd en voorschriften zijn vaag: update maken en vaststellen toetsingskader bij nemen van financieringsbeslissingen	M
Management override	Boeking kan gemaakt worden zonder expliciete goedkeuring/besluitvorming. Memoriaalboekingen en verplichtingen opnemen in een workflow, waarbij boeking pas verder kan als er akkoord is van de budgethouder.	M
Onbetaald meerwerk GroenXtra	Aanneemsommen worden gecalculeerd door calculator en geautoriseerd door projectleider en manager. Facturatie vindt plaats op basis van termijnschema. Elk project wordt jaarlijks opgeleverd. Regieopbrengsten worden vermeld door de uitvoerder op opleverstaten. Werkelijk bestede uren en materialen worden geboekt op project. Er is geen sprake van een sluitende nacalculatie per project. Sturing vindt plaats per uitvoerder (gerealiseerde uren / omzet per periode versus begroting)	M (sturen op uren personeel/materieel en netto toegevoegde waarde versus maandplanning/ jaarbegroting ,maar geen nacalculatie per project)
Post van klanten achterhouden	Toezicht op de uitvoering door postbodes (straatcontroles) is niet sluitend, steekproefsgewijze controle door dmv testpannel.	M (Imagoschade)
Kasontvangsten Kringloopbedrijf	Toezicht op volledigheid aanslaan winkelopbrengsten in kasregister (beschikken), en administratie (bewaren). Gezamenlijke controle op dagstaten (kas registratie aansluiten met ontvangen kasgeld/pinbonnen) en analyse kasverschillen.	H (Aansluiting geld-goederenbeweging ontbreekt)

	Periodieke controle kassaldi , afloopcontrole op afstorting kasgeld en periodieke rapportage van geboekte kasverschillen (kassiersfunctie) .	
Ontvreemding middelen in uitvoering	Controle tassen personeel kringloopbedrijf door leidinggevenden, controle op brandstofverbruik per voertuig (door afdeling wagenpark), bij onderdeel Productie scheiding tussen besluitvorming over magazijnontvangsten/afgiften door werkspecialisten op basis van orderadministratie en bewaarfunctie bij magazijnfunctie. Controle d.m.v cyclecount op aanwezigheid artikelen volgens voorraadadministratie.	L
Niet inleveren middelen door personeel	Tekenen voor ontvangst van middelen door werknemer, registratie verstrekte middelen door medewerker afdeling automatisering en borgen inleveren middelen door leidinggevende via workflow/checklist uitdienst	L
Valse onkostendeclaratie personeel	Leidinggevende autoriseert declaratie door medewerker. De personeelsadministratie controleert declaratieregel en nacalculatieregel. (Dit zijn harde controles, afgedwongen in de workflow indien declaratie)	L
Debiteurenbeheer	Scheiding tussen medewerker belast met invordering debiteuren en medewerker belast met verwerken. debiteurenontvangsten. Zij zijn niet belast met het autoriseren van betalingen. Telebankieren dwingt 4-ogen af bij alle betalingen. Dagelijkse controle op boeking bankjournaal (4-ogen) en maandelijkse rapportage voortgang incasso debiteuren.	L
Spookwerknemer personeel	Identificatie nieuw personeel aan de hand van geldig id-bewijs, controle op bezettingsoverzichten door leidinggevende vanuit HRM systeem, controle op tijdigheid uitdienstmeldingen (signaleren tijdige opzegging dienstverbanden voor bepaalde tijd, signaleren TWK mutaties) in HRM systeem.	L
Ongeoorloofd verzuim personeel	Verlofregistratie, verzuimregistratie, planning beschikbare uren, toezicht op aanwezigheid door leidinggevende, tijdschrijven, kwaliteitscontroles op verrichte werkzaamheden.	L (weinig thuiswerk)

Druk / Rationalisatie (softcontrols)

Cultuur *	Beheersmaatregel **
	Regeling vermoeden misstand (klokkenluidersregeling) 2016
	Ombudsvrouw aangesteld als vertrouwenspersoon integriteit 2016, jaarverslag ombudsvrouw 2021 gaat niet in op integriteit, geen klokkenluiders?
	Algemene gedragscode 2017
	Centrale klachtenregeling, geen klachten mbt integriteit?
	Nog geen apart M&O beleid opgesteld (externe fraude)
	Melden fraude in paragraaf bedrijfsvoering (is aanbeveling BBV).

* beschrijf de cultuur in onze organisatie : alert vanuit de eerste lijn op zaken die je niet behoort te doen, en met een strakke financiële bewaking vanuit planning en control. Verbetertraject loopt vanuit bedrijfsvoering inzake regie op de processen en ontwikkelen en implementeren van risico en kansen beheermodel.

** beschrijf welke maatregelen die we hebben genomen.

Ad ** Organisatorische maatregelen inzake integriteit:

Nevenfuncties melden

Vragen referenties bij indienstname / VOG

Geheimhoudingsverklaring

Informeren leidinggevende bij loonbeslag, omdat er mogelijk extra risico ontstaat

Ad ** Awareness creëren

Dilemma's inzake integriteit voorleggen / bespreken met personeel (bewustwordingstraining): softcontrols moet je vanaf het allerhoogst niveau aanpakken, voor heel de organisatie.

Leren van incidenten

Frauderisicoanalyse Diamant-groep bepalen aanvullende maatregelen voor gebieden met verhoogd restrisico

RESTRISICO'S FRAUDERISICOANALYSE

Uit de frauderisicoanalyse blijkt dat een aantal processen, ondanks de bestaande beheersmaatregelen, nog een verhoogd risico op fraude kennen. Dit betreft de onderstaande processen. Daarvan moet worden vastgesteld welke aanvullende maatregelen genomen worden om het risico verder te verkleinen.

Cybercrime

Aanvullende maatregelen: Zicht op volledigheid afdekking risico's /juistheid uitvoering beheersmaatregelen informatiebeveiliging is meerjarenplan. Er zijn geen lopende discussies met de frauderisicoverzekeraar / cybercrimeverzekeraar. Dit jaar focus op realisatie kansen op ICT gebied (AFAS, Office 365).

Prestatielevering

Aanvullende maatregelen: Zicht op volledigheid prestatielevering inkoop vraagt om aanvullend beleid. Vaststellen met management voor welke inkoopstromen we een bewijs van prestatielevering eisen en borgen in hun processen.

Opbrengsten/Kasverkeer kringloopwinkel

Aanvullende maatregelen: controle op verantwoording kasgelden door kringloopwinkels borgen in nieuwe opzet die het komend jaar wordt doorgevoerd. Volledigheid opbrengsten is niet vast te stellen, geen controleverklaring maar beoordelingsverklaring.

Integriteitsbeleid / Awareness

Beoordeling noodzaak aanvullende organisatorische maatregelen / aanvullend integriteitsbeleid meenemen in het uitvoeringsplan HRM (onboarding). Uitdragen gewenst gedrag integriteit en aanbieden bewustwordingstrainingen meenemen in projectgroep ongewenst gedrag. Ook de (rolverdeling) meldingsprocedure integriteit meenemen in deze projectgroep.