gemeente
Haarlemmermeer

De leden van de gemeenteraad van Haarlemmermeer

Postbus 250
2130 AG Hoofddorp

Bezoekadres:
Taurusavenue 100
Hoofddorp
Telefoon 0900 1852

Verzenddatum

16 JAN. 2024

Cluster	Corporate Control
Contactpersoon	Frank Bosma
Doorkiesnummer	023 567 4485
Uw brief	
Ons kenmerk	X.2023.07563
Bijlage(n)	Rapportage frauderisicoanalyse 2023
Onderwerp	Informatie over Rapportage frauderisicoanalyse 2023

Geachte heer, mevrouw,

In november 2022 heeft u de rapportage van de jaarlijkse overkoepelende frauderisicoanalyse ontvangen (X.2022.07035). Met deze brief wordt u geïnformeerd over de actualisatie hiervan.

Onze gemeente kent diverse instrumenten en regelingen ter voorkoming van fraude en misbruik en oneigenlijk gebruik. Er is een regeling Misbruik & Oneigenlijk gebruik (RV2020.000423) en er is daarnaast onder meer een gedragscode en een regeling melden vermoeden. Fraude betreft de eigen medewerkers en oneigenlijk misbruik betreft derden. Jaarlijks wordt een jaarverslag integriteit opgesteld dat u ter informatie ontvangt. Ook in de processen, procedures en interne controles is er aandacht voor de voorkoming van fraude en misbruik en oneigenlijk gebruik en er is aandacht voor risicomanagement in brede zin.

De organisatie heeft in 2022 een frauderisicoanalyse opgesteld als aanvulling op reeds bestaande instrumenten en regelingen ter voorkoming van fraude en misbruik en oneigenlijk gebruik. De frauderisicoanalyse wordt jaarlijks geactualiseerd, rekening houdende met mogelijke nieuwe latente frauderisico's. De toetsing van de beheersmaatregelen vindt plaats binnen de Verbijzonderde Interne Controle (VIC) en bij het actualiseren van deze overkoepelende frauderisicoanalyse. De geactualiseerde frauderisicoanalyse wordt jaarlijks ter kennisname aan de raad aangeboden.

Ten behoeve van de actualisatie 2023 zijn gesprekken georganiseerd met directie en clustermanagers over de (mogelijke) frauderisico's in de verschillende processen. Deze gesprekken hadden enerzijds als doel om te komen tot een actualisatie van de rapportage en anderzijds om het bewustzijn voor frauderisico's binnen de organisatie te vergroten en continue aandacht hiervoor te borgen. Met deze brief informeren wij de raad over de bevindingen en conclusies.

Bevindingen en conclusies
De actualisatie van de frauderisicoanalyse geeft geen directe aanleiding tot herprioritering van de frauderisico's en beheersmaatregelen, zoals benoemd in de rapportage van 2022. Het algemene beeld is, dat de aanvullende beheersmaatregelen door de organisatie zijn opgepakt en dat de naleving hiervan wordt getoetst door de VIC. Wel is een aantal signalen c.q. aandachtspunten naar voren gebracht, die de komende periode opgepakt zullen worden.

Naast de 'harde' beheersmaatregelen ter voorkoming van fraude, is ook nadrukkelijk aandacht gevraagd voor de inzet op soft controls, bewustwording en blijvende aandacht voor frauderisico's. Niet alle fraudegevallen zijn immers te voorkomen door middel van 'hard controls' en dat is ook niet altijd wenselijk. Het is belangrijk om een goede balans te vinden tussen controle en vertrouwen en tussen de menselijke maat en regeldrift. In dat kader is het van belang om juist ook aandacht te geven aan soft controls. In de organisatie wordt hier al op verschillende wijzen aandacht aan gegeven. Bijvoorbeeld door integriteitstrainingen en de aandacht voor frauderisico's en fraudepreventie in overleggen en de personeelsgesprekken.

Voorts is het belangrijk om doorlopend aandacht aan het onderwerp frauderisico's te besteden en dit niet te beperken tot eenmalige acties. In dit kader wordt de bewaking van opvolging van aanvullende maatregelen onderdeel van de reguliere VIC-cyclus.

De bevindingen en conclusies zijn gedetailleerd opgenomen in de 'Rapportage frauderisicoanalyse 2023'.

Misbruik en oneigenlijk gebruik
In 2024 zal een actualisatie plaatsvinden met betrekking tot het beleid rond Misbruik en oneigenlijk gebruik. In dit document wordt nader ingegaan op risico's en preventiemaatregelen omtrent misbruik en oneigenlijk gebruik. Vanwege de constatering dat er verwarring kan bestaan omtrent de verschillende begrippen die een relatie hebben met frauderisico's en elkaar soms ook overlappen, wordt hier in de actualisatie nader op ingegaan.

Wij verwachten u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
burgemeester en wethouders van de gemeente Haarlemmermeer,

de secretaris,	de burgemeester,
Cees Vermeer	Marianne Schuurmans-Wijdeven

Rapportage Frauderisicoanalyse 2023

Cluster Corporate Control en HRM

gemeente Haarlemmermeer

Inhoudsopgave

1. Inleiding (1/4)

Onze gemeente kent diverse instrumenten en regelingen ter voorkoming van fraude en misbruik en oneigenlijk gebruik. Er is een regeling Misbruik & Oneigenlijk gebruik (RV2020.000423) en er is daarnaast onder meer een gedragscode en een regeling melden vermoeden. Jaarlijks wordt een jaarverslag integriteit opgesteld. Ook in de processen, procedures en interne controles is er aandacht voor de voorkoming van fraude en misbruik en oneigenlijk gebruik en er is aandacht voor risicomanagement in brede zin.

De organisatie heeft in 2022 een frauderisicoanalyse opgesteld (X.2022.07035) als aanvulling op reeds bestaande instrumenten en regelingen ter voorkoming van fraude en misbruik en oneigenlijk gebruik. De frauderisicoanalyse wordt jaarlijks geactualiseerd, rekening houdende met mogelijke nieuwe latente frauderisico's en wordt ter kennisname aan de raad aangeboden. De toetsing van de beheersmaatregelen vindt plaats binnen de VIC en bij het actualiseren van deze overkoepelende frauderisicoanalyse.

Ten behoeve van de actualisatie 2023 zijn gesprekken georganiseerd met directie en clustermanagers over de (mogelijke) frauderisico's in de verschillende processen. Deze gesprekken hadden enerzijds als doel om te komen tot een actualisatie van de rapportage en anderzijds om het bewustzijn voor frauderisico's binnen de organisatie te vergroten en continue aandacht hiervoor te borgen.

2. Bevindingen en conclusies (1/4)

Prioritering frauderisico's en beheersmaatregelen

De update van de uitgevoerde frauderisicoanalyse geeft geen directe aanleiding tot herprioritering van de frauderisico's en beheersmaatregelen, zoals benoemd in de rapportage van 2022. Het algemene beeld is, dat de aanvullende beheersmaatregelen door de organisatie zijn opgepakt en dat de naleving hiervan wordt getoetst door de Verbijzonderde Interne Controle. Wel is een aantal signalen c.q. aandachtspunten naar voren gebracht, die de komende periode opgepakt zullen worden. Dit zijn met name:

- voor een aantal specifieke functies binnen het team OOV is het los van de VOG (P) wenselijk om meer in- en pre-employmentscreening te doen, met name functies die een relatie hebben met ondermijningsrisico's of die betrokken zijn bij de driehoek (werving- en selectieprotocol aanpassen);
- frauderisico's in relatie tot verbonden partijen en samenwerkingsverbanden vragen extra aandacht (bijvoorbeeld ter voorkoming van het betalen van dubbele facturen);
- de controle op declaratie van de thuiswerkvergoeding versus de reiskostenvergoeding vraagt aanscherping;
- naar aanleiding van incidenten wordt aandacht gevraagd voor het voorkomen van situaties waarbij (ingehuurde) medewerkers die vanuit huis werken een dubbele aanstelling hebben zonder dit te hebben gemeld;
- samenspanning blijft altijd een risico en vraagt om continue alertheid.

2. Bevindingen en conclusies (2/4)

Bewustwording en soft controls ter voorkoming van fraude

Naast de ‘harde’ beheersmaatregelen ter voorkoming van fraude, is ook nadrukkelijk aandacht gevraagd voor de inzet op soft controls, bewustwording en blijvende aandacht voor frauderisico’s. Niet alle fraudegevallen zijn immers te voorkomen door middel van ‘hard controls’ en dat is ook niet altijd wenselijk. Het is belangrijk om een goede balans te vinden tussen controle en vertrouwen en tussen de menselijke maat en regeldrift. In dat kader is het van belang om juist ook aandacht te geven aan soft controls. In de organisatie wordt hier al op verschillende wijzen aandacht aan gegeven:

- nastreven van een open houding en cultuur en ruimte geven om te leren van elkaars fouten;
- aandacht voor frauderisico’s en fraudepreventie in overleggen;
- aandacht voor medewerkers die in een kwetsbare positie zitten vanwege schulden (stimuleren om hierover in gesprek te gaan met manager of vertrouwenspersoon);
- periodiek herhalen van de training iBewustzijn/Digitale Veiligheid en Integriteitstraining (management);
- fraude is niet altijd opzettelijk, maar kan ook voortkomen uit compassie en goede bedoelingen, bijvoorbeeld om inwoners zo goed mogelijk van dienst te kunnen zijn. Omdat ook in die gevallen sprake is van fraude, wordt regelmatig vanuit het management gecommuniceerd dat ook in die gevallen actie ondernomen moet worden.

2. Bevindingen en conclusies (3/4)

Bewustwording en soft controls ter voorkoming van fraude (vervolg)

- bij relatief veel externe inhuur en een hoog verloop is extra aandacht nodig voor bewustzijn ten aanzien van frauderisico's, in het geval van externe inhuur specifiek ook omdat deze medewerkers niet het introductieprogramma voor nieuwe medewerkers volgen;
- ook voor wat betreft Privacy en Informatiebeveiliging is bewustwording een belangrijke mitigerende maatregel. Voorbeeld: hack, malafide emailverzoek tot goedkeuren van een personeelsadvertentie, CEO-fraude (phishing mail met verzoek tot spoedbetaling op verzoek van gemeentesecretaris), ongeoorloofd raadplegen van informatie en gegevens;
- een aantal clusters (Burgerzaken, Sociale Dienstverlening, Veiligheid) werkt samen onder de titel 'Vreemd verhaal', om periodiek signalen met elkaar te delen die mogelijk kunnen duiden op integriteits- of frauderisico's;
- belangrijk is om doorlopend aandacht aan het onderwerp frauderisico's te besteden en dit niet te beperken tot eenmalige acties.

2. Bevindingen en conclusies (4/4)

Raadsnotitie Misbruik en oneigenlijk gebruik

- In 2024 zal een actualisatie plaatsvinden van de raadsnotitie Misbruik en oneigenlijk gebruik. In deze notitie wordt nader ingegaan op risico's en preventiemaatregelen omtrent misbruik en oneigenlijk gebruik. Vanwege de constatering dat er verwarring kan bestaan omtrent de verschillende begrippen die een relatie hebben met frauderisico's en elkaar soms ook overlappen, zal hier in de actualisatie nader op in worden gegaan.

3. Wat is fraude?

Volgens de standaarden voor accountants (COS240) is fraude:

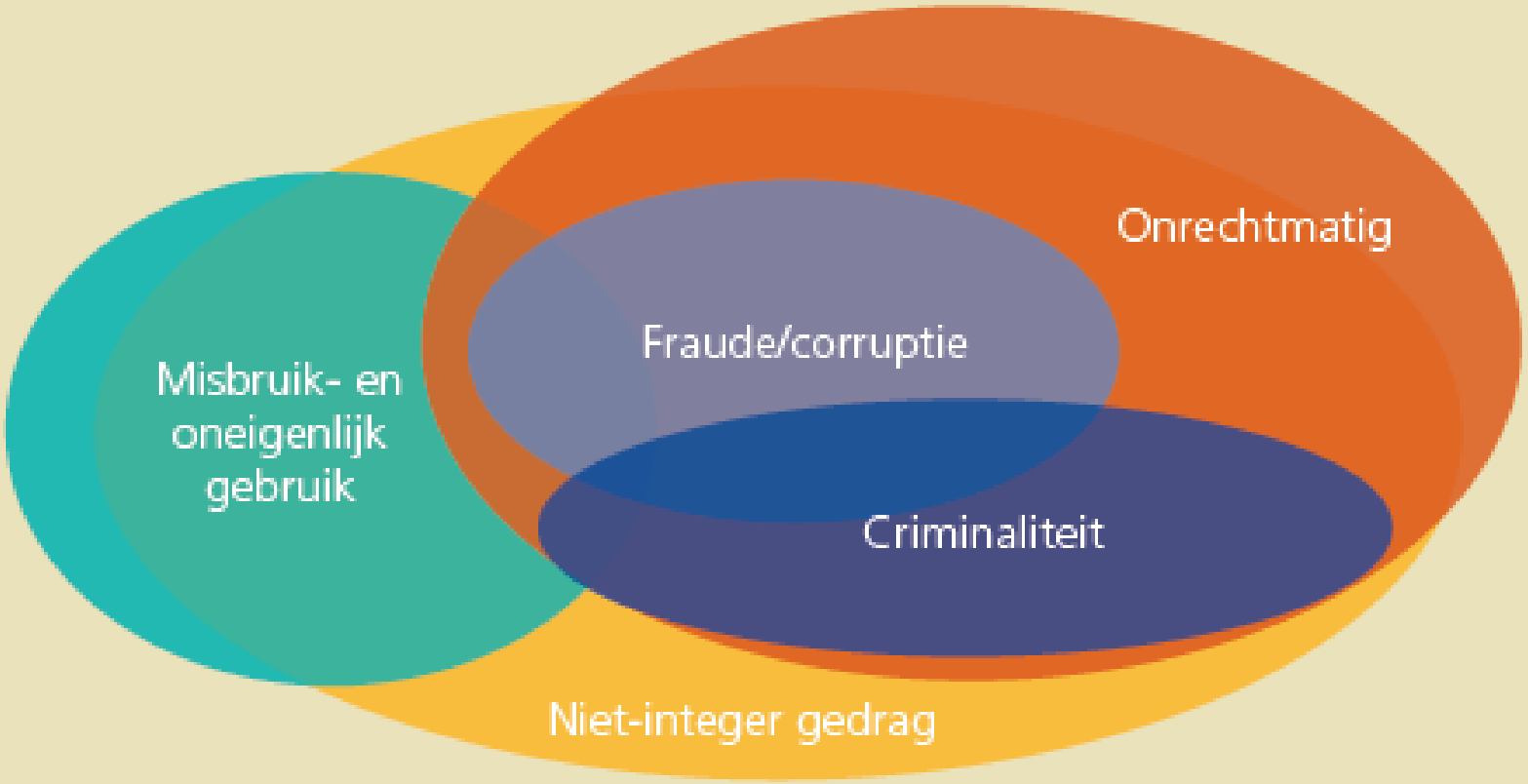
- “een opzettelijke handeling
- door één of meer leden van het management, met governance belaste personen, werknemers of derden,
- waarbij gebruik wordt gemaakt van misleiding
- teneinde een onrechtmatig of onwettig voordeel te verkrijgen”.

> Voorbeelden van fraude zijn boekhoudfraude en subsidiefraude.

> Fraude kan zowel *intern* plaatsvinden (door medewerkers) als *extern* (door inwoners, bedrijven, subsidierelaties, etc.). Externe fraude valt onder het Misbruik en oneigenlijk gebruik (M&O)-criterium in het kader van de rechtmatigheidsverantwoording.

> Fraude kan ook niet-financieel zijn, bijvoorbeeld als het doel is om een specifieke vergunning te verkrijgen.

4. Onderscheid diverse begrippen (1/3)



Figuur 1: **Onderscheid diverse begrippen**

Bron: Deloitte

4. Onderscheid diverse begrippen (2/3)

Twee centrale begrippen in het voorgaande schema zijn misbruik en oneigenlijk gebruik en fraude:

- *Fraude* is een verzamelnaam voor allerlei verwijtbaar, niet-toegestaan of niet gewenst gedrag. Fraude is een verzamelbegrip van (strafrechtelijke) bepalingen waarbij het gaat om vermogensdelicten, bijvoorbeeld: valsheid in geschrifte, verduistering, oplichting, (niet-)ambtelijke corruptie en eenvoudige en bedrieglijke bankbreuk.
- Bij *misbruik en oneigenlijk gebruik* worden overheidsgelden aangewend voor doeleinden waarvoor deze niet zijn bestemd. Op nagenoeg alle beleidsterreinen van een gemeente is misbruik en oneigenlijk gebruik mogelijk. Misbruik, oneigenlijk gebruik en fraude liggen dicht bij elkaar. Bij de begrippen misbruik en oneigenlijk gebruik gaat het over derden buiten de organisatie (extern), zoals inwoners, klanten en leveranciers van de gemeente. Hier bestaat het risico dat zij misbruik of oneigenlijk gebruik maken van middelen of diensten van de gemeente. Misbruik is onrechtmatig, oneigenlijk gebruik niet.

In deze overkoepelende frauderisico-analyse betrekken wij zowel handelingen door personen binnen de organisatie (intern) als door personen/partijen buiten de organisatie (extern).

Op de volgende sheet wordt een aantal voorbeelden gegeven bij de verschillende begrippen.

4. Onderscheid diverse begrippen (3/3)

Niet-integer gedrag/ geen fraude: Nevenactiviteiten die niet opgegeven zijn aan de werkgever, het aannemen van geschenken.

Onrechtmatig: Diefstal, verduistering: facturen (laten) betalen voor niet geleverde diensten.

Fraude/corruptie: Omkoping: het delen van de “winst” bij het betalen van niet geleverde diensten (aan het niet gemelde eigen bedrijf).

Criminaliteit: Ondermijning, witwassen van geld.

Misbruik en oneigenlijk gebruik: Het onterecht ontvangen van subsidie of een uitkering (ingevolge aanlevering van onvolledige documentatie).

Fraude/ geen M&O: corruptie, bijvoorbeeld omkoping van ambtenaar door derden.

Fraude/ M&O: versturen van valse facturen door medewerkers in dienst van de gemeente.

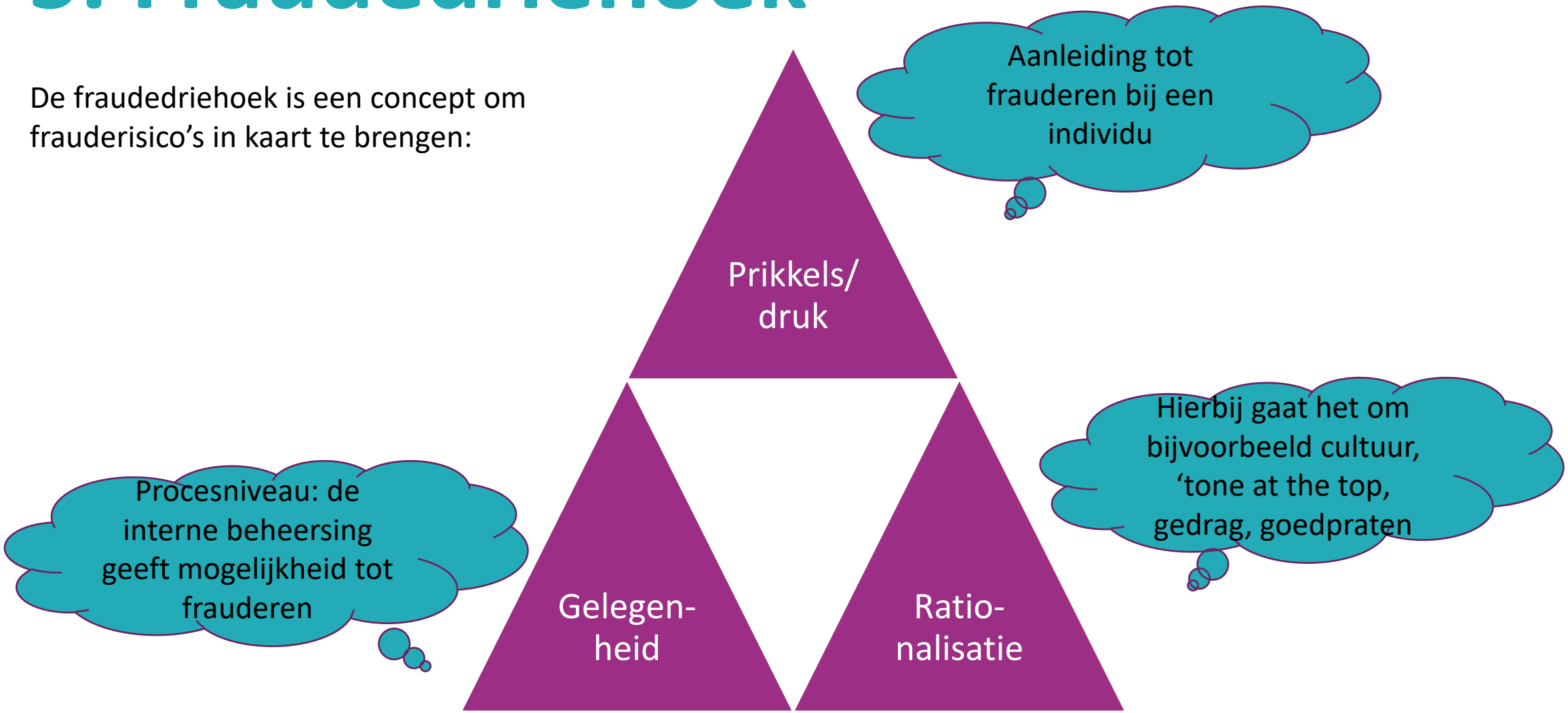
Geen fraude/ M&O: uitkeringsfraude, een inwoner van de gemeente vraagt en ontvangt ten onrechte een uitkering.

Onrechtmatig handelen/ M&O: de waarde van een opdracht bewust te laag inschatten (contractduur te laag ingeschat) om de Europese aanbestedingsregels te omzeilen.

Onrechtmatig handelen/ geen M&O: bewuste overtreding van Europese aanbestedingsregels die intern afdoende is afgestemd.

5. Fraudedriehoek

De fraudedriehoek is een concept om frauderisico's in kaart te brengen:



5.1. Fraudedriehoek: toelichting

Druk (op werk en privé)

Vanuit de organisatie of vanuit de privé situatie wordt druk opgelegd die tot fraude kan leiden (prikkel). Het gaat hierbij naast druk vanuit de organisatie (werkdruk, tijdsdruk, politieke druk of groepsdruk) bij het realiseren van doelen afgeven van vergunningen, bijstellen budgetten, subsidies e.d. ook om geld, prestige en de privésituatie (bijvoorbeeld verslaving, echtscheiding, schulden) die druk veroorzaken. Er zijn factoren aan te wijzen die druk verhogend werken en daarmee een verhoogd frauderisico voor een organisatie veroorzaken.

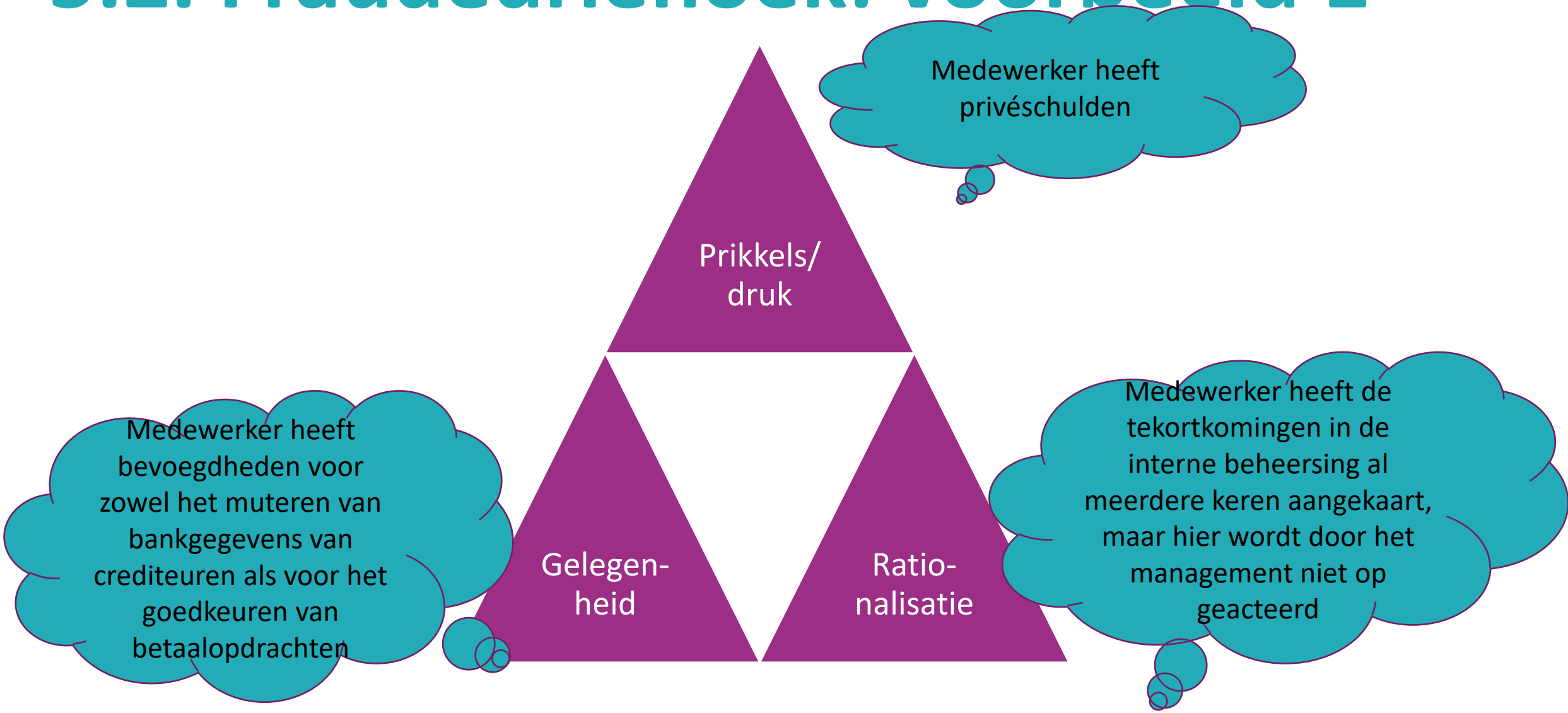
Gelegenheid (meest te beïnvloeden met hard controls)

De gelegenheid is de mogelijkheid die de organisatie openlaat (niet met beheersmaatregelen heeft afgedekt) om te frauderen. Het voorkómen van het frauderisico dient zich met name op het punt ‘gelegenheid’ te concentreren. De beheersmaatregelen ter voorkoming van gelegenheid zijn vooral de meer ‘harde’ procesmaatregelen.

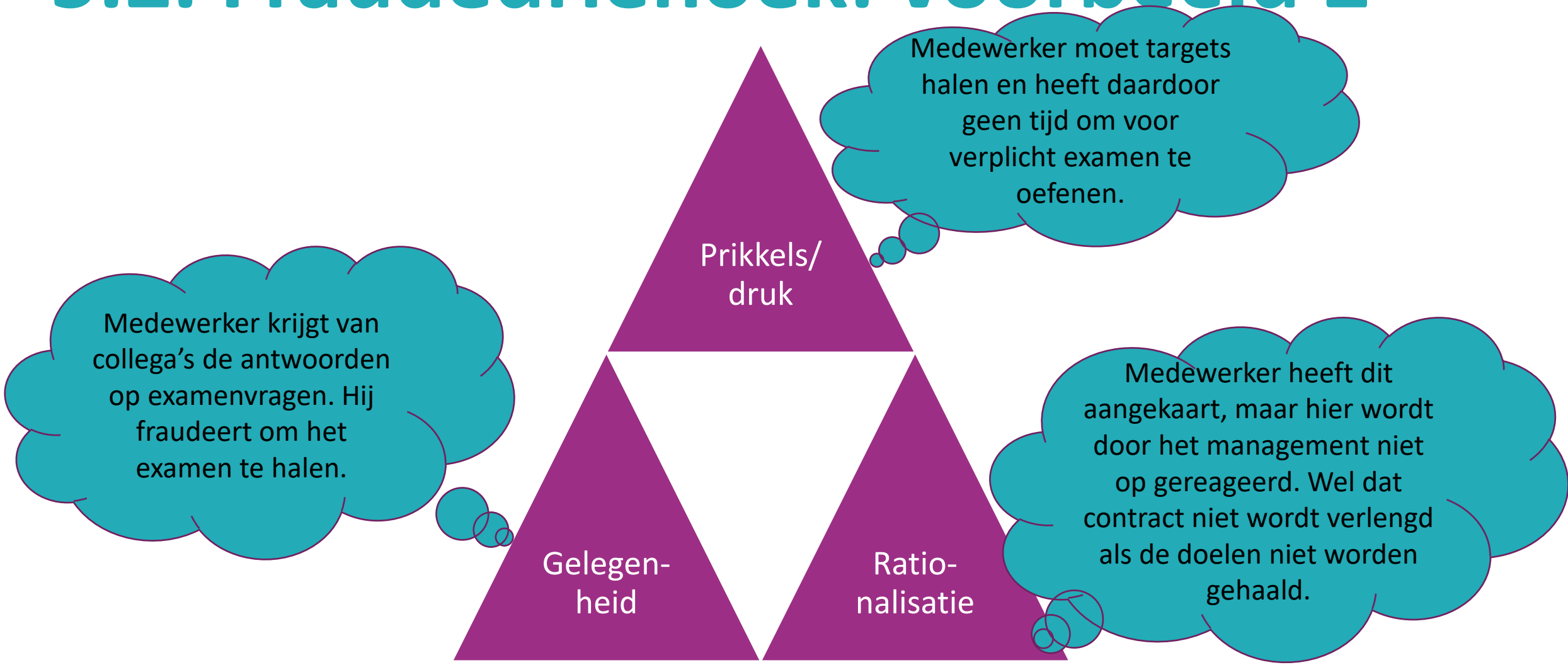
Rationalisatie (voor een deel te beïnvloeden via soft controls)

Rationalisatie is goedpraten van de fraude; “ze hebben toch geld zat” of “ik heb het risico meerdere keren aangekaart maar ze doen er niks aan”. Goed voorbeeldgedrag (‘the tone at the top’) van de leiding en het bestuur is essentieel, zodat intern geen voedingsbodem voor rationalisatie ontstaat.

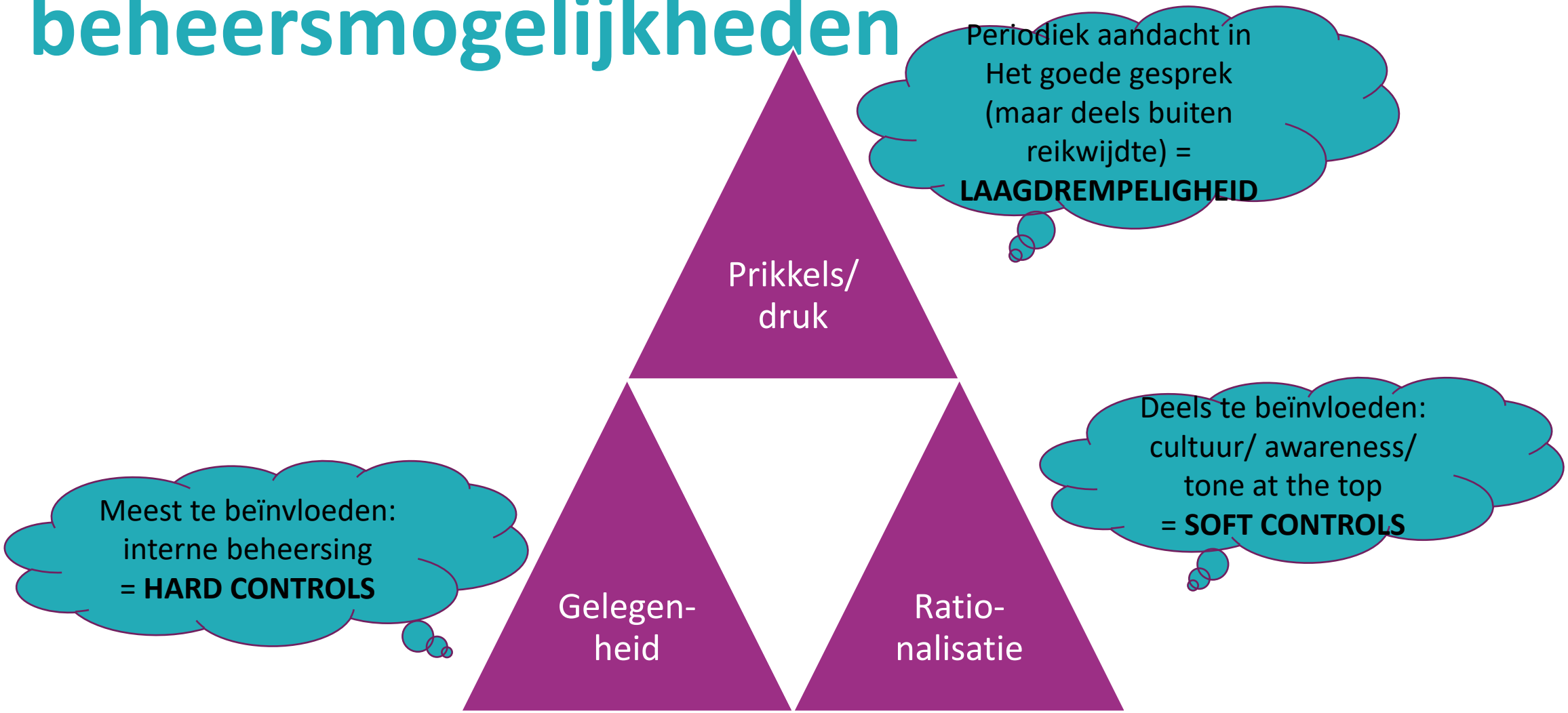
5.2. Fraudedriehoek: voorbeeld 1



5.2. Fraudedriehoek: voorbeeld 2



5.3. Fraudedriehoek: beheersmogelijkheden

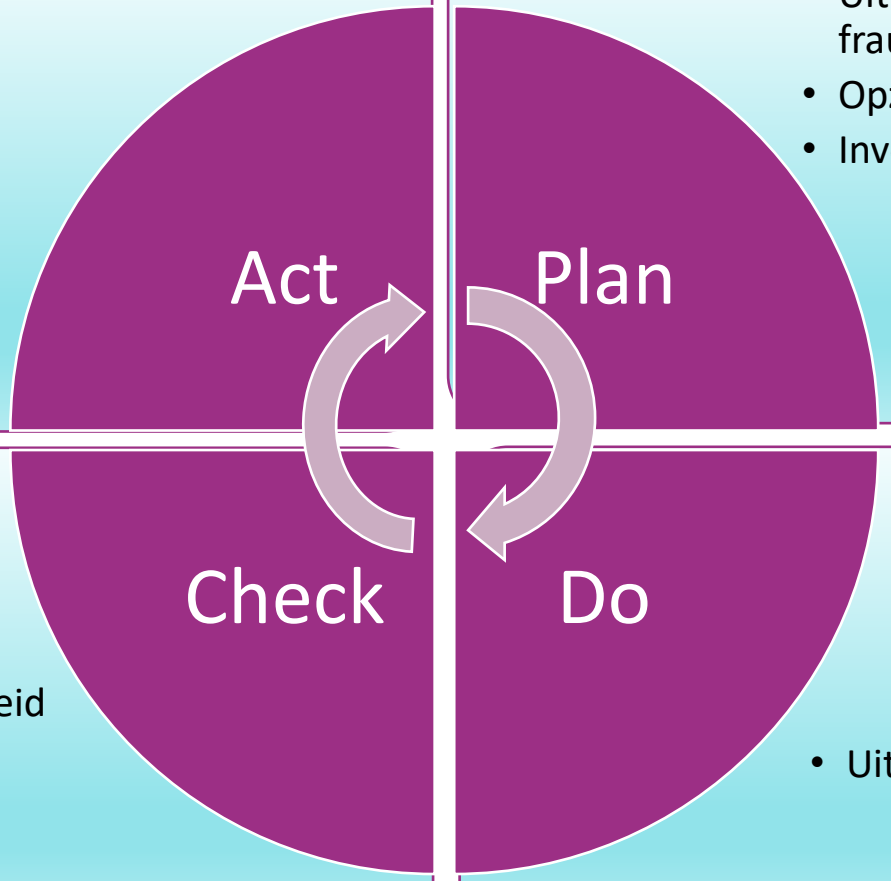


6. Cyclus frauderisicoanalyse

- Uitvoeren en actualiseren frauderisicoanalyse
- Opzetten beheersmaatregelen
- Inventariseren en accepteren restrisico's

Corporate Control: proces

College: vaststellen



- Uitvoeren van beheersmaatregelen

Proceseigenaar

- Vaststellen dat beheersmaatregelen bestaan en werken
- Vaststellen van juistheid en volledigheid van geïnventariseerde frauderisico's

Proceseigenaar: IC

Corporate Control: VIC

- Treffen van aanvullende beheersmaatregelen
- Evaluatie van (rest)risico's

Proceseigenaar

7. Aanpak

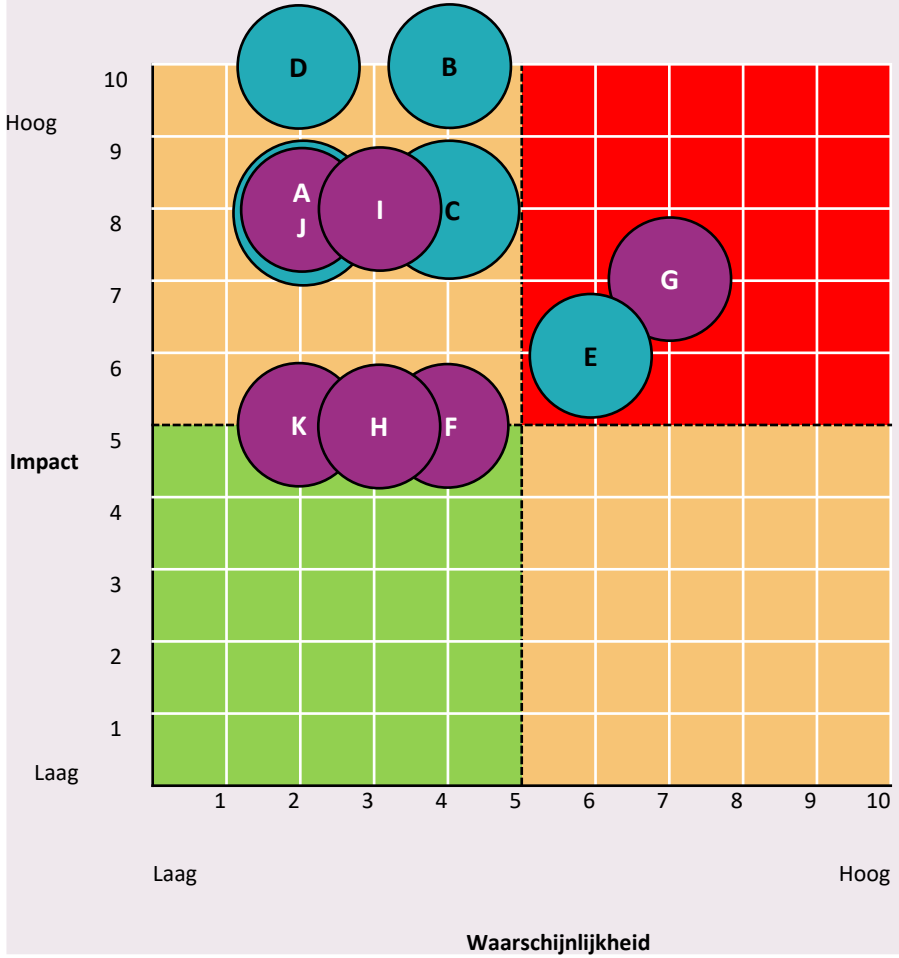
1. Inventarisatie potentiële risico's.
2. Inventarisatie aanwezige beheersmaatregelen.
3. Bepalen van het resterende frauderisico (na genomen beheersmaatregelen).
4. Bepalen van aanvullende maatregelen voor gebieden met een verhoogd restrisico.

De uitkomsten van de bovenstaande analyse zijn verwerkt in de frauderisicotabel (zie hoofdstuk 7 'Uitkomsten frauderisicoanalyse'). Deze wordt periodiek geactualiseerd.

N.B.: Bij de benoemde risico's is een inschatting gemaakt van de kans en impact. Voor de classificering hiervan is zoveel mogelijk aangesloten bij de kans- en gevolgklassen die worden gehanteerd voor het weerstandsvermogen conform de vastgestelde Notitie Risicomanagement.

8. Uitkomsten frauderisicoanalyse

8.1 Inventarisatie risico's



	Generieke frauderisico's	Kans	Impact
A	Ondermijning / integriteitsschendingen door de gemeentelijke organisatie	2	8
B	Ondermijning / integriteitsschendingen waarbij derde partijen betrokken zijn	4	10
C	Ongeoorloofde toegang	4	8
D	Verlies / lekken van kritische of privacygevoelige data	2	10
E	Onvoldoende opvolging van maatregelen bij leveranciers	6	6
	Financiële frauderisico's		
F	Frauduleuze betalingen	4	5
G	Zorgfraude	7	7
H	Fraude met declaraties / vergoedingen	3	5
I	Fraude via beoordelen leveranciers	3	8
J	Identiteitsfraude	2	8
K	Fraude met opbrengsten	2	5

N.B.: Bovenstaande prioritering, inclusief kans en impact, is gebaseerd op de risico-analyse Dreigingsbeeld HLMR uit 2021 (generieke risico's) en de risico-analyse VIC (financiële risico's). Het betreft de bruto risico's, dus zonder rekening te houden met genomen beheersmaatregelen.

8.2 Aanwezige beheersmaatregelen (1/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Hoog	Zorgfraude: Zorgleveranciers declareren meer dan wordt geleverd (kwantiteit/kwaliteit)	AO/IC: PDC goedkeuring declaratie (Indien geen startbericht zorg bij declaraties aanwezigheid is, wordt de declaratie afgekeurd en gaat een signaal uit richting zorgaanbieder). Stapeling van signalen (ook kwaliteitssignalen) is een bespreekpunt bij de contractmanagementbesprekingen. Er is geïnvesteerd op dit contractmanagement, waarbij gericht wordt gekeken naar de afgegeven beschikkingen en bijbehorende facturering. Daarnaast wordt ook een proactieve aanpak rondom prestatielevering gehanteerd op basis van monitoring van het berichtenverkeer. De accountant rapporteert dan ook de verbeterde beheersing op tijdige facturaties door zorgleveranciers. Er is een beheersmaatregel ingericht die de ontvangst van een goedkeurende accountantsverklaring van de grote zorgleveranciers monitort, zoals geadviseerd door de commissie Besluit Accountantscontrole Decentrale Overheden (BADO). Als sluitstuk geldt de VIC op prestatielevering op basis van uitvraag aan zorgleveranciers. Het vaststellen van prestaties van alle zorgfacturen, is niet passend gegeven de omvang van de werkzaamheden in relatie tot de aanwezige restrisico's. Aanvullend zijn per december 2023 twee toezichthouders JW/Wmo aangesteld t.b.v. signaal- en risico gestuurde aanpak zorgfraude. Bij verlenging wordt de prestatielevering van de voorgaande periode betrokken bij de beoordeling van de consulent voor het vervolg middels een evaluatieplan. Specifiek voor PGB: Checklist nieuwe PGB-verleners, incl. aanmelding nieuwe jeugdhulpaanbieder bij inspectieloket SD. IC (onder)uitnutting PGB tweemaal per jaar. Bij verlenging wordt de prestatielevering van de voorgaande periode betrokken bij de beoordeling van de consulent voor het vervolg middels een evaluatieplan. VIC: Controle bestaan en werking van de PDC goedkeuring, checklist nieuwe PGB-verleners en IC (onder)uitnutting PGB. Steekproefsgewijs wordt onderbouwing van prestatielevering uitgevraagd bij zorgleveranciers.

8.2 Aanwezige beheersmaatregelen (2/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Hoog	Onvoldoende opvolging van maatregelen bij leveranciers: Leveranciers komen contractuele verplichtingen niet na m.b.t. veiligheid en toegang	Overeenkomsten en contractuele verplichtingen externe leveranciers

8.2 Aanwezige beheersmaatregelen (3/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Frauduleuze betalingen (1): Organisatie betaalt nepfacturen	1) Sinds 2023 worden facturen vanaf € 5.000,- waarvoor geen verplichting is aangemaakt, niet in behandeling genomen. Er bestaat geen IC op de juistheid van de autorisatie van de aangegane verplichting. Opgemerkt wordt dat zolang deze IC niet geautomatiseerd kan worden uitgevoerd hij niet doelmatig wordt geacht. Vertrouwd wordt op de integriteit en de professionaliteit van de mdw.'s, de IC van de Budgethouder op het moment dat een factuur betaald moet worden en de VIC's. Omdat de controle door de Budgethouder geen toereikende beheersmaatregel voor het signaleren van het niet naleven van de regelgeving (waaronder de limieten) door de budgethouder zelf is, de VIC's te weinig verplichtingen beoordelen om iets over de totale massa te kunnen zeggen en de bevindingen uit de VIC Inkoopfacturen geen aanleiding geven om op soft controls te kunnen steunen, blijft de kans dat er als gevolg van situatie 1 sprake is van M&O groot. 2) Bij het aanmaken van routingcodes door een Specialist Ondersteuning Financieel Beheer van team DCFA wordt erop gelet dat de prestatie-accordeerder niet dezelfde is als de budgethouder. Echter, deze situatie kan zich wel voordoen als iemand optreedt als vervanger van de prestatie-accordeerder en/of budgethouder. E1 kan dit niet uitsluiten. Periodiek wordt er door een Mdw. ondersteuning en de TM DCFA een integrale IC uitgevoerd waarbij m.b.v. een query voor de totale massa gekeken wordt of het prestatie-akkoord door een ander is gegeven dan het budgethouderakkoord. Deze IC beheersmaatregel werkt goed, er worden weinig tekortkomingen geconstateerd en alle geconstateerde tekortkomingen worden hersteld. Om deze redenen wordt de kans dat er als gevolg van situatie 2 sprake is van M&O als zeer klein ingeschat. 3) Facturen die de routing niet juist doorlopen hebben als gevolg van onjuist gebruik van de routingcode worden door het systeem gedetecteerd. De routing is niet juist doorlopen als het prestatie-akkoord of het budgethouderakkoord ontbreekt. Het systeem zendt met betrekking tot deze facturen automatisch een e-mail naar de Helpdesk van team DCFA. Dergelijke facturen blijven als er niets gebeurt in FIO hangen en kunnen niet op de betaaladvieslijst terechtkomen. Facturen die de routing niet juist doorlopen hebben als gevolg van een fout bij de inrichting van de routingcodes komen wel op de betaaladvieslijst terecht. Dit komt incidenteel voor en wordt gesignaleerd bij de periodieke integrale interne controle door een Mdw. ondersteuning en de TM DCFA, waarbij m.b.v. een query voor de totale massa gekeken wordt of er geen betalingen hebben plaatsgevonden waarbij het prestatie-akkoord en/of het budgethouderakkoord ontbreekt. Deze IC beheersmaatregel werkt goed, er worden weinig tekortkomingen geconstateerd en alle geconstateerde tekortkomingen worden hersteld. Om deze redenen wordt de kans dat er als gevolg van situatie 3 sprake is van M&O als zeer klein ingeschat.

8.2 Aanwezige beheersmaatregelen (4/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Frauduleuze betalingen (1): Organisatie betaalt nepfacturen	4) Het is niet alleen belangrijk dat er een prestatie-akkoord en een budgethouderakkoord wordt gegeven, maar ook dat de IC's die daaraan ten grondslag moeten liggen door de prestatie-accordeerder en de budgethouder juist worden uitgevoerd. Dit blijkt regelmatig niet het geval te zijn. Tijdens de VIC blijkt dat er in veel situaties onvoldoende invulling wordt gegeven aan de rol van integraal manager en dat de organisatie weinig (effectieve) soft controls inzet om de houding en gedrag van budgethouders en mdw.'s zodanig te beïnvloeden dat IC's niet alleen formeel, maar ook materieel juist worden uitgevoerd. Om deze redenen blijft de kans dat er als gevolg van situatie 4 sprake is van M&O groot.

8.2 Aanwezige beheersmaatregelen (5/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Frauduleuze betalingen (2): Medewerker verandert IBAN crediteur in het adresboek in eigen IBAN	1) Binnen het team DCFA wordt het bankrekeningnummer in het adresboek van een crediteur door andere mdw's gewijzigd dan degenen die de juistheid van de wijziging in het systeem moeten bevestigen. Alleen met betrekking tot de wijziging van het bankrekeningnr-veld is er sprake van het 4-ogenprincipe. Bij de VIC wordt de werking van dit 4-ogenprincipe beoordeeld. Er is ook een 4-ogenprincipe op het moment dat een aan een adresboek gekoppelde factuur een ander adresboeknr / andere begunstigde krijgt. Een oordeel over de werking hiervan is geen onderdeel van de VIC. De wijziging in bankrekeningnr. is naar aanleiding van het hack-incident in 2022 onderdeel geworden van de IC en VIC werkzaamheden. Er is sprake van een integrale naam-nummer controle via mijnBNG. Bij buitenlandse rekeningnr.'s wordt de wijziging telefonisch geverifieerd op het bekende telefoonnummer van de crediteur. De telefonische verificatie wordt per email bevestigd. Bij de VIC wordt de werking van deze naam-nummer controle beoordeeld. 2) Automatisch gegenereerde betaaladvieslijsten worden vervaardigd door een Adm. mdw. crediteuren van team DCFA, automatisch voorzien van de naam van de vervaardiger. Vervolgens wordt de lijst gemaild aan de Mdw. ondersteuning FB van team DCFA die belast is met de controle van de lijst. Hierbij worden alle betalingen waarbij het systeem automatisch in het rood het woord CHECK geplaatst heeft gecontroleerd. Dit zijn in ieder geval alle PH (facturen) en PV (betaalopdrachten) betalingen > € 100.000 en alle PS betalingen (subsidies) ongeacht het bedrag en alle betalingen waarvoor geldt dat het adresnr. niet gelijk is aan het begunstigde nr. Er wordt gekeken naar de juistheid van het bankrekeningnr., de naam van de crediteur, het factuurnr. en het bedrag. De Mdw. ondersteuning laat een digitaal controlespoor achter op de lijst en plaatst digitaal een paraaf en datum op de lijst. De gecontroleerde lijst wordt o.a. opgeslagen op de P-schijf, gemaild naar de Adm. mdw. die de lijst heeft opgesteld en doorgestuurd en geprint later in het traject. Nadat de Adm. mdw. heeft vastgesteld dat de gecontroleerde lijst akkoord is bevonden, zet deze de betalingen van de lijst klaar in een betaalbatch in de BNG-applicatie (betaaltape) en zet de 1ste handtekening. De 2de handtekening wordt gezet door Specialist Ondersteuning van team Sigma of team DCFA. Dit kan alleen als de 1ste handtekening is gezet. De mdw. die de 2de handtekening gaat zetten controleert of de lijst is gecontroleerd en akkoord bevonden en of degene die de lijst heeft gecontroleerd een andere mdw. van DCFA is dan degene die de 1ste handtekening heeft gezet. Tot slot wordt zelfstandig vastgesteld dat het totaal van de gecontroleerde en akkoord bevonden lijst overeenkomt met het totaal van de klaargezette betaalbatch in de BNG-applicatie. Een oordeel over de werking van de functiescheiding en controle betaaladvieslijst is onderdeel van de VIC.

8.2 Aanwezige beheersmaatregelen (7/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Ondermijning / integriteitsschendingen waarbij derde partijen zijn betrokken (bij voorbeeld bij vergunningverlening of inkoop van diensten) samenspanning.	- Kennisdeling op gebied van integriteit en ondermijning en verbetering weerbaarheid ism de Provincie Noord Holland - Identificatie kritische functies - Jaarlijkse training management en training bij indiensttreding - Voorlichting door Rijksrechercheurs - Vertrouwenspersonen (4x) + externe VP - Beleid en richtlijnen (bijv. aannemen geschenken) en nevenwerkzaamheden - Afleggen eed - VOG(P) verklaring en screening kritische functies indiensttreding - Goed Gesprek beoordelingssysteem waar integriteit verplicht onderdeel van is - Ferm optreden bij vermoedens opzettelijke integriteitsschending - 4 ogen principe - functie scheiding bv bij facturen of projecten accorderen - relevant aanbestedingsbeleid - beperkte bevoegdheden inhuur - meldplicht – Meldpunt Integriteit / Meldpunt Vreemd verhaal
Gemiddeld	Ongeoorloofde toegang	- Toegangscontrole met diverse veiligheidszones afhankelijk van het soort functie - Inzet van fysieke beveiliging - Aandacht voor het zichtbaar dragen van toegangspas

8.2 Aanwezige beheersmaatregelen (6/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Ondermijning / integriteitsschendingen door de gemeentelijke organisatie (bijv. vervalsing handtekeningen of diefstal of misbruik zakelijke middelen zoals brandstofpas)	- Kennisdeling over integriteit en ondermijning en verbetering weerbaarheid ism de provincie - Identificatie kritische functies - Jaarlijkse training management en training bij indiensttreding (e-learning ‘MEER dan Welkom') - Voorlichting door Rijksrechercheurs - Vertrouwenspersonen (4x) + externe VP - Beleid / richtlijnen, bijv. aannemen geschenken en nevenwerkzaamheden - Afleggen eed - VOG(P) verklaring indiensttreding en screening kritische functies - Integriteit behandelen binnen Het goede gesprek beoordelingssysteem - Ferm optreden bij vermoedens opzettelijke integriteitsschending - Functiescheiding bv bij facturen of projecten accorderen - Aanbestedingsbeleid - Beperkte bevoegdheden inhuur - ‘Meldplicht en meldstructuur' - Aandacht voor nevenwerkzaamheden (Het goede gesprek)

8.2 Aanwezige beheersmaatregelen (8/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Verlies / lekken kritische of privacygevoelige data - hoog risico i.v.m. veel privacy gevoelige data (ook opgenomen als gevolg van andere digitale risico's - zie volledig risicoprofiel)	- AVG procedures zijn er, maar nog niet volledig geïmplementeerd - Melden datalekken bij AP - Melden BRP - Inrichting privacy officer en FG - Inrichting datalek procedures - Bewustwording en doorlopende training personeel - Jaarlijkse toetsing BIO-normen - ENSIA verantwoording
Gemiddeld	Fraude via beoordelen leveranciers: Bevoordelen leveranciers bij gunning opdrachten	AO/IC: EA via multidisciplinair aanbestedingsteam en Tenderned. Dit betekent dat elke partij kan inschrijven. Daarbij komt dat de inkoper betrokken is bij deze trajecten en zij ook het Tenderned deel afhandelen. Voor DAS geldt eenzelfde redenering. Daarnaast is sprake van beoordelingscommissies bij deze aanbestedingen, waarbij partijen o.b.v. objectieve criteria de leveranciers scoren. Conclusie nagenoeg geen risico. Bij MVO wordt vooraf het startformulier langs inkoop gehaald en is I&JZ bij sommige trajecten betrokken. Ook zou de offerte-uitvraag in het dossier moeten zitten, zodat vastgesteld kan worden dat meerdere partijen benaderd zijn. Hier is dus een hoger risico, omdat I&JZ niet alle beoordelingen ziet of niet altijd hierbij betrokken is. Conclusie beperkt risico. Bij EVO is het risico van bevooroordeling niet uit te sluiten, omdat daar simpelweg 1 op 1 gegund mag worden, dus bijvoorbeeld ook elk jaar een opdracht van € 10.000 aan dezelfde partij. Conclusie: Bij de EVO gunningen kan sprake zijn van bevoordeling, maar de wet verbiedt het hierbij niet om telkens aan dezelfde partij te gunnen. Het financiële risico is hier ook veel minder groot.

8.2 Aanwezige beheersmaatregelen (9/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Identiteitsfraude: Medewerker geeft reisdocument af op basis van onjuiste gegevens	AO/IC: Functiescheiding in het aanvraag- verwerking- en uitreikproces van reisdocumenten, ondersteund door blokkade in burgerzakenmodule. RAAS autorisatiebeheer, gecontroleerd door een ABR. Vaste werkprocedures bij aanvraag met vermissing en verificatie oude document inclusief handtekening en foto. Aanpak en voorkóming van fraude is en blijft een prioriteit bij alle werkzaamheden binnen burgerzaken, vastgelegd in werkprocessen die geen onderdeel van de VIC vormen.
Gemiddeld	Fraude met opbrengsten: Medewerker ontvreemdt leges per kas betaald voor reisdocument	AO/IC: Functiescheiding: Leges worden bij de aanvraag voldaan; er wordt dagelijks een omzet-overzicht inclusief (kascontrole en) verschillenoverzicht gemaakt van de aantallen aangevraagde reisdocumenten en de ontvangen leges. Dit wordt per locatie digitaal vastgelegd, waardoor inzichtelijk is wat de reden én afhandeling is van geconstateerde verschillen in aantal aanvragen en betalingen. Wanneer bij hoge uitzondering later wordt betaald, wordt dit verantwoord en vastgelegd. Een nieuw document wordt pas uitgereikt nadat de betaling is voldaan.

8.2 Aanwezige beheersmaatregelen (10/10)

Frauderisico (bruto)	Onderwerp/ risico	Beheersmaatregelen
Gemiddeld	Frauduleuze betalingen (1): Medewerker maakt uitkeringen voor zichzelf aan of verandert het IBAN in het uitkeringensysteem.	AO/IC: Functiescheiding in aanmaken uitkering en betaalbaarstelling/aanmaak crediteuren, IC autorisaties SAM, IC betalingen > € 1.500, collegiaal fiatteren uitkering (optioneel). VIC: Controle bestaan werking van de IC autorisaties SAM en IC betalingen > € 1.500. Gezien restrisico's is eind 2023 besloten functiescheiding te gaan aanbrengen in het muteren van bankrekeningnummers in het uitkeringssysteem. Zodra dit is ingericht, zal de werking van deze functiescheiding onderdeel worden van de VIC.
Gemiddeld	Fraude met declaraties/ vergoedingen: Medewerker dient declaratie in voor niet gemaakte kosten of privé kosten / dient onterecht thuiswerkvergoedingsverzoek in	AO/IC declaraties: Controle zit in elektronische processtappen en daadwerkelijke inhoudelijke controle van manager en medewerker Salarisadministratie. Elke declaratie dient te worden voorzien van een bewijsstuk cf. regelgeving en/of gemaakte afspraken en geaccordeerd door de manager. Uitbetaling vindt plaats bij het reguliere salaris. AO/IC declaraties thuiswerkvergoeding: Ook deze dienen elektronisch te worden ingediend, geaccordeerd door de manager en er is sprake van uitbetaling bij het reguliere salaris. Indien er een afwijkende vergoeding van bijvoorbeeld het thuiswerken op een roostervrije dag wordt aangevraagd, dan verschijnt een pop-up-scherm voor de werknemer, dat kan worden weggeklikt. Dit pop-up-scherm is voor de manager niet zichtbaar. Er bestaat momenteel geen efficiënte en effectieve controlemogelijkheid op de regel dat op één dag enkel een thuiswerkvergoeding òf een reiskostenvergoeding mag worden aangevraagd. HRM betwijfelt of de accordering van de aanvraag door de manager een effectieve beheersmaatregel is en beraadt zich momenteel op een effectiever beheersmaatregel. Het nieuwe personeelssyteem biedt in dit kader meer mogelijkheden. Momenteel is alleen sprake van losse controles op basis van overzichten die de PSA-coördinator opstelt voor managers. VIC: Op bestaan en werking van de AO/IC heeft VIC plaats.

8.3 Analyse

Aanvullende maatregelen voor gebieden met een verhoogd restrisico

Voor wat betreft de frauderisico's met een hoog (netto) restrisico is onderzocht welke aanvullende beheersmaatregelen wenselijk zijn om het restrisico verder te beperken, naast de al bestaande beheersmaatregelen. Bewaking van opvolging van aanvullende maatregelen vindt plaats via de reguliere VIC-cyclus.

Onderwerp / risico (netto)	Beheersmaatregelen	Risico-eigenaar
Onvoldoende opvolging van maatregelen bij leveranciers	Leveranciersmanagement (waaronder sturen op ISAE3402, ISO27001, SOC en right to audit).	Eigenaren van applicaties (ondersteund door cluster Info+)
Frauduleuze betalingen	Onder handen: Aanscherping Budgethoudersregeling, Duiding mandaten inhuur, Meer aandacht voor aandachtspunten uit de VIC m.b.t. Budgethoudersregeling en Mandaatregeling (o.a. rolverdeling en mandaten inhuur) en softcontrols, Richtlijnen documentatie prestatielevering, Onderzoek mogelijkheden efficiënte It-control(s) in het aan te schaffen financieel systeem. Opties (aanbevelingen VIC Inkoopfacturen): Aanscherping mandaten (autorisaties MijnBNG), Duiding governance m.b.t. en bij samenwerkingsverbanden, Onderzoek mogelijkheden efficiënte It-control(s) in huidige financiële en zaak- en archiefsysteem.	Clustermanager Financiën