GGD regio Utrecht

Interne frauderisicoanalyse

2027

Interne frauderisicoanalyse 2027 1
Inhoudsopgave 2
Inleiding 3
1. Frauderisicobeheersing 4
1.1 Kadernota Rechtmatigheid 4
1.2 Vormen van fraude 5
1.3 Twee belangrijke vormen van fraude 6
1.4 Bestuursstructuur 7
1.4.1 Verantwoordelijkheden Dagelijks Bestuur 7
1.4.2 Rol Algemeen Bestuur 8
1.5 Frauduleuze financiële verslaggeving 8
1.5.1 Risico's frauduleuze financiële verslaggeving 8
1.5.2 Preventieve maatregelen frauduleuze financiële verslaggeving 9
1.6 Oneigenlijke toe-eigening van bedrijfsmiddelen 9
1.6.1 Risico's toe-eigening bedrijfsmiddelen 9
1.6.2 Preventieve maatregelen toe-eigening bedrijfsmiddelen 10
1.7 Wet Bibob 11
1.8 Governance fraude 12
1.8.1 Misbruik en oneigenlijk gebruik in relatie tot fraude 14
2. Frauderisicoanalyse 15
2.1 Elementen frauderisicoanalyse 15
2.1 Fraudedriehoek 15
2.2 Frauderisico's 17
2.3 Het inschatten van risico's 17
2.4 Prioriteren van risico's 18
2.5 Interne beheersmaatregelen 18
2.6 Restrisico 19
2.7 Risico-acceptatie 19
3. Belangrijkste conclusies en aanbevelingen 20
3.1 Frauduleuze financiële verslaggeving 20
3.1.1 Conclusies 20
3.1.2 Aanbevelingen 22
3.2 Oneigenlijke toe-eigening van bedrijfsmiddelen 23
3.2.1 Conclusies 23
3.2.2 Aanbevelingen 26
Bijlage Interne frauderisicoanalyse 28
1.1 Structuur van de tabel 28
1.2 Onderdelen 29
1.3 Acties voor verbetering 30
1.4 High level inschatting 31
1.5 Tabel Frauderisicoanalyse 32

Inleiding

Fraude is een van de grootste bedreigingen voor de integriteit en betrouwbaarheid van organisaties. In de huidige complexe en snel veranderende omgeving is het cruciaal voor GGDrU om zich bewust te zijn van de verschillende vormen van fraude en de bijbehorende risico's. Dit document biedt een gedetailleerde uiteenzetting van de fraudestructuur en -risico's binnen de organisatie, met een specifieke focus op de beheersing van deze risico's.

In het eerste hoofdstuk worden de kaders van rechtmatigheid en de vormen van fraude besproken, evenals de verantwoordelijkheden van het Dagelijks Bestuur, het Algemeen Bestuur en het Directieteam. Hierin worden ook specifieke risico's gerelateerd aan frauduleuze financiële verslaggeving en de oneigenlijke toe-eigening van bedrijfsmiddelen belicht, evenals de preventieve maatregelen die getroffen kunnen worden om deze risico's te mitigeren.

Vervolgens wordt in het tweede hoofdstuk de frauderisicoanalyse gepresenteerd. Deze analyse omvat de belangrijke elementen van de fraudedriehoek, de identificatie en prioritering van risico's, en de evaluatie van interne beheersmaatregelen. Daarnaast wordt het concept van restrisico en de acceptatie van risico's besproken, wat essentieel is voor een realistische benadering van fraudepreventie.

Ten slotte worden in het derde hoofdstuk de belangrijkste conclusies en aanbevelingen gepresenteerd, die zijn gericht op het versterken van de interne controles en het bevorderen van een cultuur van integriteit binnen GGDrU. Deze aanbevelingen zijn van cruciaal belang om de risico's van frauduleuze activiteiten te beheersen en de transparantie en integriteit van de organisatie te waarborgen.

1. Frauderisicobeheersing

De verantwoordelijkheid voor het voorkomen en vroegtijdig opsporen van fraude ligt primair bij het Dagelijks Bestuur van GGDrU. In lijn met de bepalingen van de Gemeentewet, met name artikel 160 en artikel 212, is er een sterke focus op preventie. Het nemen van effectieve maatregelen is cruciaal om de kansen op frauduleuze handelingen te verkleinen. Hierdoor worden niet alleen de mogelijkheden voor fraude beperkt, maar worden individuen ook ontmoedigd om frauduleuze activiteiten te ontplooien, aangezien de kans op ontdekking en bestraffing aanzienlijk is. Deze aanpak sluit aan bij de bredere bestuurlijke verantwoordelijkheid om de integriteit van de organisatie te waarborgen en fraude actief te bestrijden.

Toelichting:

1. *Artikel 160 van de Gemeentewet: Dit artikel legt de verantwoordelijkheden van het dagelijks bestuur vast, waaronder het beheer van eigendommen en financiën binnen de gemeenschappelijke regeling. Deze bevoegdheden spelen een cruciale rol in het voorkomen van fraude door het waarborgen van goed toezicht en beheer;*

2. *Artikel 212 van de Gemeentewet: Dit artikel verplicht de gemeenschappelijke regeling om financiële verordeningen vast te stellen die gericht zijn op een doelmatig en integer beheer van middelen. Deze regelgeving staat in direct verband met fraudepreventie en draagt bij aan het creëren van een transparante en verantwoorde financiële omgeving.*

1.1 Kadernota Rechtmatigheid

De **Kadernota Rechtmatigheid**, opgesteld door de commissie Besluit Begroting en Verantwoording (commissie BBV), adviseert om geconstateerde fraude, vooral die wordt gepleegd door eigen medewerkers, op te nemen in de paragraaf bedrijfsvoering.

Fraude wordt gedefinieerd als: *"Opzettelijke handelingen door één of meerdere personen binnen de gemeenschappelijke regeling, waarbij misleiding wordt gebruikt om een onrechtmatig voordeel te behalen."*

Bij financieel significante fraude is het van essentieel belang dat deze incidenten worden gerapporteerd aan de governance-verantwoordelijken binnen de organisatie. Deze personen zijn verantwoordelijk voor het toezicht op de juistheid en betrouwbaarheid van de financiële verslaglegging en de effectiviteit van interne controles.

De externe accountant is ook verplicht om fraudegevallen op te nemen in de getrouwheidsverklaring. Deze verklaring bevestigt de juistheid en betrouwbaarheid van de financiële informatie en signaleert eventuele afwijkingen of onregelmatigheden.
Het is belangrijk op te merken dat frauduleuze handelingen niet onder de rechtmatigheidsverantwoording vallen. Dit betekent dat er geen wettelijke verplichting is om

deze gevallen in de officiële rapportage op te nemen. Dit benadrukt de noodzaak van transparantie en het waarborgen van verantwoordelijkheidsstructuren, zelfs wanneer er geen wettelijke verplichting bestaat.

Voor GGDrU biedt de Kadernota de mogelijkheid om vrijwillig fraudezaken en de getroffen maatregelen in de jaarstukken te vermelden. Dit zou bijdragen aan meer transparantie en het versterken van de interne controles binnen de organisatie. Het openlijk bespreken van fraude in de jaarstukken kan ook het vertrouwen bij stakeholders bevorderen en de effectiviteit van de governance waarborgen.

Deze aanpak sluit aan bij de frauderisicoanalyse van GGDrU. Door fraudegevallen te rapporteren en te analyseren, kan de organisatie:’

- **Interne controles versterken**: De effectiviteit van controles evalueren en verbeteren;
- **Cultuur van transparantie bevorderen**: Openheid en integriteit stimuleren, wat het vertrouwen opbouwt;
- **Preventieve maatregelen treffen**: Gerichte acties ondernemen om toekomstige frauderisico's te minimaliseren.

1.2 Vormen van fraude

Volgens het **Van Dale Groot woordenboek van de Nederlandse taal** wordt fraude gedefinieerd als: *"Bedrog, gepleegd door vervalsing van administratie."*

De term "fraude" heeft geen expliciete wettelijke definitie. Dit betekent dat er geen specifieke wet is die de term precies omschrijft. In plaats daarvan dient fraude als een overkoepelende term die verschillende (strafrechtelijke) handelingen omvat die verband houden met bedrog, misleiding of onrechtmatige winst. Voorbeelden zijn oplichting, valsheid in geschrifte en misbruik van vertrouwen.

Binnen GGDrU zijn er verschillende vormen van fraude die aanzienlijke risico's met zich meebrengen. Deze risico's kunnen niet alleen de financiële integriteit van de organisatie aantasten, maar ook het vertrouwen van de gemeenschap en de overheid ondermijnen.

Hieronder worden enkele belangrijke fraudevormen toegelicht, specifiek gericht op GGDrU:

1. **Betalen van valse facturen**: Dit betreft het indienen en betalen van facturen die opzettelijk zijn vervalst. Dit kan gebeuren met de betrokkenheid van één of meerdere medewerkers, bijvoorbeeld door fictieve leveranciers te creëren of bestaande facturen te manipuleren. Hierdoor kan GGDrU onterecht kosten worden aangerekend die nooit zijn gemaakt;
2. **Oneigenlijk gebruik van bedrijfsmiddelen**: Dit houdt in dat medewerkers bedrijfsmiddelen zoals medische apparatuur, kantoorbenodigdheden of creditcards verduisteren of ongeoorloofd gebruiken. Voorbeelden zijn privégebruik van dienstvoertuigen of kantoorartikelen, wat leidt tot financiële verliezen voor de organisatie;
3. **Fraude met belastingen en toeslagen**: Hierbij wordt opzettelijk onjuiste informatie verstrekt om onterecht belastingvoordelen of subsidies te verkrijgen. Bijvoorbeeld als

GGDrU subsidies aanvraagt op basis van valse gegevens over deelnemers aan gezondheidsprogramma's, wat kan resulteren in financiële sancties en reputatieschade;

4. **Misbruik van machtsposities**: Dit houdt in dat medewerkers ongeoorloofde gunsten verlenen aan derden in ruil voor wederdiensten. Dit kan leiden tot corruptie, zoals wanneer een medewerker een leverancier bevoordeelt in ruil voor persoonlijke voordelen, wat de integriteit van de inkoopprocessen van GGDrU ondermijnt;

5. **Fraude bij inkoop- en aanbestedingstrajecten**: Dit kan plaatsvinden wanneer verschillende partijen samenspannen om onrechtmatige voordelen te behalen. Dit ondermijnt de transparantie en eerlijkheid van het aanbestedingsproces van GGDrU, wat kan leiden tot overprijzen of kwaliteitsproblemen met ingekochte diensten of goederen;

6. **Cyberfraude**: Dit omvat activiteiten zoals phishing, spoofing en malwareverspreiding, gericht op het verkrijgen van toegang tot vertrouwelijke gegevens of financiële middelen van GGDrU. Cyberfraude kan ernstige gevolgen hebben, zoals datalekken en financiële schade;

7. **Greenwashing**: Dit betreft het misleiden van de gemeenschap door GGDrU zich duurzamer voor te stellen dan in werkelijkheid het geval is. Dit kan gebeuren door het presenteren van niet-bestaande of overdreven milieuvriendelijke initiatieven. Dit kan leiden tot verlies van vertrouwen bij stakeholders en juridische gevolgen.

1.3 Twee belangrijke vormen van fraude

In de accountancyregelgeving worden twee belangrijke vormen van fraude onderscheiden, die in deze frauderisicoanalyse centraal staan:

1. **Frauduleuze financiële verslaggeving**: Deze vorm van fraude houdt in dat financiële gegevens opzettelijk worden gemanipuleerd om een vertekend beeld te schetsen van de financiële situatie van een organisatie. Het doel kan variëren van het verbeteren van de zichtbaarheid van de organisatie tot het aantrekken van investeerders of het verkrijgen van leningen. De gevolgen van deze fraude zijn aanzienlijk, omdat ze de transparantie en betrouwbaarheid van financiële rapportages ondermijnen, wat kan leiden tot verlies van vertrouwen van belanghebbenden en mogelijk juridische repercussies. Daarom is het van groot belang om dit type fraude grondig te onderzoeken en te begrijpen;

2. **Oneigenlijke toe-eigening van bedrijfsmiddelen**: Dit betreft het ongeoorloofd gebruiken of toewijzen van bedrijfsmiddelen, zoals geld, goederen of apparatuur, tot het punt van diefstal of verduistering. Vaak worden deze handelingen ondersteund door valse documenten of onjuiste verklaringen, waardoor het moeilijker wordt om het frauduleuze gedrag te detecteren. Deze vorm van fraude komt vooral voor in operationele processen waar medewerkers toegang hebben tot bedrijfsmiddelen. De risico’s zijn aanzienlijk, vooral in situaties waar toezicht en controle tekortschieten. Het is cruciaal om een effectief beheer en controlemechanismen in te voeren om bedrijfsmiddelen te beschermen tegen misbruik.

De frauderisicoanalyse richt zich niet alleen op het identificeren van deze vormen van fraude, maar ook op het verkrijgen van diepgaand inzicht in preventieve maatregelen en controlemechanismen. Er wordt speciale aandacht besteed aan het herkennen van signalen die kunnen wijzen op mogelijke onregelmatigheden, evenals aan het implementeren van effectieve

strategieën om deze risico's te beheersen. Het uiteindelijke doel is om GGDrU in staat te stellen een robuust beleid te ontwikkelen dat de fraudepreventie versterkt en de integriteit van de financiële verslaggeving waarborgt.

1.4 Bestuursstructuur

De bestuursstructuur van GGDrU is van groot belang voor de frauderisicoanalyse. Effectieve governance en toezicht zijn essentieel om de financiële integriteit te waarborgen en frauderisico's te minimaliseren. De bestuursorganen van de gemeenschappelijke regeling dragen de primaire verantwoordelijkheid voor het voorkomen en ontdekken van fraude en onjuistheden.

Hieronder volgt een samenvatting van de relevante bestuursorganen:

1. **Algemeen Bestuur (AB)**:
   Het Algemeen Bestuur is het hoogste bestuursorgaan en is verantwoordelijk voor het vaststellen van beleid en toezicht op de uitvoering ervan. Hun betrokkenheid is essentieel voor het creëren van een cultuur van integriteit en transparantie, wat helpt bij het verminderen van frauderisico's;

2. **Dagelijks Bestuur (DB)**:
   Het Dagelijks Bestuur voert het beleid uit en zorgt voor de dagelijkse gang van zaken. Hun rol in het implementeren van controlemechanismen en risicobeheersing is cruciaal om fraude te voorkomen en tijdig te signaleren;

3. **Directieteam (DT)**:
   Het directieteam is verantwoordelijk voor de operationele leiding en de uitvoering van het beleid. Een sterke focus op interne controles en transparante financiële processen binnen de directie kan helpen om frauduleuze activiteiten te detecteren en te voorkomen.

1.4.1 Verantwoordelijkheden Dagelijks Bestuur

In de Gemeentewet zijn bepalingen opgenomen die de verantwoordelijkheden van het Dagelijks Bestuur duidelijk uiteenzetten. Deze verantwoordelijkheden zijn cruciaal voor het waarborgen van financiële integriteit en transparantie binnen de organisatie. Hieronder volgen de belangrijkste taken van het Dagelijks Bestuur:

1. **Implementeren van de strategie**: Het Dagelijks Bestuur is verantwoordelijk voor de uitvoering van de strategische plannen van de organisatie. Dit omvat het waarborgen van integriteit en transparantie in alle financiële rapportages;

2. **Beheren van risico's**: Het Dagelijks Bestuur moet risico's identificeren, evalueren en beheersen die kunnen leiden tot fraude of misbruik van middelen binnen de activiteiten van de gemeenschappelijke regeling;

3. **Opzetten van interne risicobeheersingssystemen**: Het bestuur dient effectieve interne controles en systemen te waarborgen die in staat zijn om risico's tijdig te signaleren en passende maatregelen te nemen;

4. **Naleven van wet- en regelgeving**: Het is essentieel dat de organisatie zich houdt aan relevante wetten en regels om juridische problemen en reputatierisico's te voorkomen;

5. **Integer handelen**: Het Dagelijks Bestuur moet ervoor zorgen dat alle beslissingen transparant en eerlijk worden genomen, zonder dat persoonlijke belangen de objectiviteit in gevaar brengen;

6. **Rapporteren aan het Algemeen Bestuur**: Transparante rapportage is van groot belang voor effectief toezicht. Het Dagelijks Bestuur moet regelmatig verslag doen aan het Algemeen Bestuur over de uitvoering van de strategie, risicobeheersing en naleving van wet- en regelgeving.

1.4.2 Rol Algemeen Bestuur

Het Algemeen Bestuur heeft een belangrijke kaderstellende en controlerende rol. Dit betekent dat het toezicht houdt op het beleid van het Dagelijks Bestuur en de organisatie. Het doel hiervan is om de kansen op fraude, corruptie en niet-integer gedrag te minimaliseren. Door middel van effectieve controles en evaluaties kan het Algemeen Bestuur bijdragen aan een cultuur van integriteit en transparantie binnen de organisatie.

1.5 Frauduleuze financiële verslaggeving

Frauduleuze financiële verslaggeving kan aanzienlijke gevolgen hebben voor GGDrU, zowel op financieel als op reputatiegebied. Het is essentieel om de belangrijkste risico's in deze context te begrijpen, omdat deze niet alleen de integriteit van de organisatie in gevaar kunnen brengen, maar ook het vertrouwen van stakeholders kunnen ondermijnen.

1.5.1 Risico's frauduleuze financiële verslaggeving

De belangrijkste risico's in deze context zijn:

1. **Manipulatie van financiële gegevens:**
   Bij GGDrU kan dit inhouden dat kosten voor medische voorraden of personeelsuitgaven opzettelijk worden gemanipuleerd. Dit leidt tot een vertekend beeld van de financiële gezondheid van de organisatie en kan het vertrouwen van de gemeenschap ondermijnen;

2. **Onjuiste rapportage:**
   Het verstrekken van een verkeerd beeld van de financiële positie kan ervoor zorgen dat belangrijke beslissingen, zoals budgetallocaties voor zorgprogramma's of publieke gezondheidscampagnes, worden genomen op basis van onjuiste informatie. Dit kan ernstige gevolgen hebben voor de effectiviteit van de dienstverlening en de gezondheid van de gemeenschap;

3. **Belangenverstrengeling:**
   Beslissingen die niet in het belang van GGDrU zijn, kunnen schadelijk zijn. Bijvoorbeeld, als medewerkers betrokken zijn bij inkoopprocessen waarbij persoonlijke belangen spelen, kan dit leiden tot inefficiënte uitgaven van publieke middelen en een verlies van vertrouwen van burgers en andere stakeholders;

4. **Onvoldoende interne controle:**
   Een gebrek aan toezicht en controlemechanismen binnen GGDrU kan frauduleuze activiteiten vergemakkelijken. Het is essentieel dat er adequate interne controles zijn,

zoals regelmatige audits en monitoring van financiële processen, om afwijkingen tijdig te signaleren;

5. **Gebrek aan transparantie:**
   Onvoldoende openheid over financiële processen kan leiden tot wantrouwen van het publiek en andere belanghebbenden. GGDrU moet ervoor zorgen dat financiële rapportages helder en toegankelijk zijn, zodat belanghebbenden inzicht hebben in hoe publieke middelen worden beheerd en besteed.

Elk van deze risico's kan aanzienlijke gevolgen hebben voor GGDrU, waaronder schade aan de reputatie, juridische complicaties en financiële verliezen.

1.5.2 Preventieve maatregelen frauduleuze financiële verslaggeving

Door proactief maatregelen te treffen om deze risico's te identificeren en te beheersen, kan GGDrU haar financiële integriteit waarborgen en het vertrouwen van de gemeenschap versterken. Dit kan onder andere de volgende acties inhouden:

- **Implementatie van sterke interne controles**: Regelmatige audits, gescheiden verantwoordelijkheden en duidelijke procedures zijn cruciaal voor het waarborgen van de financiële integriteit;

- **Bevordering van een cultuur van ethisch gedrag**: Trainingen voor medewerkers over integriteit en ethisch handelen zijn noodzakelijk om een omgeving te creëren waarin fraude en onethisch gedrag niet worden getolereerd;

- **Waarborging van transparantie**: GGDrU moet open communiceren over haar financiële processen en besluitvorming om het vertrouwen van de gemeenschap en andere belanghebbenden te behouden.

Door deze proactieve maatregelen te nemen, kan GGDrU niet alleen de financiële integriteit waarborgen, maar ook het vertrouwen van de gemeenschap versterken.

1.6 Oneigenlijke toe-eigening van bedrijfsmiddelen

Binnen GGDrU, waar medewerkers toegang hebben tot verschillende financiële middelen en andere bedrijfsmiddelen, zoals medische voorraden, apparatuur en vervoermiddelen, bestaat het risico op oneigenlijke toe-eigening. Dit houdt in dat medewerkers deze middelen onterecht voor persoonlijke doeleinden gebruiken. Dergelijke handelingen kunnen leiden tot financieel mismanagement en ondermijning van de organisatie.

1.6.1 Risico’s toe-eigening bedrijfsmiddelen

Voorbeelden van dergelijke praktijken zijn onder andere:

1. **Verduistering van vaccins of medische benodigdheden**: Medewerkers met toegang tot voorraden van vaccins, medische apparatuur of beschermende middelen (zoals mondmaskers en handschoenen) kunnen deze ontvreemden of doorverkopen voor privégebruik. Dit is vooral risicovol tijdens schaarste, bijvoorbeeld tijdens pandemieën;

2. **Oneigenlijk gebruik van dienstauto's of andere vervoersmiddelen**: Medewerkers die dienstauto's gebruiken voor werkdoeleinden, zoals huisbezoeken, kunnen deze

voertuigen ook voor privéritten inzetten zonder toestemming, wat neerkomt op misbruik van bedrijfsmiddelen;

3. **Privégebruik van mobiele telefoons en andere apparaten die eigendom zijn van GGDrU**: Het gebruik van mobiele telefoons en andere apparaten, zoals tablets en laptops, die eigendom zijn van GGDrU voor persoonlijke doeleinden, bijvoorbeeld het versturen van privéberichten of het uitvoeren van niet-werkgerelateerde taken, kan ongemerkt gebeuren, vooral wanneer er geen strenge controles zijn op het gebruik van deze middelen;

4. **Onterechte declaratie van reis- en verblijfskosten**: Medewerkers die voor werk reizen of overnachten, kunnen privé-uitgaven onterecht opvoeren als zakelijke kosten, zoals maaltijden of hotels die niet werkgerelateerd zijn;

5. **Gebruik van kantoorartikelen voor thuisgebruik**: Medewerkers met toegang tot kantoorbenodigdheden (zoals papier en inkt) kunnen deze voor privédoeleinden gebruiken, wat bij herhaaldelijk gebruik kan leiden tot aanzienlijke verliezen;

6. **Verduistering van subsidie- of projectgelden**: Medewerkers die verantwoordelijk zijn voor het beheren van projectsubsidies en gelden voor gezondheidsprogramma's of onderzoek kunnen deze middelen onterecht toewijzen aan andere projecten of zelfs gedeeltelijk verduisteren, vooral bij gebrek aan toezicht;

7. **Misbruik van creditcards**: Medewerkers met een zakelijke creditcard voor werkgerelateerde uitgaven kunnen deze kaarten ook gebruiken voor privé-uitgaven, die vervolgens onterecht als zakelijke kosten worden gedeclareerd.

Daarnaast zijn er andere veelvoorkomende praktijken van oneigenlijke toe-eigening, zoals:

- **Diefstal van bedrijfsmiddelen**: Het wegnemen van tablets, mobiele telefoons, kantoorartikelen, medische verbruiksgoederen, of andere apparatuur voor persoonlijk gebruik;

- **Verduistering van geld**: Het onterecht aanwenden van contante middelen of budgetten voor persoonlijke uitgaven;

- **Valse declaraties**: Het indienen van onjuiste of gefingeerde onkostenvergoedingen voor niet-gemaakte uitgaven;

- **Misbruik van toegangsrechten**: Het gebruiken van toegang tot bedrijfsmiddelen zonder toestemming of buiten de zakelijke context.

Door specifiek aandacht te besteden aan deze risico's kan GGDrU de oneigenlijke toe-eigening van bedrijfsmiddelen voorkomen en de financiële integriteit van de organisatie waarborgen.

1.6.2 Preventieve maatregelen toe-eigening bedrijfsmiddelen

In een organisatie zoals GGDrU, waar publieke middelen worden beheerd en financiële integriteit cruciaal is voor het vertrouwen in de dienstverlening, is het essentieel om sterke interne controles te hanteren. Deze controles helpen zowel bij het voorkomen als het detecteren van frauduleuze activiteiten.

Preventieve maatregelen kunnen onder andere de volgende aspecten omvatten:

1. **Regelmatige inventariscontroles van medische voorraden**: Voer frequente controles uit op medische voorraden om discrepanties en ongeoorloofd gebruik tijdig te signaleren. Dit draagt bij aan de beschikbaarheid van essentiële middelen en zorgt ervoor dat alle producten en materialen correct zijn geregistreerd en verantwoord;

2. **Strenge procedures voor het gebruik van dienstvoertuigen en elektronische apparaten**: Stel duidelijke richtlijnen op voor het gebruik van dienstvoertuigen en elektronische apparatuur om oneigenlijk gebruik te voorkomen en de efficiëntie te waarborgen. Daarnaast moeten medewerkers zich bewust zijn van de gevolgen van misbruik;

3. **Duidelijke declaratieprotocollen met meerdere goedkeuringslagen**: Implementeer een systeem waarin declaraties door meerdere autoriteiten moeten worden goedgekeurd. Dit helpt onterechte claims en fraude te minimaliseren door extra controlemechanismen in te bouwen, en zorgt ervoor dat alleen geverifieerde en legitieme uitgaven worden vergoed;

4. **Zorgvuldige monitoring van subsidie- en projectgelden door externe controle**: Voer regelmatig externe audits uit om de juiste besteding van publieke middelen te waarborgen en financiële onregelmatigheden te identificeren. Dit zorgt voor transparantie en houdt de organisatie verantwoordelijk voor het gebruik van toegewezen middelen;

5. **Strikte procedures voor kasbeheer**: Hoewel het gebruik van contant geld steeds minder voorkomt, is het belangrijk om regelmatig de digitale kasstromen te controleren. Dit helpt afwijkingen tijdig op te sporen en de financiële integriteit te waarborgen. Bij verschillende afdelingen kan het gebruik van pinbetalingen leiden tot typefouten; zorg ervoor dat deze betalingen zorgvuldig worden gecontroleerd en geverifieerd met duidelijke registratieprocedures;

6. **Beperkte toegang tot bedrijfsmiddelen**: Verleen toegang tot kantoorartikelen en andere middelen alleen aan bevoegde medewerkers. . Voer regelmatige inventariscontroles uit om eventuele tekorten op te sporen en te zorgen voor een goede documentatie van de uitgifte en ontvangst van deze middelen;

7. **Strenge declaratie- en goedkeuringsprocedures**: Implementeer een meerlagig goedkeuringsproces voor onkostendeclaraties om ongeoorloofd gebruik van de financiële middelen van GGDrU te voorkomen, die bestemd zijn voor operationele kosten, investeringen en andere uitgaven. Dit proces vereist ook dat medewerkers relevante documentatie indienen en onregelmatigheden rapporteren.

Deze preventieve maatregelen zijn cruciaal voor het waarborgen van de financiële integriteit en de bescherming van publieke middelen binnen een organisatie als GGDrU. Hierdoor wordt de nadruk gelegd op monitoring, bewustwording en verantwoordelijkheid, waardoor de organisatie beter voorbereid is om oneigenlijke toe-eigening van bedrijfsmiddelen te voorkomen.

1.7 Wet Bibob

De **Wet Bibob** ((Wet bevordering integriteitsbeoordelingen door het openbaar bestuur) biedt GGDrU de mogelijkheid om de integriteit van de organisatie te waarborgen door proactief

onderzoek te doen naar de integriteit van zakenpartners, zoals leveranciers of opdrachtnemers. Hiermee kan worden voorkomen dat GGDrU onbewust samenwerkt met partijen die betrokken zijn bij criminele activiteiten, wat essentieel is voor het verantwoord beheer van publieke middelen. Daarnaast helpt de wet het risico op reputatieschade te minimaliseren en bevordert het transparante en ethische besluitvorming binnen de organisatie.

Hieronder worden enkele belangrijke aandachtspunten verder toegelicht:

- **Integriteitsbeoordeling**: De Wet Bibob stelt GGDrU in staat om de integriteit van subsidie- en vergunningaanvragers te toetsen. Dit is cruciaal om samenwerkingen met risicovolle partijen te vermijden;

- **Voorkomen van misbruik**: Met de Bibob kan GGDrU ervoor zorgen dat overheidsgelden niet worden misbruikt door externe partijen met ongepaste doeleinden. Dit bevordert de bescherming van publieke middelen;

- **Bevordering van vertrouwen**: Integriteitsbeoordelingen versterken het vertrouwen van de gemeenschap in GGDrU en garanderen burgers dat hun belastinggeld op een ethische manier wordt beheerd;

- **Verantwoordelijkheden**: De wet benadrukt de verantwoordelijkheid van GGDrU om een effectief risicobeheerbeleid te ontwikkelen. Dit omvat duidelijke criteria en procedures voor het beoordelen van aanvragen;

- **Samenwerking met andere overheden**: De Wet Bibob biedt een uniform kader voor integriteitsbeoordelingen en fraudepreventie, wat de samenwerking met andere gemeenten en provincies vergemakkelijkt;

- **Preventieve maatregelen**: De Wet Bibob kan deel uitmaken van een breder pakket aan preventieve maatregelen van GGDrU, gericht op het minimaliseren van zowel interne als externe fraude- en misbruikrisico's.

1.8 Governance fraude

In het rapport **'Deloitte Gemeente Governance Fraude'** uit 2007 worden belangrijke aspecten van governancefraude besproken die de integriteit en rechtmatigheid van gemeenten ondermijnen. Dit onderwerp is ook van groot belang voor GGDrU, omdat de organisatie, als publieke gezondheidsinstelling, vergelijkbare risico's tegenkomt. De bevindingen van het rapport benadrukken de noodzaak voor GGDrU om alert te zijn en effectieve maatregelen te nemen ter bescherming van de integriteit van haar processen en middelen.

Governancefraude verwijst naar frauduleuze activiteiten binnen de governance-structuur van een organisatie. Deze fraude vormt een directe bedreiging voor goed bestuur, transparantie en integriteit. Het kan verschillende vormen aannemen, zoals belangenverstrengeling, misbruik van macht of verduistering van middelen.

Om deze risico's te beheersen, is het essentieel om mogelijke frauduleuze handelingen proactief te identificeren en te mitigeren. Een frauderisicoanalyse is hierbij een waardevol instrument; het helpt om kwetsbare processen en functies binnen de organisatie systematisch in kaart te brengen. Door deze analyse te combineren met de **Wet Bibob**, kan GGDrU niet alleen de integriteit van zakenpartners waarborgen, maar ook de interne risico's op governancefraude effectief aanpakken. Beide maatregelen dragen bij aan het creëren van een integere en transparante werkomgeving.

Governancefraude omvat verschillende belangrijke aspecten, waaronder:

1. **Definitie**: Governance fraude omvat opzettelijke misleiding of manipulatie door bestuursleden, management of andere functionarissen binnen een organisatie. Dit kan resulteren in onrechtmatige voordelen voor individuen of groepen, ten koste van de organisatie;

2. **Voorbeelden**:

    - **Frauduleuze financiële verslaglegging**: Dit betreft het opzettelijk vervalsen van financiële documenten om een gunstiger financieel beeld van de organisatie te presenteren dan werkelijkheid is;

    - **Misbruik van macht**: Dit kan onder meer inhouden dat ongeoorloofde gunsten worden verleend aan vrienden of familie, of het onterecht gebruik van bedrijfsresources, zoals personeel, financiële middelen en technologie;

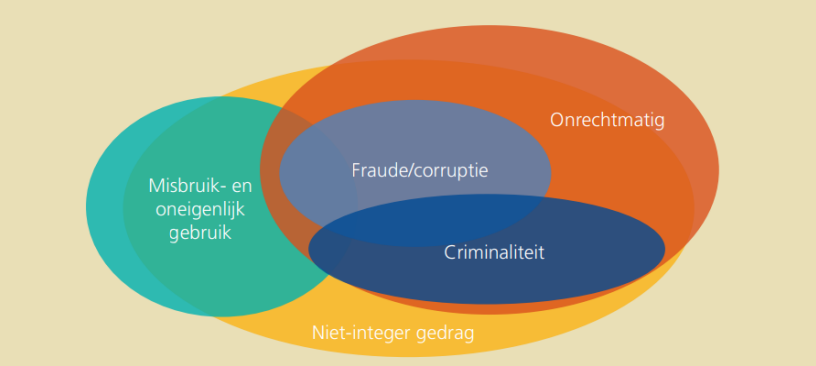
    - **Corruptie**: Het bieden of aannemen van steekpenningen om zakelijke beslissingen te beïnvloeden;

3. **Impact**: Governance fraude kan ernstige gevolgen hebben, waaronder reputatieschade, juridische sancties en financiële verliezen. Het kan ook het vertrouwen van stakeholders, zoals medewerkers en de gemeenschap, ondermijnen;

4. **Preventie**: Om governance fraude te voorkomen, moeten organisaties sterke interne controles, transparante processen en ethische richtlijnen implementeren. Het bevorderen van een cultuur van integriteit en verantwoordelijkheid is hierbij cruciaal;

5. **Relevantie voor publieke organisaties**: In de context van publieke instellingen, zoals overheden en gemeenschappelijke regelingen, is governance fraude bijzonder zorgwekkend. Het kan leiden tot misbruik van publieke middelen en vermindert het vertrouwen van het publiek in de overheid.

In de figuur hieronder uit het rapport 'Deloitte Gemeente Governance Fraude' uit 2007 wordt een helder onderscheid gemaakt tussen verschillende termen die betrekking hebben op onrechtmatig gedrag binnen organisaties. Deze figuur laat zien hoe concepten zoals misbruik en oneigenlijk gebruik, fraude en corruptie, onrechtmatig handelen, criminaliteit en niet-integer gedrag met elkaar zijn verbonden:



Figuur 1: **Onderscheid diverse begrippen**

Deloitte Gemeente Governance Fraude uit 2007

Voor GGDrU zijn termen zoals transparantie, ethiek en verantwoordelijkheidsbesef van groot belang, omdat ze de integriteit en rechtmatigheid van de organisatie ondermijnen. Wanneer deze principes worden geschonden, kan dit leiden tot wantrouwen onder stakeholders, verlies van reputatie en zelfs juridische gevolgen hebben, wat de effectiviteit en het vertrouwen in de organisatie in gevaar brengt:

1. **Misbruik en oneigenlijk gebruik**: Dit verwijst naar het onterecht aanwenden van publieke middelen door externe partijen, zoals burgers, leveranciers of gemeenten, die gebruikmaken van de diensten van GGDrU. Dit kan leiden tot verspilling van overheidsgelden en ondermijnt het vertrouwen in de organisatie;

2. **Fraude en corruptie**: Deze begrippen hebben betrekking op opzettelijke misleiding door interne medewerkers of bestuursleden van GGDrU, gericht op het verkrijgen van persoonlijke of financiële voordelen. Dit kan schadelijk zijn voor de transparantie en integriteit van de organisatie;

3. **Onrechtmatig handelen**: Dit omvat handelingen die in strijd zijn met de geldende wet- en regelgeving voor GGDrU, wat kan leiden tot juridische consequenties en reputatieschade;

4. **Criminaliteit**: Hoewel GGDrU zich voornamelijk richt op publieke gezondheid, kan het ook te maken krijgen met strafbare feiten, zoals diefstal of verduistering van middelen. Dit kan de operationele effectiviteit en geloofwaardigheid van de organisatie schaden;

5. **Niet-integer gedrag**: Dit betreft gedragingen die de ethische normen van GGDrU ondermijnen. Dit kan de relatie met belanghebbenden, zoals gemeenten en burgers, negatief beïnvloeden en het vertrouwen in de organisatie aantasten.

1.8.1 Misbruik en oneigenlijk gebruik in relatie tot fraude

Een belangrijk aspect van de rechtmatigheidsverantwoording van GGDrU betreft misbruik en oneigenlijk gebruik. Dit verwijst naar de onrechtmatige inzet van overheidsgelden voor niet-bestemde doeleinden, vaak door externe partijen zoals burgers, leveranciers en gemeenten. Dit risico kan leiden tot financiële verliezen en een verminderd vertrouwen in de organisatie. Daarom is het cruciaal om effectieve maatregelen te nemen voor risicobeheersing en transparante inzet van middelen.

Fraude daarentegen betreft handelingen van bestuursleden of medewerkers binnen de organisatie. Het onderscheid tussen interne (fraude) en externe (misbruik en oneigenlijk gebruik) is belangrijk, omdat het helpt bij het ontwikkelen van beleid en controlemechanismen. Hierdoor kunnen gerichte maatregelen worden genomen om zowel interne als externe risico's te beheersen, wat bijdraagt aan de integriteit van de organisatie en het vertrouwen van de gemeenschap versterkt.

Omdat misbruik en oneigenlijk gebruik op bijna alle beleidsterreinen kunnen voorkomen, is het van essentieel belang dat er doeltreffende preventieve en corrigerende maatregelen zijn. Voor gedetailleerde informatie over het beleid verwijzen wij naar de nota "Misbruik en Oneigenlijk Gebruik," die de onderliggende filosofie, uitgangspunten en risicoanalyses beschrijft.

2. Frauderisicoanalyse

Het is essentieel dat GGDrU zich bewust is van de mogelijke frauderisico's en dat er effectieve maatregelen worden genomen om deze te identificeren en aan te pakken. Door sterke interne controles, transparante processen en een cultuur van ethisch gedrag te bevorderen, kan de organisatie de kans op fraude aanzienlijk verminderen en haar financiële integriteit waarborgen.

2.1 Elementen frauderisicoanalyse

Hieronder volgt een toelichting op de belangrijkste elementen van de frauderisicoanalyse, zoals weergegeven in de tabel:

1. **Frauderisicoanalyse**: Dit is een systematische methode om de risico's van fraude te identificeren en te begrijpen, evenals de interne beheersmaatregelen die zijn ingesteld om deze risico's te beheersen of te minimaliseren;

2. **In kaart brengen van frauderisico's**: De analyse helpt bij het vaststellen van specifieke risico's die kunnen leiden tot fraude, met name in relatie tot de activiteiten en processen van GGDrU;

3. **Bijlage**: Dit gedeelte van het document bevat een gedetailleerde tabel die de belangrijkste factoren die bijdragen aan frauderisico's opsomt. Deze factoren zijn relevant voor de specifieke activiteiten en processen van GGDrU;

4. **Inzicht in frauderisico's**: De tabel biedt duidelijkheid over welke specifieke risico's binnen de organisatie aanwezig zijn en hoe deze verband houden met verschillende processen;

5. **Interne beheersmaatregelen**: Voor elk geïdentificeerd risico worden de maatregelen vermeld die zijn getroffen om het risico te beheersen. Dit kan bestaan uit procedures, controles of richtlijnen die zijn ingesteld om fraude te voorkomen of op te sporen;

6. **Periodieke evaluatie**: De frauderisicoanalyse is geen eenmalige gebeurtenis. Het is belangrijk om deze analyse regelmatig te evalueren en bij te werken, zodat deze relevant blijft in het licht van veranderingen binnen de organisatie of haar activiteiten.

2.1 Fraudedriehoek

De frauderisicoanalyse kan effectief worden versterkt door het concept van de fraudedriehoek. Deze driehoek biedt inzicht in de typische kenmerken en gedragspatronen van fraudeurs, waardoor risico’s beter te identificeren en begrijpen zijn.

De fraudedriehoek, ontwikkeld door criminoloog Donald Cressey in 1953, stelt dat drie elementen essentieel zijn voor het ontstaan van fraude: druk, gelegenheid en rationalisatie.

Deze elementen worden als volgt gedefinieerd:

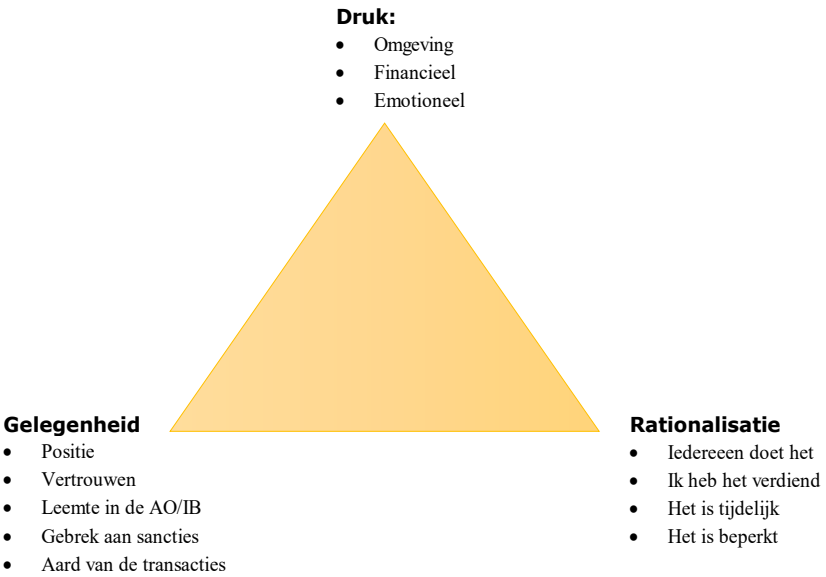
- **Druk**: Dit verwijst naar de motivatie of druk die iemand voelt om te frauderen, zoals financiële problemen of persoonlijke crises;

- **Gelegenheid**: Dit betreft de omstandigheden die iemand in staat stellen om fraude te plegen, bijvoorbeeld zwakke interne controles of gebrek aan toezicht;

- **Rationalisatie**: Dit is het proces waarbij een fraudeur zijn of haar handelingen rechtvaardigt, bijvoorbeeld door te denken dat het 'voor een goed doel' is of dat niemand erdoor zal worden benadeeld.

De afbeelding hieronder illustreert de samenhang tussen deze drie elementen. Door de fraudedriehoek te integreren in de frauderisicoanalyse kan GGDrU effectievere maatregelen ontwikkelen om fraude te voorkomen en op te sporen.

De fraudedriehoek



De afbeelding toont de drie essentiële factoren die samenkomen voor het plegen van fraude:

1. **Druk**: De fraudeur ervaart een stimulans om te frauderen, zoals financiële problemen, een luxe levensstijl, of de ambitie om een promotie te behalen;

2. **Gelegenheid**: De fraudeur heeft de mogelijkheid om te frauderen, vaak door tekortkomingen in de interne beheersing, zoals een zwakke administratieve organisatie en onvoldoende interne controle;

3. **Rationalisatie**: De fraudeur rechtvaardigt zijn of haar handelen, bijvoorbeeld door te denken: "Ik heb er recht op" of "Het valt wel mee."

De meeste fraudegevallen ontstaan door druk, maar de gelegenheid speelt ook een cruciale rol. Veel fraudeurs worden gestimuleerd door zwakke interne controles, zoals onvoldoende scheiding van taken of onduidelijke procedures. De rationalisatie hangt samen met de organisatiecultuur en het voorbeeldgedrag van het management, wat zowel positief als negatief kan zijn. Terwijl druk en rationalisatie sterk afhankelijk zijn van de individuele

fraudeur, kan de organisatie vooral de gelegenheid beïnvloeden door sterke interne controles en duidelijke procedures in te voeren.

2.2 Frauderisico's

In de frauderisicoanalyse worden verschillende frauderisico's gecategoriseerd op basis van hoofdthema's. Voor elk risico wordt een duidelijke definitie gegeven.

Een risico verwijst naar een mogelijke gebeurtenis die gevolgen kan hebben voor de doelstellingen van de organisatie. Frauderisico's zijn echter bijzonder omdat ze drie specifieke kenmerken hebben:

1. **Opzettelijke handeling**: De fraudeur handelt bewust en met opzet;
2. **Misleiding**: Er wordt bedrog of misleiding gebruikt om de fraude te verbergen;
3. **Onrechtmatig voordeel**: Het uiteindelijke doel is het verkrijgen van een onterecht voordeel.

Frauderisico's vormen niet alleen een bedreiging voor het behalen van de organisatiedoelstellingen, maar kunnen ook leiden tot aanzienlijke reputatieschade en juridische gevolgen.

Door proactief na te denken over de mogelijke risico's waarmee GGDrU te maken kan krijgen, kan de organisatie maatregelen nemen om deze risico's te voorkomen of de impact ervan te minimaliseren.

2.3 Het inschatten van risico's

De risicografiek (zie afbeelding hieronder) biedt een overzicht van de kans dat een risico zich voordoet en de impact ervan als het zich daadwerkelijk voordoet. De x-as toont de waarschijnlijkheid van het risico, terwijl de y-as de omvang van de impact weergeeft. In de rechterbovenhoek van de grafiek bevinden zich de risico's die zowel een hoge kans van optreden hebben als een grote impact wanneer ze zich voordoen.

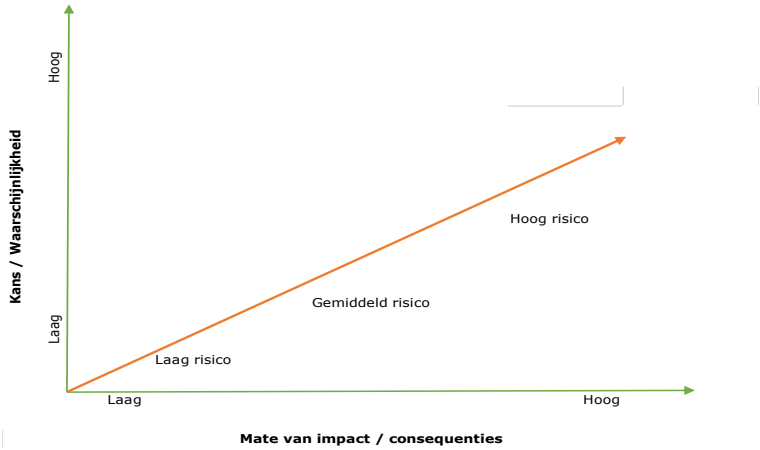
Een risico is een gebeurtenis die zich kan voordoen en die, indien dat gebeurt, invloed heeft op de doelstellingen van de organisatie. Risico's omvatten daarom twee belangrijke elementen:

- **De kans dat het gebeurt**: Dit is de waarschijnlijkheid dat het risico zich daadwerkelijk voordoet;
- **De grootte van de impact**: Dit verwijst naar de ernst van de gevolgen die het risico met zich meebrengt als het zich voordoet.

Voor de beoordeling van de waarschijnlijkheid van een risico is een score toegekend: hoog risico (H), gemiddeld risico (M) of laag risico (L). Daarnaast is voor elk risico de impact ingeschat, met classificaties als laag, gemiddeld of hoog.

Deze inschatting van risico's is gemaakt zonder rekening te houden met bestaande beheersmaatregelen en is dus niet gebaseerd op meetbare feiten.

De risicografiek



2.4 Prioriteren van risico's

Op basis van de inschatting van zowel de kans als de impact van een risico, wordt elk risico gewogen. Dit helpt ons te bepalen hoe we met het betreffende risico moeten omgaan. Met de risicomatrix (zie afbeelding hieronder) kunnen we de risico's met de hoogste prioriteit identificeren. Dit zijn in ieder geval de risico's die zowel een grote impact als een hoge waarschijnlijkheid hebben. Risico's met een lage kans van optreden, maar die wel een grote impact kunnen veroorzaken, verdienen ook aandacht.

Niet elk frauderisico uit de analyse is even waarschijnlijk of heeft een grote financiële impact. Hoe groter de kans dat een risico zich voordoet en hoe ernstiger de financiële gevolgen, des te belangrijker het is om dit risico te beheersen. Door een kleurenschema te hanteren (rood, geel of groen) wordt duidelijk welke risico's meer aandacht vereisen en welke minder significant zijn.

De risicomatrix

Kans / Waarschijnlijkheid			
Hoog	Gemiddeld	Hoog	Hoog
Gemiddeld	Laag	Gemiddeld	Hoog
Laag	Laag	Laag	Gemiddeld
	Laag	Gemiddeld	Hoog
	Mate van impact / consequenties		

2.5 Interne beheersmaatregelen

Elke organisatie loopt het risico op fraude en moet daarom maatregelen treffen om deze risico's te beheersen. Door de specifieke frauderisico's voor GGDrU in kaart te brengen, kunnen we de noodzakelijke interne beheersmaatregelen vaststellen om ongewenste gebeurtenissen te verminderen of te voorkomen. Het is echter belangrijk om te beseffen dat interne beheersmaatregelen fraude nooit volledig kunnen uitsluiten.

In de frauderisicoanalyse (zie bijlage) is per frauderisico vastgesteld in hoeverre de bestaande interne beheersmaatregelen het risico afdekken. Frauderisico's worden zowel preventief als

detectief beheerd. Een voorbeeld van een preventieve maatregel is het vier-ogenprincipe bij betalingen. Een detectieve maatregel kan bijvoorbeeld het maandelijks controleren van gewijzigde bankrekeningnummers zijn, op basis van correspondentie met leveranciers.

De beheersmaatregelen kunnen fysiek, administratief en/of technisch zijn, zoals functiescheiding, het vier-ogenprincipe en het automatiseren van handmatige processen. Daarnaast zijn er ook minder tastbare maatregelen gericht op het stimuleren van gewenst gedrag, zoals de interne gedragscode, die duidelijk maakt wat er van medewerkers wordt verwacht. Verder bevat de klokkenluidersregeling richtlijnen voor het melden van vermoedens van misstanden binnen GGDrU.

2.6 Restrisico

Restrisico verwijst naar het risico dat overblijft nadat de bestaande beheersmaatregelen zijn toegepast. Het omvat de frauderisico's die niet door deze maatregelen zijn afgedekt.

Het Dagelijks Bestuur is verantwoordelijk voor het classificeren van deze restrisico's op basis van hun impact en waarschijnlijkheid. Als blijkt dat de kans op fraude bij een niet-afgedekt risico groot is of de impact significant, is het belangrijk om de beslissing om dit restrisico te accepteren opnieuw te overwegen.

Daarnaast is het Dagelijks Bestuur verantwoordelijk voor het implementeren van beheersmaatregelen en het inschatten van de restrisico's. Het is aan te raden dat de bevindingen over de acceptatie van deze restrisico's ter goedkeuring worden voorgelegd aan het Algemeen Bestuur, in het kader van hun toezichthoudende rol.

Volledige eliminatie van risico's is meestal niet haalbaar. Zelfs met effectieve beheersmaatregelen blijft er vaak een bepaald risico bestaan. Bovendien kan het in de praktijk moeilijk zijn om opzet aan te tonen, vaak door gebrekkige interne controles en een laag fraudebewustzijn. Dit kan leiden tot afwijkingen van processen zonder opzet. Daarom is het essentieel om voortdurend te investeren in fraudepreventie en het verbeteren van interne controles. Deze controles richten zich vooral op processen met in- en uitgaande geldstromen en helpen fouten en onjuistheden te voorkomen. De nadruk ligt hierbij op het controleren of medewerkers zich houden aan de gemaakte procesafspraken.

2.7 Risico-acceptatie

De frauderisico's die niet volledig worden afgedekt door de bestaande interne beheersmaatregelen worden geanalyseerd. Hierbij maken we een onderscheid tussen acceptabele en onacceptabele risico's. Als maatregelen voor een specifiek risico nog niet onmiddellijk of volledig zijn geïmplementeerd, kan het nodig zijn om dit risico tijdelijk te accepteren. De mate van acceptatie wordt hierbij beoordeeld.

Voor onacceptabele frauderisico's worden altijd aanvullende beheersmaatregelen getroffen. De grootste risico's bevinden zich vaak in de processen van inkoop, voorraadbeheer, kasbeheer en declaraties. Een belangrijk middel in de strijd tegen fraude is het aanbrengen van voldoende functiescheiding op kritische punten binnen deze processen.

De meeste kennis over mogelijke frauderisico's en interne beheersmaatregelen is aanwezig binnen de organisatie zelf. Het is echter ook van belang dat de externe accountant op de hoogte is van de uitgevoerde frauderisicoanalyse. De accountant kan beoordelen of deze analyse van voldoende kwaliteit is en aanbevelingen doen voor verbeteringen.

3. Belangrijkste conclusies en aanbevelingen

In dit hoofdstuk worden de belangrijkste conclusies en aanbevelingen gepresenteerd. Deze zijn gebaseerd op de eerder uitgevoerde frauderisicoanalyse en bieden inzicht in de huidige risico's binnen de organisatie. De aanbevelingen zijn gericht op het versterken van interne beheersmaatregelen, het verbeteren van processen en het bevorderen van een cultuur van integriteit.

Door deze stappen te volgen, kan GGDrU effectiever omgaan met risico's op frauduleuze activiteiten, zoals frauduleuze financiële verslaglegging en ongeoorloofde toe-eigening van bedrijfsmiddelen. Dit zal bijdragen aan het waarborgen van de integriteit en transparantie van de organisatie.

3.1 Frauduleuze financiële verslaggeving

3.1.1 Conclusies

Potentiële risicocategorieën

Gemiddeld tot hoog risico:

- **Veranderende wet- en regelgeving:** De frequent veranderende wetgeving creëert een kwetsbaarheid voor GGDrU, aangezien nieuwe eisen voor financiële verslaggeving snel moeten worden geïmplementeerd. Dit kan leiden tot verwarring en fouten in de rapportages;

- **Exploitatieverliezen:** De continuïteit van GGDrU komt onder druk te staan door exploitatieverliezen, wat het risico op negatieve financiële rapportages vergroot. Dit kan de geloofwaardigheid van de organisatie schaden en het vertrouwen van belanghebbenden verminderen;

- **Druk op het management:** De druk om financiële doelstellingen te behalen kan leiden tot compromissen in de kwaliteit en integriteit van financiële rapportages. Dit verhoogt de kans op frauduleuze praktijken en verkeerde informatieverstrekking;

- **Complexe transacties:** Bij ongebruikelijke of complexe transacties, vooral met gelieerde partijen, is het cruciaal om de economische waarde correct weer te geven. Fouten of misinterpretaties kunnen ernstige juridische en financiële gevolgen hebben;

- **Inschakeling van tussenpersonen:** Het inschakelen van tussenpersonen, zoals consultants of derde partijen, zonder duidelijke rechtvaardiging kan de effectiviteit van de geleverde diensten ondermijnen en leiden tot ondoorzichtige transacties. Dit vergroot de kans op corruptie en fraude;

- **Interne beheersing:** Onvoldoende toezicht en het inzetten van onervaren medewerkers verhogen de kans op fouten en onregelmatigheden in de financiële verslaggeving, wat de betrouwbaarheid van de rapportages ondermijnt;

- **Communicatie en cultuur:** Ineffectieve communicatie binnen de organisatie en een gebrek aan betrokkenheid bij ethische normen kunnen de naleving van regels en procedures ondermijnen, wat leidt tot een cultuur waarin fouten en fraude worden getolereerd.

Laag tot gemiddeld risico:

- **Schattingen en oordelen:** Subjectieve schattingen met betrekking tot materiële vaste activa en verplichtingen verhogen het risico op fouten, vooral wanneer het management zich bewust is van significante tekortkomingen in de interne controles. Dit kan leiden tot verkeerde financiële rapportages en een vermindering van de betrouwbaarheid van de jaarrekening;

- **Rechtvaardiging van handelingen:** Het management kan soms administratieve handelingen rechtvaardigen die niet aan de geldende normen voldoen, wat het risico op ongepast gedrag vergroot en de integriteit van de organisatie aantast.

Laag risico:

- **Operationele kasstromen:** Regelmatig negatieve operationele kasstromen kunnen de financiële gezondheid van GGDrU bedreigen, wat kan leiden tot liquiditeitsproblemen en een tekort aan middelen voor essentiële operaties;

- **Sterke financiële positie:** Hoewel een sterke financiële positie voordelen biedt, kan dit ook leiden tot onduidelijke voorwaarden voor leveranciers en een gebrek aan transparantie in zakelijke relaties. Hierdoor neemt het risico op misstanden toe. Met een stevige financiële basis kan de neiging ontstaan om minder streng te onderhandelen met leveranciers, wat kan resulteren in minder duidelijke afspraken en verantwoordelijkheden;

- **Personeelsverloop:** Hoog verloop in senior management kan de continuïteit en expertise in governance bedreigen, wat negatieve gevolgen kan hebben voor de besluitvorming en de strategische richting van de organisatie;

- **Managementfocus:** Een sterke focus van het management op resultaatontwikkeling kan leiden tot kortetermijndenken en risico's met zich meebrengen, zoals het negeren van belangrijke controles of het onder druk zetten van medewerkers om resultaten te behalen.

Conclusie

De analyse van de risicocategorieën onthult verschillende significante bedreigingen voor de integriteit van de financiële verslaggeving bij GGDrU. Belangrijke risico's die hierin naar voren komen zijn:

1. **Veranderende regelgeving:** De frequent wijzigende wet- en regelgeving stelt GGDrU bloot aan nieuwe eisen die niet altijd tijdig of adequaat kunnen worden geïmplementeerd. Dit kan leiden tot onvolledige of onjuiste financiële rapportages, wat de reputatie van de organisatie kan schaden;

2. **Druk op financiële prestaties:** Het management staat onder aanzienlijke druk om financiële doelstellingen te behalen, wat kan resulteren in het maken van onethische keuzes of het verdoezelen van financiële problemen. Deze druk kan de kwaliteit van de

financiële rapportages negatief beïnvloeden en de kans op frauduleuze activiteiten vergroten;

3. **Tekortkomingen in interne controles:** Onvoldoende toezicht en gebrekkige interne controlemechanismen verhogen het risico op fouten en onregelmatigheden in de financiële administratie. Wanneer interne controles niet effectief zijn, kunnen frauduleuze handelingen gemakkelijk onopgemerkt blijven, wat leidt tot financiële verliezen en een gebrek aan vertrouwen van belanghebbenden.

Belang van proactieve aanpak
Voor GGDrU is het van essentieel belang om deze risico's proactief te adresseren. Dit houdt in dat de organisatie:

- **Regelmatig risicoanalyses uitvoert** om kwetsbaarheden in de financiële verslaggeving te identificeren en te begrijpen;

- **Het verbeteren en doorontwikkelen van de interne controlefunctie** om ervoor te zorgen dat deze effectief is en zich aanpast aan veranderende omstandigheden.

- **Cultuur van transparantie en ethiek bevordert** binnen de organisatie om het bewustzijn van medewerkers te vergroten over het belang van eerlijke en nauwkeurige financiële rapportages.

Door deze maatregelen te implementeren, kan GGDrU de integriteit en betrouwbaarheid van haar financiële verslaggeving waarborgen, wat cruciaal is voor het behoud van het vertrouwen van stakeholders en voor het voorkomen van frauduleuze activiteiten. Dit draagt bij aan de algehele continuïteit en stabiliteit van de organisatie.

3.1.2 Aanbevelingen

Door deze aanbevelingen te implementeren, kan GGDrU de integriteit van haar financiële verslaggeving waarborgen en haar weerbaarheid tegen frauduleuze activiteiten versterken. Gezien de eerder benoemde risico's en de noodzaak voor een proactieve aanpak, worden hieronder enkele aanbevelingen voor GGDrU gepresenteerd:

1. **Versterken van interne controles:**
    - Voer een uitgebreide beoordeling van de bestaande interne controles uit en identificeer eventuele tekortkomingen;
    - Implementeer robuuste controlemechanismen, zoals functiescheiding en regelmatige interne audits, om de kans op fouten en fraude te minimaliseren;

2. **Opleiding en bewustwording:**
    - Organiseer trainingen voor medewerkers en management over de nieuwste wet- en regelgeving, ethische normen en fraudepreventie;
    - Stimuleer een cultuur van transparantie en verantwoordelijkheid, waarbij medewerkers worden aangemoedigd om onregelmatigheden te melden;

3. **Monitoring en rapportage:**
    - Implementeer een continu monitoringssysteem voor financiële processen en rapportages om tijdig afwijkingen of ongebruikelijke transacties te identificeren;
    - Zorg voor duidelijke rapportagelijnen en een protocol voor het escaleren van financiële problemen aan het management;

4. **Beoordeling van risico's:**
    - Voer regelmatig risicobeoordelingen uit om te evalueren hoe veranderende wetgeving en bedrijfsomstandigheden de organisatie kunnen beïnvloeden;
    - Pas de risicomanagementstrategieën aan op basis van de uitkomsten van deze beoordelingen.

5. **Transparantie in financiële verslaggeving:**
    - Zorg voor een heldere en begrijpelijke presentatie van financiële gegevens die voldoet aan de wettelijke eisen;
    - Overweeg externe audits om de betrouwbaarheid van financiële rapportages te waarborgen en het vertrouwen van stakeholders te versterken;

6. **Beheer van complexe transacties:**
    - Ontwikkel richtlijnen voor de beoordeling van ongebruikelijke of complexe transacties, vooral met gelieerde partijen, om ervoor te zorgen dat ze in overeenstemming zijn met de geldende regelgeving;

7. **Tussenpersonen en leveranciersbeheer:**
    - Voer due diligence uit bij het inschakelen van tussenpersonen en leveranciers om de transparantie van hun transacties te waarborgen;
    - Zorg ervoor dat er duidelijke contractuele afspraken zijn met tussenpersonen die hun rol rechtvaardigen.

3.2 Oneigenlijke toe-eigening van bedrijfsmiddelen

3.2.1 Conclusies

Potentiële risicocategorieën

Hoog risico:

- **Bedrijfsmiddelen**: Tablets, laptops en mobiele telefoons brengen aanzienlijke risico's voor diefstal en misbruik met zich mee, vooral bij onduidelijkheid over eigendom. Gebrek aan heldere eigendomsdocumentatie vergroot de kans op verlies en bemoeilijkt het opsporen van deze bedrijfsmiddelen. Dit geldt ook voor andere bedrijfsmiddelen, zoals kantoorartikelen, medische verbruiksgoederen en apparatuur, waar onduidelijkheid kan leiden tot ongeoorloofd gebruik, zoals het verkeerd inzetten van kantoormateriaal voor persoonlijke doeleinden en het ontvreemden van van medische hulpmiddelen zoals steriele handschoenen.

Gemiddeld tot hoog risico:

- **Onvoldoende scheiding van taken**: Het ontbreken van een duidelijke verdeling van verantwoordelijkheden binnen processen kan leiden tot fraude. Wanneer één persoon meerdere stappen in een proces beheert, zoals goedkeuring, uitvoering en controle, is de kans op misbruik groter. Dit kan resulteren in ongepaste handelingen zonder dat dit tijdig wordt opgemerkt;

- **Gebrekkige onafhankelijke controles**: Een tekortkoming in onafhankelijke controles verhoogt eveneens het risico op fraude. Zonder externe verificatie of toezicht is het

moeilijk om afwijkingen of onregelmatigheden tijdig te detecteren, wat de kans op financiële schade vergroot;

- **Onvoldoende kennis van IT**: Wanneer het management niet over voldoende IT-kennis beschikt, vergroot dit de kans op oneigenlijk gebruik van bedrijfsmiddelen door IT-personeel. Een gebrek aan begrip van technologische processen kan resulteren in onvoldoende toezicht op IT-activiteiten, waardoor medewerkers onterecht toegang krijgen tot gevoelige informatie. Dit verhoogt het risico op misbruik van systemen en bedrijfsmiddelen, wat de integriteit en veiligheid van de organisatie in gevaar brengt;

- **Onvoldoende monitoring en documentatie**: Gebrek aan adequate monitoring en documentatie van transacties creëert kansen voor frauduleuze activiteiten. Wanneer transacties niet goed worden bijgehouden of gecontroleerd, kunnen afwijkingen en onregelmatigheden onopgemerkt blijven. Dit vergroot de kans dat medewerkers ongeoorloofde handelingen verrichten zonder dat dit tijdig wordt ontdekt, wat kan leiden tot financiële verliezen en schending van de integriteit van de organisatie.

Gemiddeld risico:

- **Veranderingen in salarissen en promoties**: Aanpassingen in salarissen en promoties kunnen ontevredenheid onder medewerkers veroorzaken, wat de kans op fraude vergroot. Wanneer medewerkers zich benadeeld of onvoldoende erkend voelen, kunnen ze geneigd zijn om ongepaste handelingen te verrichten uit frustratie of om hun onvrede te uiten. Dit kan leiden tot financiële schade en een negatieve impact op de organisatiecultuur;

- **Onvoldoende toezicht op uitgaven en registratie**: Gebrek aan adequate toezicht op uitgaven en onvolledige registratie van gewerkte uren kan leiden tot onterecht toegeëigende middelen. Wanneer uitgaven niet goed worden gecontroleerd en uren niet nauwkeurig worden vastgelegd, is de kans groter dat medewerkers misbruik maken van middelen of meer uren declareren dan daadwerkelijk gewerkt. Dit kan resulteren in financiële verliezen voor de organisatie en kan de betrouwbaarheid van financiële rapportages ondermijnen.

Laag tot gemiddeld risico:

- **Digitale betalingen en contant geld**: Ondanks de verschuiving naar digitale betalingen blijven er risico's bestaan. Fraude, vooral bij ongeoorloofde of onjuiste transacties, laat zien dat strikte controle- en monitoringsmaatregelen essentieel zijn voor de integriteit van financiële processen. Zonder goede controles kunnen ongepaste handelingen plaatsvinden, wat kan leiden tot financiële verliezen en de betrouwbaarheid van de organisatie aantasten;

- **Onvoldoende administratie van bedrijfsmiddelen:** Een gebrekkige administratie van bedrijfsmiddelen, in combinatie met het tolereren van kruimeldiefstal, vormt een aanzienlijk risico. Wanneer bedrijfsmiddelen niet goed worden geregistreerd of bijgehouden, kunnen diefstallen en onterecht gebruik gemakkelijk onopgemerkt blijven. Dit kan leiden tot accumulatie van verliezen, waarbij zelfs ogenschijnlijk kleine bedragen samen kunnen oplopen tot significante financiële schade voor de organisatie. Een strikte administratie en cultuur van verantwoordelijkheidsgevoel zijn cruciaal om dergelijke risico's te minimaliseren

Laag risico:

- **Bepaalde voorraaditems**: Bij GGDrU kunnen specifieke voorraaditems, zoals medische voorraden en kantoorbenodigdheden, in combinatie met onvoldoende controle door het management leiden tot oneigenlijk gebruik. Voorbeelden hiervan zijn het onterecht gebruiken van medische apparatuur voor persoonlijk gebruik of het niet registreren van gebruikte kantoorartikelen. Effectieve monitoring en beheer zijn essentieel om deze risico's te minimaliseren en te voorkomen dat middelen onterecht worden gebruikt, wat kan resulteren in hogere kosten en verlies van middelen.

Conclusie

Deze analyse benadrukt dat de GGDrU proactief moet optreden om de interne controles te versterken en een cultuur van bewustzijn te creëren. Dit is essentieel om de risico's van oneigenlijke toe-eigening van bedrijfsmiddelen te verminderen en de integriteit van de organisatie te waarborgen. Enkele belangrijke aandachtspunten zijn:

- **Gebrekkige kennis van informatietechnologie**: Dit tekort binnen het management kan leiden tot een verhoogd risico op frauduleuze activiteiten, vooral in een tijdperk waarin digitale systemen steeds belangrijker worden;

- **Impact van personeelsveranderingen op medewerkerstevredenheid**: Ontevreden medewerkers kunnen frauduleus gedrag vertonen, vooral als ze zich niet gewaardeerd voelen;

- **Slechte administratie en tolerantie van kruimeldiefstal**: Dit ondermijnt de algehele beveiliging van bedrijfsmiddelen.

Belang van proactieve aanpak

De volgende aandachtspunten zijn cruciaal voor het verbeteren van de interne controles en het bevorderen van een positieve organisatiecultuur:

- **Proactieve stappen**: GGDrU moet proactief handelen om de interne controles te verbeteren;

- **Versterken van controlemechanismen**: Er moet aandacht zijn voor het verbeteren en versterken van bestaande controlemechanismen;

- **Gerichte training**: Faciliteer training voor medewerkers op het gebied van compliance en risicobeheer om hen beter toe te rusten;

- **Cultuur van transparantie**: Bevorder een cultuur van transparantie en verantwoordelijkheid binnen de organisatie;

- **Medewerkerbetrokkenheid**: Zorg ervoor dat medewerkers zich meer betrokken voelen bij de organisatie;

- **Melden van onethisch gedrag**: Dit vergroot de kans dat medewerkers onethisch gedrag sneller melden, wat de integriteit van GGDrU ten goede komt.

Door deze maatregelen te implementeren, kan GGDrU het risico van oneigenlijke toe-eigening van bedrijfsmiddelen aanzienlijk reduceren. Dit draagt niet alleen bij aan de bescherming van de financiële integriteit van de organisatie, maar helpt ook om het vertrouwen van

stakeholders te waarborgen en de algehele reputatie van GGDrU te versterken. Een goed functionerende organisatie die transparant en verantwoordelijk opereert, is beter voorbereid om de toekomstige uitdagingen aan te gaan.

3.2.2 Aanbevelingen

Door deze aanbevelingen op te volgen, kan GGDrU de risico's van oneigenlijke toe-eigening van bedrijfsmiddelen effectief minimaliseren en de integriteit van de organisatie waarborgen. Een proactieve aanpak met focus op training, monitoring en transparantie is essentieel voor het realiseren van een veilige en verantwoordelijke werkomgeving:

1. **Versterken van interne controles:**
    - Implementeer duidelijke scheidingen van taken binnen de organisatie om te voorkomen dat één persoon teveel controle heeft over processen. Dit kan bijvoorbeeld door verantwoordelijkheden te verdelen tussen verschillende medewerkers;

2. **Training en opleiding:**
    - Bied gerichte training aan voor het management en medewerkers over informatietechnologie, risicobeheer en fraudepreventie. Dit vergroot de bewustwording van IT-risico's en versterkt de vaardigheden van medewerkers om technologie veilig en effectief te gebruiken;

3. **Robuuste monitoring en documentatie:**
    - Ontwikkel en implementeer systemen voor monitoring en documentatie van transacties om fraude te detecteren en te voorkomen. Zorg ervoor dat deze systemen regelmatig worden geëvalueerd en verbeterd;

4. **Transparante beloningsstructuren:**
    - Ontwerp en implementeer transparante belonings- en promotiestructuren die gericht zijn op medewerkerstevredenheid, rekening houdend met de beperkingen van de cao. Dit draagt bij aan een positieve werkomgeving en vermindert het risico op frauduleus gedrag;

5. **Strikte controlemaatregelen voor contante en digitale betalingen**:
    - Implementeer strikte controlemaatregelen voor zowel contante als digitale betalingen, zoals dubbele verificatie en dagelijkse audits, om onterecht gebruik van middelen te voorkomen;

6. **Verbetering van administratieve procedures:**
    - Evalueer en verbeter de administratieve procedures rondom bedrijfsmiddelen om onduidelijkheden te voorkomen. Dit omvat ook het ontwikkelen van richtlijnen voor het omgaan met kruimeldiefstal en een cultuur van verantwoordelijkheid bevorderen;

7. **Regelmatige risico-evaluaties:**
    - Voer regelmatig risico-evaluaties uit om nieuwe risico's tijdig te identificeren en aan te pakken. Dit kan helpen om de effectiviteit van de interne controles te waarborgen en aan te passen aan veranderende omstandigheden;

8. **Cultuur van verantwoordelijkheid en zorgvuldigheid:**

- Stimuleer een organisatiecultuur die verantwoordelijkheid en zorgvuldigheid bevordert. Dit kan door het implementeren van ethische richtlijnen en het bevorderen van open communicatie over risico's en verantwoordelijkheden.

Bijlage Interne frauderisicoanalyse

De interne frauderisicoanalyse van GGDrU biedt waardevolle inzichten in de specifieke risicofactoren die verband houden met fraude binnen de organisatie. Het geeft een overzicht van potentiële kwetsbaarheden en helpt GGDrU om gerichte maatregelen te nemen ter preventie, detectie en beheersing van fraude.

De frauderisicoanalyse van GGDrU geeft een duidelijk overzicht van de geïdentificeerde frauderisico's, de genomen interne beheersmaatregelen en waar verdere acties nodig zijn. Dit document is van cruciaal belang voor het risicobeheer binnen GGDrU, omdat het helpt bij het prioriteren van risicogebieden en het versterken van de maatregelen om fraude effectief te voorkomen en te beheersen.

Het is van belang om zowel frauduleuze financiële verslaggeving als het ongeoorloofd toe-eigenen van bedrijfsmiddelen te analyseren. Beide risico's bedreigen niet alleen de financiële stabiliteit van de organisatie, maar ook haar reputatie en integriteit. Door deze risico's te identificeren en aan te pakken, kan de organisatie een cultuur van transparantie en verantwoordelijkheid bevorderen, wat de duurzaamheid en het succes op de lange termijn ten goede komt.

1.1 Structuur van de tabel

De interne frauderisico's zijn gepresenteerd in de vorm van een tabel, die een gestructureerd overzicht biedt van de verschillende risicofactoren en de bijbehorende beheersmaatregelen. Deze opzet maakt het gemakkelijk om de informatie snel te begrijpen en te vergelijken.

Toelichting op de tabel:

- **Duidelijke indeling**: De tabel is opgebouwd uit verschillende kolommen die elk een specifiek aspect van het frauderisico belichten. Hierdoor kan men in één oogopslag zien welke risico's er zijn, hun impact en de genomen maatregelen;
- **Overzichtelijkheid**: Door de gegevens in een tabel te presenteren, wordt de informatie overzichtelijker dan in een lange tekst. Dit helpt betrokkenen om snel de belangrijkste punten te identificeren en te begrijpen;
- **Vergelijkbaarheid**: De tabelstructuur maakt het mogelijk om verschillende risico's met elkaar te vergelijken op basis van kans, impact en overige relevante criteria. Dit is cruciaal voor het prioriteren van acties en het toewijzen van middelen;

- **Actiegericht**: Aan het eind van de tabel is er ruimte om aan te geven welke verdere acties vereist zijn. Dit stimuleert een proactieve benadering van risicobeheer.

1.2 Onderdelen

De tabel over interne frauderisico's is opgebouwd uit verschillende secties die samen een compleet overzicht geven van de risico's en maatregelen. Hieronder worden de onderdelen toegelicht:

---

1. Risicofactoren bij fraude
Deze sectie biedt een overzicht van de factoren die mogelijk bijdragen aan frauduleuze activiteiten binnen GGDrU. Dit helpt bij het identificeren van de bronnen van risico.

---

2. Identificatie van potentiële frauderisico's
Hier wordt aangegeven of er potentiële risico's zijn, weergegeven met een eenvoudig "Ja" of "Nee". Dit maakt het gemakkelijk om snel te zien of er aanleiding is voor verder onderzoek.

---

3. Omschrijving potentiële frauderisico's Deze kolom bevat een gedetailleerde beschrijving van elk geïdentificeerd frauderisico, waardoor de aard en context van elk risico duidelijk worden;

---

4. Kans (H, M, L)
Hier wordt de waarschijnlijkheid aangegeven dat het frauderisico zich voordoet, ingedeeld in hoog (H), midden (M) of laag (L). Dit helpt bij het inschatten van de urgentie van elk risico:

- **Hoog (H)**: Grote kans dat het risico zich voordoet, wat onmiddellijke aandacht en maatregelen vereist (bijv. beperkte controle op financiële transacties);
- **Midden (M)**: Gemiddelde kans op het risico, wat regelmatig monitoring en mogelijk extra beheersmaatregelen nodig heeft (bijv. zwakke plekken in crediteurengegevens);
- **Laag (L)**: Kleine kans dat het risico zich voordoet, waardoor het minder prioriteit heeft en doorgaans geen directe actie vereist (bijv. robuuste controles en goede naleving);

---

5. Impact (H, M, L)
Hier wordt de mogelijke impact van het risico beoordeeld, eveneens ingedeeld in hoog, midden of laag. Dit geeft inzicht in de gevolgen als het risico zich daadwerkelijk voordoet:

- **Hoog (H)**: Ernstige gevolgen, zoals aanzienlijke financiële verliezen, reputatieschade of juridische problemen (bijv. frauduleuze betalingen aan valse crediteuren);
- **Midden (M)**: Merkbare impact die kan leiden tot aanzienlijke kosten of tijdelijke verstoringen, maar de organisatie kan zich doorgaans herstellen (bijv. foutieve betalingen aan legitieme crediteuren);
- **Laag (L)**: Minimale gevolgen met weinig tot geen impact op de organisatie; risico's kunnen gemakkelijk worden gecorrigeerd zonder significante schade (bijv. kleine administratieve fouten);

---

6. Welke interne beheersmaatregelen zijn getroffen?
Deze sectie beschrijft de acties en maatregelen die de organisatie heeft genomen om het risico op fraude te verminderen en te beheersen;

---

7. Rest-risico (H, M, L)
Dit geeft aan welk risico nog overblijft na de implementatie van de interne beheersmaatregelen, gecategoriseerd als hoog, midden of laag. Dit laat zien hoe effectief de maatregelen zijn geweest:

- **Hoog (H)**: Aanzienlijk risico blijft over, wat aangeeft dat de beheersmaatregelen niet effectief zijn en ernstige gevolgen kunnen veroorzaken (bijv. voortdurende mogelijkheden voor fraude);
- **Midden (M)**: Risico is verminderd, maar er blijft een merkbare kans bestaan, wat duidt op enige effectiviteit van de maatregelen, maar ook op zwakke punten (bijv. onvolledige controles in het betalingsproces).
- **Laag (L)**: Minimal risico met een kleine kans dat het zich voordoet, wat aangeeft dat de beheersmaatregelen succesvol zijn geweest (bijv. robuuste interne controles die fraude effectief minimaliseren);

---

8. Actie vereist?
In deze laatste kolom wordt aangegeven of er aanvullende acties nodig zijn om het risico verder te verminderen. Dit stimuleert een proactieve aanpak van risicobeheer.

Deze indeling biedt een helder en gestructureerd overzicht van de verschillende secties die essentieel zijn voor het begrijpen en beheren van interne frauderisico's binnen de GGDrU.

1.3 Acties voor verbetering

In dit gedeelte van de tabel worden specifieke acties beschreven die GGDrU kan ondernemen om de geïdentificeerde frauderisico's te verminderen of op te lossen, met een focus op het beperken van het rest-risico. Het doel is om een proactieve aanpak te hanteren, waarbij niet alleen de huidige risico's effectief worden beheerd, maar ook wordt geïnvesteerd in het verbeteren van processen en controles om toekomstige risico's te voorkomen. Deze acties zijn specifiek afgestemd op elke risicofactor en zijn ontworpen om de algehele weerbaarheid van de organisatie te versterken, zodat het resterende risico op frauduleuze activiteiten verder kan worden geminimaliseerd.

Voor elk geïdentificeerd frauderisico worden concrete maatregelen voorgesteld, zoals het versterken van interne controles, het implementeren van trainingsprogramma's voor medewerkers, en het aanpassen van bestaande procedures. Deze acties zijn gericht op het vergroten van de weerbaarheid van de organisatie tegen fraude en het minimaliseren van het rest-risico. Door een cultuur van transparantie en verantwoordelijkheidsbesef te bevorderen, wordt niet alleen de kans op frauduleuze activiteiten verkleind, maar wordt ook een solide basis gelegd voor het duurzaam beheren van toekomstige risico's.

1.4 High level inschatting

De tabel biedt een "high level inschatting" van de beheersing van frauderisico's en vertegenwoordigt een strategische en globale evaluatie van hoe effectief een organisatie zoals GGDrU in staat is om fraude te beheren. De term "high level" duidt erop dat deze beoordeling op een abstract niveau plaatsvindt, waarbij de focus ligt op het bredere plaatje en niet op de specifieke details van individuele processen of casussen.

In deze context helpt de tabel om een overzicht te krijgen van de belangrijkste risico's en de maatregelen die zijn genomen om deze te beheersen. Door deze aanpak kan GGDrU een helder inzicht krijgen in haar algemene fraudeweerbaarheid en de effectiviteit van bestaande controlemechanismen, zonder in de complexiteit van operationele details te verzeilen.

Dit houdt in dat:

- **Strategische beoordeling:** Deze inschatting biedt een overzicht van de algemene effectiviteit van de bestaande controles en maatregelen zonder te diep in de details van de operationele uitvoering te duiken;

- **Risico-identificatie:** De focus ligt op het identificeren van de belangrijkste frauderisico's die de organisatie kunnen bedreigen, evenals de effectiviteit van de bestaande mechanismen die zijn geïmplementeerd om deze risico's te beheersen;

- **Beleidsanalyse:** Hierbij wordt gekeken naar de beleidslijnen en procedures die zijn ingesteld om fraude te voorkomen en hoe goed deze in de praktijk functioneren;

- **Overzichtelijke aanpak:** Dit soort evaluatie helpt bij het ontwikkelen van een breed begrip van de risico's, zodat strategische beslissingen kunnen worden genomen over waar verbeteringen nodig zijn.

Het doel van deze inschatting is om een helder en strategisch inzicht te krijgen in de capaciteit van GGDrU om fraude te voorkomen, op te sporen en te reageren. Hierdoor kan de organisatie gerichte acties ondernemen om eventuele kwetsbaarheden te adresseren en een cultuur van transparantie en verantwoordelijkheid te bevorderen.
Door deze hoge beoordeling kan GGDrU niet alleen de huidige situatie begrijpen, maar ook toekomstige risico's anticiperen en plannen ontwikkelen voor een effectievere beheersing van frauderisico's.

1.5 Tabel Frauderisicoanalyse

Tabel Frauderisicoanalyse

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
1. Frauduleuze financiële verslaggeving		Frauduleuze financiële verslaggeving kan leiden tot verkeerde beslissingen door investeerders, aandeelhouders en andere stakeholders. Als financiële cijfers worden gemanipuleerd, kunnen de werkelijke prestaties van de organisatie verkeerd worden geïnterpreteerd, wat kan leiden tot financiële verliezen en reputatieschade. Frauduleuze financiële verslaggeving verwijst naar opzettelijk onjuiste of misleidende informatie die wordt opgenomen in de financiële rapportage van een organisatie. Het doel is meestal om het financiële beeld van het bedrijf gunstiger voor te stellen dan het in werkelijkheid is, bijvoorbeeld door winst te verhogen, verliezen te verbergen of schulden te minimaliseren. Dit type fraude kan inhouden: • Het manipuleren van cijfers in de balans of winst- en verliesrekening; • Het opzettelijk verkeerd boeken van inkomsten of uitgaven; • Het niet rapporteren van bepaalde verplichtingen of het verbergen van schulden; • Valsheid in geschrifte, zoals het creëren van fictieve transacties of het vervalsen van documenten.					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		Het doel van frauduleuze financiële verslaggeving kan variëren van het misleiden van investeerders of aandeelhouders tot het verkrijgen van gunstigere financieringsvoorwaarden of het voorkomen van faillissement. Organisaties die zich schuldig maken aan deze praktijken kunnen te maken krijgen met juridische sancties, reputatieschade, en verlies van vertrouwen bij stakeholders.					
1.1 Druk	**De factor druk verwijst naar de motivatie of de omstandigheden die individuen ertoe aanzetten om fraude te plegen.**	Dit kan voortkomen uit persoonlijke of financiële problemen, zoals schulden, een hoge levensstandaard of de behoefte om een bepaalde status te behouden. Daarnaast kan de druk ook voortkomen uit externe factoren, zoals prestatiedruk vanuit de organisatie of verwachtingen van leidinggevenden. Deze druk kan een sterke drijfveer vormen voor individuen om ongepaste acties te overwegen als een manier om aan hun behoeften te voldoen of om aan de verwachtingen te voldoen.					
1.1.1 De financiële stabiliteit en winstgevendheid kunnen worden bedreigd door economische omstandigheden in de publieke gezondheidszorg of door specifieke exploitatiefactoren, zoals blijkt uit:		Economische omstandigheden verwijzen naar de algehele staat van de economie, inclusief factoren zoals groei, werkloosheid, inflatie, rentevoeten, consumentenvertrouwen, internationale handel en overheidsbeleid, die allemaal invloed hebben op economische activiteit en levensstandaard.					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		Exploitatiefactoren zijn variabelen die de winstgevendheid en efficiëntie van een organisatie beïnvloeden, zoals kostenstructuur, productiviteit, bezettingsgraad, omzet, prijsstelling, proces efficiëntie en marktvraag. De risico's die GGDrU kan ondervinden als gevolg van externe en interne factoren die de financiële gezondheid beïnvloeden hebben onder meer betrekking hebben op: • **Economische omstandigheden**: Dit omvat factoren zoals recessies, stijgende kosten van grondstoffen, veranderende marktvraag, en concurrentiedruk die de winstgevendheid kunnen ondermijnen; • **Exploitatie-omstandigheden**: Dit verwijst naar interne factoren zoals inefficiënties in bedrijfsprocessen, ongeplande uitgaven, of problemen met de toeleveringsketen die de operationele stabiliteit en financiële prestaties van een organisatie kunnen aantasten.					
• Kwetsbaarheid door frequent veranderende wet- en regelgeving; • Nieuwe eisen voor financiële verslaggeving en wettelijke verplichtingen of andere regelgeving.	Ja	Er zijn potentiële frauderisico's te identificeren in verschillende contexten, vooral binnen financiële verslaggeving, bedrijfsvoering en overheidsinstellingen: 1. **Financiële verslaggeving**: Dit kan gebeuren als medewerkers cijfers manipuleren om betere	H ☹	H ☹	**1. Financiële Verslaggeving**: • **Interne controles:** Interne controlemechanismen zoals goedkeuringsprocessen voor financiële rapportages. Dit bevat onder meer het vereisen van meerdere digitale handtekeningen voor het goedkeuren van belangrijke documenten;	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		prestaties te suggereren dan daadwerkelijk het geval is, vaak onder druk van externe verwachtingen of interne doelen. 2. **Corruptie**: Dit kan zich uiten in omkoping of misbruik van bevoegdheden door medewerkers die in ruil voor voordelen besluiten nemen die niet in het belang van de organisatie zijn. 3. **Verlies van middelen**: Dit kan voortkomen uit ongepaste toegang tot bedrijfsmiddelen, waarbij medewerkers bijvoorbeeld geld of goederen verduisteren. Belangrijke factoren bij het identificeren van deze risico's: • **Organisatorische cultuur**: Een cultuur die druk legt op prestaties zonder adequate controles kan fraude in de hand werken; • **Complexiteit van processen**: Complexe financiële transacties en onvoldoende toezicht kunnen leiden tot opportuniteiten voor fraude. Opportuniteiten verwijzen naar kansen of mogelijkheden die zich voordoen, vaak in een context waarin ze benut kunnen worden om een			• **Training en bewustwording:** Regelmatig training voor medewerkers over ethische normen en richtlijnen voor financiële rapportage. Dit helpt om een cultuur van transparantie te bevorderen; • **Externe audits:** Het inschakelen van externe auditors om financiële verslagen te controleren en de nauwkeurigheid te waarborgen. Dit fungeert als een extra laag van toezicht. **2. Corruptie**: • **Gedragscode:** Duidelijke gedragscode die corrupt gedrag verbiedt en sancties vaststelt voor overtredingen. Dit bevat ook richtlijnen voor het omgaan met geschenken en andere voordelen; • **Klokkenluidersregeling:** Meldingssysteem voor medewerkers om verdachte activiteiten of corruptie te rapporteren zonder angst voor repercussies; • **Regelmatige audits:** Regelmatige interne en externe audits om ervoor te zorgen dat er geen misbruik van bevoegdheden plaatsvindt. **3. Verlies van Middelen**: • **Toegangscontrole:** Strikte toegangscontroles voor bedrijfsmiddelen, zoals digitale betaalmiddelen en waardevolle goederen. Dit houdt in dat alleen bevoegde medewerkers toegang		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		voordeel te behalen of om een doel te bereiken.			hebben tot bepaalde gebieden of systemen; • **Inventarisbeheer:** Regelmatig inventariseren en nauwkeurig vastleggen van bedrijfsmiddelen om een up-to-date administratie te garanderen en verliezen of verduisteringen tijdig op te sporen. Dit zorgt ervoor dat afwijkingen snel worden herkend, waardoor de kans op financiële schade door misbruik of vermissing van bedrijfsmiddelen aanzienlijk wordt verminderd; • **Beveiligingsmaatregelen:** Fysieke beveiliging van bedrijfsmiddelen door middel van camera's, alarmsystemen en andere beveiligingsmaatregelen om diefstal te voorkomen.		

Acties voor verbetering:
Om de risico's van financiële verslaggeving, corruptie en verlies van middelen effectief te beheersen, zijn de volgende acties vereist:

1. **Financiële Verslaggeving:**
   - **Implementatie van interne controles:** Zorg voor meer gedetailleerde procedures en regelmatige interne audits om afwijkingen te identificeren, en zorg voor scheiding van verantwoordelijkheden in de rapportageprocessen;
2. **Corruptie:**
   - **Training en cultuurverandering:** Voer trainingen uit over ethisch gedrag en anti-corruptiebeleid, en bevorder een organisatiecultuur waarin openheid en integriteit worden aangemoedigd;
3. **Verlies van Middelen:**
   - **Versterking van toegangscontrole en monitoring:** Implementeer strikte toegangscontroles tot bedrijfsmiddelen en gebruik technologie om de toegang en het gebruik van middelen te monitoren.

Overkoepelende acties:

- Voer regelmatig risicobeoordelingen uit om nieuwe risico's te identificeren en evalueer bestaande beheersmaatregelen.
- Zorg voor een transparant rapportagesysteem om afwijkingen en risico's tijdig te rapporteren aan het management en relevante stakeholders.

• Exploitatieverliezen die de continuïteit van de	Ja	Potentiële risico's bij exploitatieverliezen die de continuïteit van de bedrijfsvoering onder druk	H 	H 	• **Marktonderzoek en diversificatie**: Het uitvoeren van regelmatig marktonderzoek om trends en	M tot H 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
bedrijfsvoering onder druk zetten		zetten, kunnen onder andere de volgende factoren omvatten: • **Verminderde Omzet**: Een daling in de vraag naar diensten kan leiden tot lagere omzet, waardoor de exploitatieverliezen toenemen. Dit kan ontstaan door economische recessies, veranderende voorkeuren van inwoners in regio Utrecht, of verhoogde concurrentie. In een ravijnjaar kunnen gemeenten in financiële problemen komen, waardoor ze genoodzaakt zijn om bezuinigingen door te voeren, projecten uit te stellen of op zoek te gaan naar extra financiering; • **Verhoogde Kosten**: Stijgende kosten voor grondstoffen voor vaccins e.d., arbeid of andere operationele uitgaven kunnen de winstgevendheid aantasten. Dit kan ook het gevolg zijn van inflatie of verstoringen in de toeleveringsketen. • **Onvoldoende kapitaal**: Wanneer GGDrU niet over voldoende financiële reserves beschikt, kunnen exploitatieverliezen de mogelijkheid om operationele kosten te dekken ernstig onder druk zetten. Dit kan leiden tot een negatieve spiraal van schulden en verdere verliezen; • **Wet- en regelgeving**: Niet-naleving van wet- en regelgeving kan leiden tot boetes, rechtszaken, of andere juridische			gedragsveranderingen te analyseren, stelt GGDrU in staat om tijdig in te spelen op deze veranderingen en diensten hierop aan te passen. Door diensten te diversifiëren, kan GGDrU haar afhankelijkheid van één enkele inkomstenbron minimaliseren. • **Kostenbeheersing**: Budgetterings- en kostenbewakingssystemen helpen GGDrU om stijgende kosten vroegtijdig te signaleren en effectief te beheersen. Daarnaast kan het onderhandelen met leveranciers over prijzen en voorwaarden bijdragen aan het verlagen van kosten en het verbeteren van de financiële efficiëntie. • **Financieel risicomanagement**: Zorgen voor voldoende financiële reserves en effectief kasstroombeheer om operationele kosten te dekken. Het gebruik van verzekeringen is essentieel voor het mitigeren van risico's en het waarborgen van financiële stabiliteit. • **Naleving van wet- en regelgeving**: Duidelijke richtlijnen en procedures die helpen bij het navigeren door de complexe wereld van wet- en regelgeving. Dit omvat trainingen voor medewerkers, waarin ze bewust worden gemaakt van de juridische verplichtingen en de gevolgen van niet-naleving. Door audits uit te voeren, kan GGDrU de naleving van de regelgeving controleren en eventuele tekortkomingen tijdig aanpakken; • **Imago en reputatie beheren en beschermen:** Duidelijke en transparante communicatie is essentieel om klanten (individuen en	☹	

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		gevolgen die niet alleen financiële schade, maar ook reputatieschade met zich meebrengen**;** • **Reputatieschade**: Exploitatieverliezen kunnen het imago van GGDrU schaden, wat leidt tot verlies van klanten. De klanten van GGDrU omvatten individuen en gezinnen, scholen, zorginstellingen, gemeentebesturen, bedrijven en kwetsbare groepen die profiteren van diensten op het gebied van publieke gezondheid. Dit kan een langdurige impact hebben op de financiële prestaties; • **Medewerkersmotivatie**: Financiële druk kan leiden tot verminderde moraal onder medewerkers, wat kan resulteren in lagere productiviteit, hogere ziekteverzuim en een grotere kans op personeelsverloop; • **Risico van fraude**: In tijden van financiële druk kunnen medewerkers of leidinggevenden verleid worden om frauduleuze activiteiten te ondernemen om persoonlijke of organisatorische verliezen te compenseren; • **Onvoorziene gebeurtenissen**: Pandemieën en natuurrampen, of andere onvoorziene gebeurtenissen kunnen de operationele capaciteit van GGDrU bedreigen, wat leidt tot directe en indirecte financiële verliezen.			gezinnen, scholen, zorginstellingen, gemeentebesturen, bedrijven en kwetsbare groepen die gebruikmaken van diensten op het gebied van publieke gezondheid) goed te informeren over gezondheidsmaatregelen, vaccinaties en andere belangrijke onderwerpen. Door consistente en begrijpelijke boodschappen te verspreiden, kan GGDrU misverstanden voorkomen en de betrokkenheid van de gemeenschap vergroten; • **Medewerkerstevredenheid en motivatie**: Medewerkersenquêtes bieden waardevolle inzichten in de moraal en betrokkenheid van medewerkers. Daarnaast is het aanbieden van opleidingsmogelijkheden en carrièreontwikkeling essentieel; • **Fraudepreventie**: Bewustwordingsprogramma's over frauderisico's en meldingsprocedures dragen bij aan een cultuur van alertheid en verantwoordelijkheid, waarbij medewerkers zich bewust zijn van de risico's en weten hoe ze verdachte activiteiten moeten rapporteren; • **Crisis- en continuïteitsplanning**: Noodplan voor onvoorziene gebeurtenissen, zoals pandemieën of natuurrampen, om de operationele capaciteit te waarborgen. Daarnaast worden trainingen georganiseerd om de paraatheid van de organisatie te evalueren en te testen		
Acties voor verbetering:							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Om de risico's van exploitatieverliezen die de continuïteit van de bedrijfsvoering onder druk zetten effectief aan te pakken, zijn verschillende acties vereist: 1. **Risicoanalyse en -evaluatie**: ○ Voer regelmatig risicobeoordelingen uit om de huidige en opkomende risico's in kaart te brengen. Dit omvat het monitoren van economische trends, concurrentieanalyses en veranderingen in consumentenvoorkeuren; 2. **Financiële planning en liquiditeitsbeheer**: ○ Zorg voor een solide financiële planning die de organisatie helpt om voldoende reserves aan te houden. Implementeer een effectief liquiditeitsbeheer om ervoor te zorgen dat operationele kosten altijd gedekt kunnen worden; 3. **Kostenbeheersing**: ○ Voer kostenbesparende maatregelen door, zoals het heronderhandelen van contracten met leveranciers of het optimaliseren van operationele processen om kosten te verlagen; 4. **Training en ontwikkeling**: ○ Bied trainingen aan voor medewerkers om hen bewust te maken van risico's, inclusief ethische en compliance-trainingen om fraude te voorkomen. Dit verhoogt ook de medewerkersmotivatie en betrokkenheid; 5. **Communicatie en transparantie**: ○ Zorg voor een open communicatiekanaal binnen de organisatie waar medewerkers zich vrij voelen om zorgen te uiten over mogelijke risico's of onregelmatigheden. Dit kan ook helpen bij het identificeren van vroegtijdige signalen van problemen; 6. **Toegangscontrole en beveiliging**: ○ Implementeer strikte toegangscontroles tot bedrijfsmiddelen, en voer regelmatig controles uit om te zorgen dat alleen geautoriseerde personen toegang hebben; 7. **Monitoring en rapportage**: ○ Ontwikkel systemen voor voortdurende monitoring van financiële prestaties en rapportage van afwijkingen. Zorg ervoor dat het management regelmatig op de hoogte wordt gesteld van risico's en prestaties; 8. **Crisismanagement en noodplannen**: ○ Ontwikkel crisismanagementplannen en noodprocedures voor onvoorziene gebeurtenissen pandemieën en natuurrampen om snel en effectief te kunnen reageren.							
• Herhaaldelijke negatieve operationele kasstromen of het onvermogen om kasstromen uit operationele activiteiten te genereren	Ja	Bij GGDrU kunnen herhaaldelijke negatieve operationele kasstromen of het onvermogen om kasstromen uit operationele activiteiten te genereren verschillende potentiële risico's met zich meebrengen: • **Financiële Stabiliteit**: Herhaaldelijke negatieve kasstromen kunnen leiden tot een verslechtering van de financiële positie, waardoor het moeilijker wordt om lopende kosten, zoals salarissen en operationele uitgaven te dekken; • **Beperkte Diensten**: Wanneer er onvoldoende kasstromen zijn, kan	H 	H 	• **Financieel Management en monitoring**: Het financieel beheersysteem dat regelmatig de kasstromen monitort. Door bijvoorbeeld maandelijkse rapportages te genereren, kan GGDrU vroegtijdig eventuele financiële tekorten identificeren en daarop anticiperen. Dit omvat verschillende essentiële elementen: ○ **Budgettering**: Dit proces omvat het opstellen van gedetailleerde budgetten die de verwachte inkomsten en uitgaven van de organisatie voor een bepaalde periode vastleggen.	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		GGDrU gedwongen worden om diensten te verminderen of uit te stellen. Dit kan invloed hebben op belangrijke gezondheidsprogramma's en de algehele volksgezondheid in de regio; • **Verminderde Investeringen**: Negatieve kasstromen kunnen ook het vermogen van GGDrU om te investeren in noodzakelijke infrastructuur en technologie beperken, wat essentieel is voor het verbeteren van de efficiëntie en effectiviteit van de gezondheidszorg; • **Reputatierisico**: Financiële problemen kunnen de reputatie van GGDrU aantasten, vooral als er publieke zorgen zijn over de continuïteit en kwaliteit van de dienstverlening; • **Verlies van Vertrouwen**: Zowel de gemeenschap als externe stakeholders, zoals gemeenten en zorgpartners, kunnen hun vertrouwen in GGDrU verliezen als de financiële situatie onduidelijk of onbetrouwbaar is. • **Regelgeving en toezicht**: Herhaalde financiële problemen kunnen leiden tot extra toezicht.			○ **Kasstroombeheer**: Het monitoren van inkomende en uitgaande geldstromen om ervoor te zorgen dat er altijd voldoende liquiditeit is om operationele kosten te dekken; ○ **Financiële rapportage**: Het opstellen van regelmatige rapportages die inzicht geven in de financiële situatie van de organisatie, waaronder balansoverzichten en winst- en verliesrekeningen; ○ **Risicobeheer**: Identificeren en evalueren van financiële risico's, zoals fluctuaties in inkomsten, en het implementeren van maatregelen om deze risico's te beheersen; ○ **Compliance en regelgeving**: Zorgen dat de organisatie voldoet aan alle relevante wet- en regelgeving op het gebied van financiële verslaggeving en belastingverplichtingen; ○ **Prestatieanalyse**: Het analyseren van financiële gegevens om de prestaties van de organisatie te beoordelen en strategische beslissingen te nemen. Tegelijkertijd is het verifiëren van de geleverde diensten van cruciaal belang om te waarborgen dat zij voldoen aan de verwachtingen; ○ **Interne controles**: Procedures die zijn ontworpen om de nauwkeurigheid van financiële rapportages te waarborgen en fraude of fouten te voorkomen.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					• **Diversificatie van inkomstenbronnen**: Het ontwikkelen van nieuwe diensten of programma's die additionele inkomsten genereren. Dit kan bijvoorbeeld door het aanbieden van trainingen, workshops of adviesdiensten aan andere zorginstellingen of gemeenschappen; • **Kostenbeheersing**: Het doorvoeren van een strikte kostenbeheersing door onnodige uitgaven te verminderen en efficiëntieverbeteringen door te voeren in de organisatie. Dit kan ook inhouden dat processen worden herzien om verspilling te minimaliseren; • **Onderhandelen met leveranciers**: Het aangaan van onderhandelingen met leveranciers over prijsverlagingen en gunstigere voorwaarden kan helpen om de operationele kosten te verlagen en financiële ruimte te creëren; • **Strategische samenwerkingen**: Het aangaan van partnerschappen met andere organisaties of gemeentes om middelen te delen en gezamenlijke projecten te ontwikkelen. Dit kan niet alleen kosten besparen, maar ook de impact van gezondheidsinitiatieven vergroten; • **Versterking van communicatie**: Het verbeteren van de communicatie met stakeholders en de gemeenschap om transparantie te waarborgen. Dit kan helpen bij het opbouwen van vertrouwen en het vergroten van de betrokkenheid van de gemeenschap, wat op zijn beurt kan leiden tot meer gebruik van de aangeboden diensten;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					• **Training en ontwikkeling van medewerkers**: Investeren in de training van medewerkers om hen beter voor te bereiden op veranderingen en uitdagingen binnen de organisatie. Goed opgeleide medewerkers kunnen bijdragen aan een efficiënter functioneren van de organisatie.		
Acties voor verbetering Bij herhaaldelijke negatieve operationele kasstromen of het onvermogen om kasstromen uit operationele activiteiten te genereren, zijn er verschillende acties die de GGD kan ondernemen om de situatie te verbeteren. Door deze acties te ondernemen, kan GGDrU haar financiële situatie verbeteren en de negatieve kasstromen aanpakken: • **Kostenbeheersing**: Voer een grondige analyse uit van alle operationele kosten en identificeer gebieden waar besparingen kunnen worden gerealiseerd. Dit kan inhouden dat niet-essentiële uitgaven worden verminderd of dat processen worden geoptimaliseerd om efficiëntie te verhogen; • **Ontwikkel nieuwe diensten of producten** die extra inkomsten kunnen genereren, zoals workshops, opleidingen of consultatiediensten; • **Implementeer een geavanceerd financieel beheersysteem** dat regelmatig de kasstromen monitort en inzicht biedt in de financiële situatie. Dit omvat het opstellen van maandelijkse rapportages om afwijkingen tijdig te identificeren. Dit systeem biedt diverse functionaliteiten die de financiële planning, rapportage, en analyse optimaliseren; • **Ga in gesprek met leveranciers** om betere prijzen en voorwaarden te bedingen. Dit kan helpen om de operationele kosten te verlagen; • **Zoek samenwerking met andere organisaties of overheden** om middelen te delen en gezamenlijke initiatieven op te zetten. Dit kan helpen om kosten te verlagen en tegelijkertijd de impact van de diensten te vergroten; • **Versterk de communicatie met gemeenten en inwoners** om vertrouwen te creëren en meer steun te genereren voor de aangeboden diensten. Dit kan ook leiden tot meer betrokkenheid en gebruik van de diensten.							
1.1.2 Het management staat onder overmatige druk om aan de vereisten of verwachtingen van derden te voldoen, als gevolg van:		GGDrU kan verschillende risico's ondervinden als het management onder overmatige druk staat om aan de vereisten of verwachtingen van derden te voldoen. Hier zijn enkele belangrijke risico's: **1. Reputatierisico**: • **Verlies van vertrouwen**: Wanneer GGDrU niet aan de verwachtingen van de gemeenschap, de overheid of andere belanghebbenden voldoet, kan dit leiden tot een afname van het vertrouwen. Dit kan schadelijk zijn voor de					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		reputatie van de organisatie en kan het moeilijk maken om effectief te functioneren in de toekomst; • Voorbeeld: Een negatieve publieke reactie op een vaccinatieprogramma kan het vertrouwen in GGDrU ondermijnen; **2. Financieel risico**: • **Budgetbeperkingen**: De druk om aan externe vereisten te voldoen kan leiden tot extra uitgaven of onvoorziene kosten, waardoor het financiële beheer van GGDrU onder druk komt te staan. Dit kan resulteren in negatieve operationele kasstromen; • Voorbeeld: Onvoorziene kosten in verband met nieuwe gezondheidsinitiatieven kunnen de bestaande budgetten overschrijden; **3**. **Operationeel Risico**: • Afname van efficiëntie: Overmatige druk kan leiden tot een versnelling van besluitvormingsprocessen, wat kan resulteren in een gebrek aan zorgvuldigheid en verminderde efficiëntie. Dit kan ook leiden tot fouten in de uitvoering van programma's of diensten;					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		• Voorbeeld: Het inperken van gezondheidsinspecties of het niet goed naleven van protocollen kan de kwaliteit van de dienstverlening aantasten; **4. Juridisch en compliance risico:** • Schending van wet- en regelgeving: Wanneer de organisatie onder druk staat, kan het risico op niet-naleving van wettelijke verplichtingen toenemen. Dit kan juridische gevolgen hebben en leiden tot sancties of boetes; • Voorbeeld: Onjuiste rapportage of het niet voldoen aan de vereisten voor openbare gezondheid kan juridische repercussies hebben; **5. Personeelsrisico:** • **Verlies van personeel**: Hoge druk en stress kunnen leiden tot burn-out of een hoge personeelsverloop, wat de continuïteit van de organisatie in gevaar kan brengen; • Voorbeeld: Medewerkers kunnen GGDrU verlaten vanwege de hoge werkdruk en de stress die gepaard gaat met het voldoen aan externe verwachtingen.					
• Verwachtingen van externe belanghebbenden met	Hoewel er potentiële						

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
betrekking tot de financiële resultaten, met name verwachtingen die onrealistisch of te ambitieus zijn, inclusief diegene die door het management zijn gesuggereerd, zoals overmatige optimistische persberichten of uitspraken in jaarverslagen;	risico's zijn verbonden aan deze verwachtingen, worden deze risicofactor in deze context niet verder besproken.						
• De noodzaak voor extra financiering, zowel uit eigen middelen als via externe bronnen, is essentieel om concurrerend te blijven, inclusief de financiering van belangrijke investeringen; • Het veiligstellen van financiering voor belangrijke investeringen is cruciaal voor de lange termijn duurzaamheid en effectiviteit van een organisatie. Het stelt de organisatie in staat om te blijven voldoen aan de behoeften van de gemeenschap en haar diensten te verbeteren;	Aangezien er dit jaar geen behoefte is aan aanvullende externe financiering, worden potentiële risico's op dit moment niet verder besproken.	De noodzaak voor aanvullende financiering kan ook relevant zijn voor GGDrU, zodat de organisatie voldoende middelen heeft om haar diensten effectief te blijven aanbieden. De afhankelijkheid van externe financiering kan leiden tot een verhoogde schuldenlast, wat financiële druk kan uitoefenen op de organisatie. Dit kan ook resulteren in hogere rentelasten. Gezien het feit dat extra financiering voor dit jaar niet noodzakelijk is, wordt er op dit moment niet ingegaan op de potentiële risico's.			GGDrU hanteert een zorgvuldige afweging bij het nemen van financieringsbeslissingen. Dit betekent dat GGDrU gedegen evaluaties uitvoert om de noodzaak en impact van aanvullende financiering te bepalen, zonder overhaast te werk te gaan. Daarnaast heeft GGDrU een sterke focus op financiële stabiliteit, wat essentieel is voor het waarborgen van de continuïteit van haar diensten. Door risico's proactief te minimaliseren, toont GGDrU aan dat zij zich bewust is van de mogelijke problemen die kunnen voortvloeien uit externe financiering en hier zorgvuldig mee omgaat.		
• Het vermogen om schulden af te lossen of om te voldoen aan de voorwaarden in financieringsovereenkomst is aanzienlijk beperkt;	Op dit moment is er nog voldoende financiële ruimte, worden potentiële risico's met						

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
	betrekking tot het aflossen van schulden of het voldoen aan de voorwaarden in financierings-overeenkomsten niet verder besproken.						
• De verwachte of daadwerkelijke negatieve impact van het rapporteren van ongunstige financiële resultaten op belangrijke lopende transacties, waaronder**:** • **Contractuele Overeenkomsten**: Dit omvat lopende contracten met leveranciers, partners en klanten, zoals overeenkomsten voor de levering van diensten of producten; • **Financierings-overeenkomsten**: Lopende leningen, kredietovereen-komsten of andere vormen van externe financiering die regelmatig terugbetaald moeten worden; • **Inkomsten uit diensten**: Dit omvat inkomsten die voortkomen uit de	Ja	Deze risico's benadrukken de noodzaak voor GGDrU om proactief financieel beheer te voeren en transparant te communiceren over haar financiële situatie om het vertrouwen van alle belanghebbenden te behouden: **1. Contractuele overeenkomsten**: • **Verlies van Vertrouwen**: Slechte financiële resultaten kunnen leiden tot wantrouwen bij leveranciers en gemeenten, wat kan resulteren in het beëindigen van contracten of ongunstige voorwaarden; • **Hogere Kosten**: Leveranciers kunnen prijsverhogingen doorvoeren of weigeren verdere kredietverlening, waardoor de operationele kosten stijgen; **2. Financieringsovereenkomsten**: • **Verhoogde rentetarieven**: Ongunstige financiële resultaten kunnen de kredietwaardigheid van GGDrU schaden, wat leidt tot hogere rentetarieven bij	M tot H 😐☹	M tot H 😐☹	**1. Financieel beheer**: Strikte budgetterings- en kostenbewakingssystemen om financiële prestaties continu te monitoren. Dit helpt om afwijkingen tijdig te signaleren en aanpassingen te maken; **2. Risicobeheer**:Risicobeheerplannen dat mogelijke financiële en operationele risico's in kaart brengt en beheersmaatregelen definieert. Dit omvat regelmatige risicobeoordelingen en updates; **3. Interne controleprocessen**: Interne controles, zoals dubbele goedkeuring voor belangrijke uitgaven en regelmatige audits om de naleving van procedures te waarborgen en frauduleuze activiteiten te voorkomen; **4. Training en opleiding**: Regelmatige training van personeel over financiële normen en procedures, zodat medewerkers goed op de hoogte zijn van hun verantwoordelijkheden en de gevolgen van niet-naleving; **5. Transparante communicatie**: Het bevorderen van open communicatie over financiële prestaties en uitdagingen binnen de organisatie. Dit helpt bij het opbouwen van vertrouwen	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
diensten die GGDrU levert, zoals vaccinaties, gezondheidsinspecties en andere publieke gezondheidstaken; • **Onderhouds-contracten**: Overeenkomsten voor het onderhoud van apparatuur of infrastructuur die essentieel zijn voor de operationele werking van GGDrU zijn cruciaal om de continuïteit van haar diensten, zoals gezondheidszorg, preventie en infectieziektebestrijding, te waarborgen. Deze overeenkomsten zorgen ervoor dat medische apparatuur, informatiesystemen en andere infrastructuren regelmatig worden onderhouden en geüpdatet, wat bijdraagt aan een betrouwbare en effectieve werking. • **Subsidies en subsidieaan-vragen**: Lopende aanvragen voor overheidssubsidies of andere financiële		nieuwe leningen of herfinanciering van bestaande schulden; • **Beperkingen op financiering**: Kredietverleners kunnen terughoudender worden bij het verstrekken van nieuwe financieringen, wat de cashflow en investeringsmogelijkheden kan beïnvloeden; **3. Inkomsten uit Diensten**: • **Verminderde Vraag**: Slechte financiële prestaties kunnen het vertrouwen van de gemeenschap in de diensten van GGDrU ondermijnen, wat kan leiden tot een afname van de vraag naar essentiële diensten zoals vaccinaties en gezondheidsinspecties; • **Schade aan reputatie**: Negatieve publiciteit over financiële problemen kan de reputatie van GGDrU schaden, wat ook gevolgen kan hebben voor de inkomsten; **4. Onderhoudscontracten**: • **Verhoogde onderhoudskosten**: Onvoldoende financiering kan leiden tot het uitstellen van noodzakelijke onderhoudscontracten, waardoor de kosten op de lange termijn stijgen en			onder medewerkers en belanghebbenden; **6. Monitoring van externe betrekkingen**: Het actief volgen van relaties met leveranciers, financiers en gemeenten om eventuele problemen tijdig te signaleren en op te lossen; **7. Diversificatie van inkomsten**: Het ontwikkelen van nieuwe diensten of producten om de afhankelijkheid van één enkele inkomstenbron te verminderen, wat de financiële stabiliteit kan vergroten; **8. Feedbacksystemen**: Het inrichten van systemen voor het verzamelen van feedback van medewerkers en gemeenten om operationele inefficiënties en risico's vroegtijdig te identificeren.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
steun die essentieel kunnen zijn voor de werking en groei van de organisatie. • **Personeelskosten**: Regelmatige uitgaven die verband houden met salarissen, sociale lasten en andere personeelsgerelateerde kosten.		apparatuur of infrastructuur kan falen; • **Operationele storing**: Niet-naleving van onderhoudscontracten kan resulteren in operationele onderbrekingen en verhoogde uitgaven voor noodreparaties; **5. Subsidies en subsidieaanvragen**: • **Moeilijkheden bij subsidieaanvragen**: Slechte financiële resultaten kunnen het moeilijk maken om subsidies te verkrijgen, wat essentieel is voor het uitvoeren van bepaalde programma's en initiatieven; • **Beperkingen in projectfinanciering**: Terugtrekking van subsidies door overheden of andere instanties; **6. Personeelskosten**: • **Salarisbeperkingen**: Ongunstige financiële resultaten kunnen leiden tot bezuinigingen op personeelskosten, wat het moreel en de motivatie van medewerkers kan beïnvloeden; • **Personeelsverloop**: Onzekerheid over de financiële gezondheid kan leiden tot een hoger verloop, wat extra kosten met zich					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		meebrengt voor werving en training van nieuw personeel.					
Acties voor verbetering Door deze acties te implementeren, kan GGDrU de potentiële risico's minimaliseren en haar operationele en financiële prestaties verbeteren. Het is essentieel dat de organisatie zich proactief opstelt en blijft investeren in zowel processen als mensen om haar doelen te bereiken en het vertrouwen van belanghebbenden te behouden: • **Versterken van financieel beheer**: Door gebruik te maken van geavanceerde software voor budgettering kan GGDrU de financiële planning verbeteren en beter anticiperen op toekomstige uitgaven en inkomsten; • **Risicoanalyse en monitoring**: Periodieke risicobeoordelingen uitvoeren om nieuwe risico's te identificeren en bestaande risico's te herbeoordelen. Dit helpt bij het vroegtijdig signaleren van problemen; • **Training en ontwikkeling**: Trainingen aanbieden die gericht zijn op zowel financiële als operationele competenties. Dit verhoogt de bewustwording van risico's en versterkt de naleving van interne processen; • **Verbeteren van interne controleprocessen**: Extra controles invoeren, zoals onafhankelijke audits en kwaliteitscontroles, om te zorgen dat processen en procedures effectief worden nageleefd; • **Transparante communicatie**: Open communicatie tussen verschillende afdelingen en met externe stakeholders (dit verwijst naar individuen, groepen of organisaties die belang hebben bij of invloed uitoefenen op een bepaalde kwestie, project of organisatie). Dit helpt om misverstanden te voorkomen en bevordert samenwerking; • **Diversificatie van inkomsten**: Onderzoeken en implementeren van nieuwe diensten of producten die aansluiten bij de behoeften van inwoners, om de afhankelijkheid van een enkele inkomstenbron te verminderen; • **Feedbacksystemen**: Regelmatig onderzoeken uitvoeren om feedback van gemeenten en medewerkers te verzamelen. Gebruik deze informatie om verbeteringen aan te brengen in de dienstverlening en operationele processen; • **Strategische planning**: Strategische plannen ontwikkellen die de organisatie voorbereiden op toekomstige uitdagingen en kansen, inclusief financiële stabiliteit en groei; • **Externe relaties beheren**: Relaties onderhouden om vertrouwen op te bouwen en eventuele problemen vroegtijdig aan te pakken; • **Gebruik van technologie**: Gebruik maken van technologie om processen te automatiseren en data-analyse te verbeteren, wat kan helpen bij het maken van beter onderbouwde beslissingen.							
1.1.3 De beschikbare gegevens wijzen erop dat de persoonlijke financiële situatie van leden van het management en personen die verantwoordelijk zijn voor governance, onder druk staat door de financiële prestaties van GGDrU. Governance verwijst naar het geheel van processen, regels en structuren die bepalen hoe een organisatie wordt geleid		Er zijn verschillende risico's voor GGDrU die verband houden met governance om de integriteit en effectiviteit van GGDrU te waarborgen. Hieronder een opsomming van deze risico's: 1. **Gebrek aan transparantie**: Onvoldoende communicatie over financiële en operationele prestaties kan leiden tot wantrouwen bij stakeholders en een verslechtering van de relatie met de gemeenschap;					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
en gecontroleerd. Het omvat de manier waarop beslissingen worden genomen, hoe verantwoordelijkheden worden verdeeld, en hoe verantwoording wordt afgelegd, waaronder:		2. **Verantwoordingsplicht**: Als leden van het management of bestuur niet goed verantwoording afleggen, kan dit leiden tot juridische problemen en reputatieschade; 3. **Inadequaat risicobeheer**: Gebrek aan effectieve risicobeheerprocessen kan ervoor zorgen dat GGDrU niet adequaat kan reageren op financiële of operationele crises; 4. **Ethische schendingen**: Het niet naleven van ethische normen kan leiden tot schandalen en verlies van vertrouwen bij zowel interne als externe stakeholders; 5. **Regelgeving en compliance**: Het niet voldoen aan relevante wet- en regelgeving kan resulteren in boetes, sancties of andere juridische repercussies; 6. **Interne conflicten**: Onenigheid binnen het management of tussen bestuursleden kan leiden tot inefficiënte besluitvorming en strategie-implementatie.					
• Significante bestanddelen van hun beloning (zoals bonussen) zijn gekoppeld aan het bereiken van ambitieuze doelstellingen met betrekking tot de operationele resultaten, de financiële positie of de kasstromen;	Er zijn momenteel geen potentiële risico's geïdentificeerd.	GGDrU werkt niet met bonussen, waardoor potentiële risico's die verband houden met prestatie-afhankelijke beloningen aanzienlijk beperkt blijven. Dit helpt om een stabiele werkomgeving te creëren waarin de focus ligt op het leveren van kwaliteit en het waarborgen van de financiële gezondheid zonder de druk van ambitieuze doelstellingen die financiële prikkels met zich meebrengen.					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• Verstrekte persoonlijke borgstellingen voor de schulden van GGDrU verwijzen naar de garanties die individuen of bestuurders geven om de financiële verplichtingen van de organisatie te dekken;	Aangezien GGDrU geen persoonlijke borgstellingen hanteert, zijn de potentiële risico's die hiermee gepaard gaan beperkt.	Dit betekent dat er geen persoonlijke aansprakelijkheid is voor bestuurders of medewerkers in het geval van financiële verplichtingen van de organisatie. Hierdoor blijft de financiële druk op individuen laag, wat de focus op de operationele taken en verantwoordelijkheden vergemakkelijkt.					
• Druk op het management en uitvoerend personeel om de financiële doelstellingen te behalen die zijn vastgesteld door de personen verantwoordelijk voor het governance-proces.	Ja	Deze risico's benadrukken het belang van een evenwichtige benadering van financiële doelstellingen, waarbij zowel de financiële prestaties als de kwaliteit van dienstverlening en het welzijn van het personeel in overweging worden genomen: **1. Besluitvorming onder druk**: De stress om financiële doelstellingen te bereiken kan leiden tot impulsieve of slecht doordachte beslissingen. Dit kan resulteren in onethisch gedrag of het negeren van belangrijke procedurele stappen; **2. Verlies van motivatie en moraal**: Als het personeel zich constant onder druk gezet voelt om resultaten te leveren, kan dit leiden tot burn-out, verminderde werktevredenheid en hogere personeelsverloop. **3. Kwaliteit van de dienstverlening**: De focus op het behalen van financiële doelstellingen kan ten koste gaan van de kwaliteit van de geleverde diensten. Het personeel kan geneigd zijn om shortcuts te	M 	H 	• **Evenwichtige prestatie-indicatoren**: Een set van prestatie-indicatoren, die niet alleen financiële resultaten, maar ook kwaliteitsnormen voor dienstverlening en medewerkerstevredenheid in overweging neemt. Dit helpt bij het creëren van een bredere focus en vermindert de druk om uitsluitend financiële doelen te behalen. • **Training en ontwikkeling**: Trainingen voor het management en medewerkers, gericht op ethische besluitvorming, stressmanagement en effectief communiceren. Opleidingsprogram-ma's maken medewerkers bewust van ethische normen. Stressmanagement en effectief communiceren kan helpen bij het verbeteren van de besluitvorming en het verminderen van de impact van druk; • **Regelmatige evaluatie van doelstellingen**: Regelmatig evaluaties van gestelde financiële doelstellingen en de impact ervan	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		nemen of de aandacht voor klanttevredenheid te verwaarlozen. 4. **Reputatieschade**: Als financiële druk leidt tot negatieve uitkomsten, zoals slechte dienstverlening of schandalen, kan dit de reputatie van GGDrU schaden en het vertrouwen van de gemeenschap ondermijnen. 5. **Compliance-risico's**: Bij het streven naar financiële doelen kunnen wettelijke en ethische richtlijnen worden genegeerd, wat kan leiden tot juridische problemen en sancties. .			op de organisatie. Dit kan helpen bij het identificeren van eventuele negatieve gevolgen en het aanpassen van de doelstellingen indien nodi; • **Open communicatie**: Cultuur van openheid en transparantie waar medewerkers hun zorgen kunnen uiten zonder angst voor repercussies. Dit kan helpen om problemen vroegtijdig te signaleren en aan te pakken; • **Ondersteuning van welzijn van medewerke**rs: Programma's voor het welzijn van medewerkers, zoals counseling, flexibele werktijden en teamuitjes. Dit kan bijdragen aan een betere werk-privébalans en de algehele moraal verbeteren; • **Risicoanalyse en -beheersing**: Regelmatige risico-inventarisatie bij het identificeren van potentiële risico's en compliance-issues; • **Interne audits**: Naleving van beleid en procedures; • **Feedbackmechanismen**: medewerkers kunnen zorgen uiten zonder angst voor repercussies, wat een open cultuur bevordert. • **Het gebruik van technologie en software**: Om compliance-activiteiten te volgen en rapporten te genereren. Dit kan helpen bij het tijdig identificeren van risico's en afwijkingen.		
Acties voor verbetering							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Een evenwichtige benadering van financiële en niet-financiële doelstellingen, zoals klanttevredenheid en medewerkerswelzijn, om de druk op financiële resultaten te verminderen., evenals de noodzaak voor transparante communicatie en ondersteunend leiderschap. Het implementeren van stressmanagementprogramma's en regelmatige feedbacksystemen is cruciaal om de druk op personeel te verminderen en de algehele organisatiecultuur te verbeteren.							
1.2 Gelegenheid	**De factor gelegenheid verwijst naar de omstandig-heden die individuen in staat stellen om fraude te plegen.**	Voor GGDrU betekent dit dat er adequate interne controles en procedures moeten zijn om te voorkomen dat medewerkers misbruik maken van hun positie, vooral in situaties waar toegang tot middelen en informatie niet goed wordt gecontroleerd.					
1.2.1 De activiteiten van GGDrU bieden kansen voor frauduleuze financiële verslaggeving door de complexiteit van financiële transacties en beperkte interne controles. Een gebrek aan transparantie en toezicht kan eveneens bijdragen aan het risico op manipulatie van financiële gegevens. Het is cruciaal dat GGDrU sterke controlesystemen instelt en een cultuur van integriteit bevordert om deze risico's te verkleinen, waaronder:		Bij GGDrU zijn er verschillende risico's verbonden aan gelegenheid voor frauduleuze financiële verslaggeving, waaronder: • **Manipulatie van financiële gegevens**: Individuen kunnen financiële gegevens aanpassen om een beter financieel resultaat te presenteren, wat kan leiden tot onjuiste informatie aan belanghebbenden; • **Onvoldoende interne controles**: Gebrek aan adequate interne controles maakt het makkelijker voor medewerkers om frauduleuze activiteiten uit te voeren zonder dat dit snel wordt opgemerkt; • **Verlies van Vertrouwen**: Als frauduleuze activiteiten aan het licht komen, kan dit leiden tot een verlies van vertrouwen van de gemeenschap en andere belanghebbenden, wat schadelijk is voor de reputatie van GGDrU;					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		• **Wettelijke Gevolgen**: Fraude kan leiden tot juridische consequenties, inclusief boetes en rechtszaken, wat ook financiële implicaties voor de organisatie kan hebben; • **Impact op de kwaliteit van diensten**: De focus op het verbergen van financiële problemen kan ten koste gaan van de kwaliteit van de aangeboden diensten, wat uiteindelijk nadelig is voor de gemeenschap die GGDrU bedient.					
• Transacties met verbonden partijen die significant zijn en buiten de normale bedrijfsvoering vallen, evenals transacties met verbonden partijen die mogelijk door een ander auditkantoor worden gecontroleerd. Een verbonden partij is een rechtspersoon waarin GGDrU zowel een bestuurlijk als een financieel belang heeft;	GGDrU heeft geen verbonden partijen.	Verbonden partijen zijn organisaties waaraan GGDrU zich bestuurlijk en financieel verbindt. Verbonden partijen bestaan uit deelnemingen door GGDrU in gemeenschappelijke regelingen, NV's, BV's, stichtingen, verenigingen, coöperaties en Publiek Private Samenwerking constructies. Omdat GGDrU geen verbonden partijen heeft, zijn de potentiële risico's die gewoonlijk samenhangen met transacties met deze partijen aanzienlijk verminderd. Dit betekent dat de organisatie minder blootgesteld is aan conflicten van belang en risico's met betrekking tot de transparantie en integriteit van financiële transacties.					
• Een sterke financiële positie van GGDrU kan haar in staat stellen om invloed uit te oefenen op leveranciers of gemeenten, wat kan leiden tot het opleggen van voorwaarden	Ja	Het is van groot belang dat GGDrU transparante en eerlijke voorwaarden hanteert in al haar zakelijke relaties. Door dit te doen, kan de organisatie de risico's van ongepast gedrag minimaliseren en een ethische bedrijfsvoering waarborgen. Dit vraagt	L 	L 	Toch blijft het belangrijk voor GGDrU om alert te blijven op deze risico's en proactief maatregelen te nemen om mogelijke ongepaste situaties te voorkomen. Het ontwikkelen van duidelijke inkoopprocedures en het onderhouden van goede relaties met leveranciers zijn cruciaal	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
die mogelijk niet in lijn zijn met marktstandaarden. Dit kan resulteren in ongepaste of niet-transparante transacties, waarbij de integriteit van de organisatie in gevaar kan komen. Het is belangrijk dat GGDrU transparante en eerlijke voorwaarden hanteert in haar zakelijke relaties om dergelijke risico's te vermijden en een ethische bedrijfsvoering te waarborgen;		om een voortdurende evaluatie van de bedrijfsrelaties en het handhaven van hoge standaarden in alle transacties: 1. **Contractuele druk:** Een sterke financiële positie kan GGDrU in staat stellen om onredelijke contractvoorwaarden op te leggen. Dit kan leiden tot wrok bij leveranciers en mogelijk resulteren in juridische geschillen of onderbrekingen in de levering van diensten of producten; 2. **Afhankelijkheid van specifieke leveranciers:** Indien GGDrU voorwaarden oplegt die bepaalde leveranciers bevoordelen, kan dit leiden tot een ongezonde afhankelijkheid van deze leveranciers. Dit verhoogt het risico op verstoringen in de toeleveringsketen, vooral als die leveranciers problemen ondervinden; 3. **Reputatierisico:** Het kan de reputatie van GGDrU schaden als blijkt dat zij niet transparant handelt in haar relaties De kans op de bovengenoemde risico's voor GGDrU is over het algemeen laag. Dit komt omdat GGDrU een publieke organisatie is die onderhevig is aan strikte regelgeving en toezicht, wat helpt bij het beperken van ongeschikte transacties en ongepaste druk. Bovendien zijn er vaak mechanismen en richtlijnen, die ervoor zorgen dat bijvoorbeeld inkoopprocessen transparant en			om de kans op dergelijke risico's verder te minimaliseren. Voor GGDrU kunnen de volgende beheersmaatregelen relevant zijn om risico's, zoals ongepaste transacties met leveranciers, te minimaliseren: 1. **Transparante inkoopprocedures**: Duidelijke richtlijnen en processen voor inkoop die zorgen voor eerlijke concurrentie en transparantie bij het selecteren van leveranciers; 2. **Compliance en toezicht**: Regelmatig audits en toezicht op de naleving van inkoop- en contractuele verplichtingen om ervoor te zorgen dat de organisatie zich houdt aan relevante wet- en regelgeving; 3. **Leveranciersbeoordeling**: Grondige beoordelingen van leveranciers voordat contracten worden afgesloten, inclusief financiële stabiliteit, reputatie en naleving van normen; 4. **Training en opleiding**: Training medewerkers over ethische inkooppraktijken en hoe te handelen bij mogelijke belangenconflicten; 5. **Feedback- en klachtmechanismen**: Kanalen voor medewerkers en externe partijen om zorgen of overtredingen te melden zonder angst voor repercussies; 6. **Risico-inventarisatie**: Regelmatig beoordelen van de		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		eerlijk verlopen.Toch blijft het belangrijk voor GGDrU om alert te blijven op deze risico's en proactief maatregelen te nemen om mogelijke ongepaste situaties te voorkomen. Het ontwikkelen van duidelijke inkoopprocedures en het onderhouden van goede relaties zijn cruciaal om de kans op dergelijke risico's verder te minimaliseren.			risico's verbonden aan zakelijke relaties en het opstellen van een plan om deze risico's te mitigeren; 7. **Contractuele clausules**: Het opnemen van specifieke clausules in contracten die gedragsnormen en consequenties bij schendingen vastleggen.		
Acties voor verbetering Door deze acties te ondernemen, kan GGDrU de risico's van ongepaste transacties verder minimaliseren en de integriteit van haar zakelijke relaties waarborgen: 1. **Onafhankelijke audits**: Regelmatige onafhankelijke audits van leveranciersrelaties kunnen helpen om de naleving van voorwaarden en transparantie te waarborgen. Dit creëert een extra laag van controle en helpt om eventuele ongepaste transacties te identificeren; 2. **Training en bewustwording**: Het implementeren van trainingen voor medewerkers en betrokken stakeholders over ethische inkooppraktijken en het belang van transparantie kan helpen om een cultuur van integriteit binnen de organisatie te bevorderen; 3. **Stakeholderdialoog**: Actieve dialoog met verschillende stakeholders, daarbij werkt GGDrU in de regio Utrecht samen met bijvoorbeeld huisartsen, welzijnsorganisaties, scholen, politie en zorginstellingen., kan helpen om verwachtingen helder te krijgen en ervoor te zorgen dat de voorwaarden eerlijk en transparant zijn; 4. **Beleid voor verantwoord inkopen**: Het ontwikkelen en implementeren van een beleid voor verantwoord inkopen dat richtlijnen geeft voor het omgaan met leveranciers, kan ervoor zorgen dat alle transacties voldoen aan ethische standaarden; 5. **Klokkenluiderssystemen**: Het opzetten van een klokkenluiderssysteem waarin medewerkers en leveranciers verdachte activiteiten kunnen melden zonder angst voor repercussies, kan bijdragen aan het waarborgen van transparantie en integriteit; 6. **Evaluatie van leverancierscriteria**: Het aanpassen van de selectiecriteria voor leveranciers, zodat niet alleen financiële, maar ook ethische en transparante bedrijfsvoering worden meegenomen, kan helpen om ongepaste transacties te voorkomen; 7. **Regelmatige rapportage**: Het implementeren van een systeem voor regelmatige rapportage en monitoring van leverancierspresta ties kan helpen om eventuele afwijkingen tijdig te signaleren en aan te pakken.						
• Activa, verplichtingen, opbrengsten of kosten die gebaseerd zijn op significante schattingen, waarbij de berekeningen sterk afhankelijk zijn van subjectieve oordelen of onzekerheden die moeilijk te verifiëren zijn;	Ja	GGDrU kan hier een potentieel risico lopen. Activa, verplichtingen, opbrengsten of kosten die zijn gebaseerd op significante schattingen, vooral wanneer ze afhankelijk zijn van subjectieve oordelen of onzekerheden, kunnen leiden tot financiële onnauwkeurigheden of verkeerde interpretaties. Dit soort inschattingen maakt het moeilijk om financiële resultaten te verifiëren en kan risico's met zich meebrengen, zoals:	M 	H 	1. **Strikte interne controles**: Interne controleprocessen rondom schattingen en boekhoudkundige beslissingen, met duidelijke goedkeuringsniveaus en periodieke evaluaties door onafhankelijke partijen; 2. **Documentatie van schattingen**: Uitgebreide documentatie van de aannames, methodologieën en gegevens die worden gebruikt om financiële schattingen te onderbouwen, zodat deze	L tot M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		• **Foutieve rapportages**: Wanneer schattingen verkeerd blijken te zijn, kunnen de financiële resultaten onbetrouwbaar worden. • **Wettelijke en compliance risico's**: Onjuiste inschattingen kunnen leiden tot niet-naleving van financiële richtlijnen of wettelijke verplichtingen. • **Verlies van vertrouwen**: Stakeholders, zoals gemeenten of samenwerkingspartners, kunnen vertrouwen verliezen in de financiële stabiliteit en integriteit van GGDrU.			transparant zijn en kunnen worden gevalideerd; 3. **Externe toetsing**: Regelmatig externe audits, die helpen bij het valideren van financiële schattingen en het identificeren van risico's en verband houden met subjectieve beoordelingen; 4. **Scenarioanalyses**: Verschillende scenarioanalyses om te evalueren hoe veranderingen in aannames de financiële cijfers kunnen beïnvloeden. Dit helpt bij het inschatten van mogelijke afwijkingen; 5. **Opleiding en training**: Om medewerkers en management goed op de hoogte van de risico's van subjectieve schattingen en onzekerheden te laten zijn en hen bewust maken van het belang van nauwkeurigheid en transparantie; 6. **Periodieke herbeoordeling**: Regelmatig herbeoordeling van de aannames en schattingen, vooral bij veranderingen in externe omstandigheden of in de organisatie zelf, kan helpen om eventuele afwijkingen tijdig op te sporen.		

Acties voor verbetering

De volgende acties kunnen worden ondernomen om schattingen en subjectieve oordelen binnen het financiële beheer te verbeteren:

1. **Periodieke evaluatie van schattingen**: GGDrU kan regelmatig de belangrijkste schattingen herzien en bijstellen, vooral in het kader van veranderingen in publieke gezondheidszorg, wetgeving, of financieringsmodellen die onzekerheid met zich meebrengen;
2. **Externe validatie en consultatie**: Door het betrekken van externe specialisten of auditors voor gevoelige schattingen, kan GGDrU de objectiviteit en betrouwbaarheid van financiële rapportages verhogen;
3. **Training van financieel personeel**: Opleidingen en workshops gericht op het verbeteren van de capaciteiten van medewerkers, vooral rond financiële schattingen en modellen, kunnen helpen om beter onderbouwde beslissingen te nemen;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
4. **Scenario-planning in de zorgsector**: GGDrU kan gebruikmaken van scenario-analyse om verschillende uitkomsten te simuleren bij het maken van financiële schattingen. Dit helpt om goed voorbereid te zijn op schommelingen in bijvoorbeeld vaccinatiecampagnes of zorguitgaven.							
• Bij GGDrU kunnen significante, ongebruikelijke of zeer complexe transacties voorkomen, vooral transacties die vlak voor het einde van een verslagperiode plaatsvinden met gelieerde partijen, leiden tot complicaties waarbij de economische realiteit belangrijker is dan de juridische structuur. Het is van cruciaal belang dat GGDrU de economische werkelijke waarde van deze transacties correct weergeeft, zodat financiële rapportages een realistisch beeld geven en mogelijke misstanden en worden voorkomen. Bij het verwerken van dergelijke transacties moet dus worden gefocust op de economische substantie boven formele juridische kenmerken om integriteit en transparantie te waarborgen;	Ja	Dit principe houdt in dat: 1. Substantie boven vorm: De focus ligt op de werkelijke inhoud en uitkomsten van de transactie, in plaats van op hoe deze juridisch is vormgegeven; 2. Economische impact: De economische resultaten, zoals winst, risico's en voordelen voor de betrokken partijen, zijn bepalend voor de beoordeling van de transactie, ongeacht hoe deze juridisch is gestructureerd; 3. Beoordeling van transacties: In sommige gevallen kunnen transacties die juridisch gezien op een bepaalde manier zijn ingericht, in de praktijk andere gevolgen hebben. Bijvoorbeeld, een transactiestructuur die bedoeld is om belastingvoordelen te behalen, kan als niet-legitiem worden beschouwd als de economische realiteit dit niet ondersteunt; 4. Regelgeving en transparantie: Dit principe wordt vaak gebruikt om te voorkomen dat partijen misbruik maken van juridische structuren om economische verplichtingen	M 	H 	• **Duidelijke richtlijnen**: Heldere richtlijnen en procedures op voor het omgaan met complexe en ongebruikelijke transacties; • **Interne controles**: Interne controles om het toezicht op transacties te waarborgen en risico's tijdig te identificeren; • **Training en bewustwording**: Trainingen aan medewerkers over de juiste verwerking van financiële transacties en de noodzaak van transparantie; • **Evaluatie en monitoring**: Regelmatig evaluaties van significante transacties en monitoren naleving van de richtlijnen; • **Externe audits**: Onafhankelijke externe audits om de integriteit van de financiële verslaggeving te waarborgen en potentiële risico's te identificeren.	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		of verantwoordelijkheden te ontlopen. GGDrU dient hierbij rekening te houden met een aantal potentiële risico's: • Misinterpretatie van economische realiteit: Het risico dat de economische werkelijke waarde van een transactie niet correct wordt weergegeven in de financiële rapportages, wat kan leiden tot verkeerde besluitvorming en een verstoord beeld van de financiële gezondheid van de organisatie; • Fraude en onregelmatigheden: De complexiteit van dergelijke transacties kan het risico op frauduleuze activiteiten vergroten, vooral als er onvoldoende interne controles zijn. • Regelgevingsrisico's: Het niet correct rapporteren van deze transacties kan leiden tot nalevingsproblemen, wat juridische en financiële gevolgen kan hebben voor GGDrU. • Reputatieschade: Als de transacties als ongepast of niet-transparant worden gezien, kan dit de reputatie van GGDrU schaden en het vertrouwen van belanghebbenden ondermijnen.					
Acties voor verbetering GGDrU kan verschillende acties ondernemen om de risico's van significante, ongebruikelijke of complexe transacties te beheersen en om te waarborgen dat de economische realiteit van deze transacties correct wordt weergegeven. Hier zijn enkele aanbevelingen: 1. **Beleidsontwikkeling**:							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ Ontwikkel duidelijke richtlijnen en beleid voor de verwerking van complexe transacties, waarbij de nadruk ligt op de noodzaak om de economische realiteit boven de juridische structuur te prioriteren; 2. **Training en Opleiding**: ○ Bied trainingen aan voor personeel dat betrokken is bij financiële transacties om hen bewust te maken van de risico's en hen te onderwijzen over het belang van transparantie en ethische overwegingen; 3. **Interne Controles**: ○ Implementeer striktere interne controles en goedkeuringsprocessen voor transacties met gelieerde partijen, vooral als deze vlak voor het einde van de verslagperiode plaatsvinden.							
• Significante activiteiten die plaatsvinden in het buitenland of grensoverschrijdende activiteiten in jurisdicties met verschillende bedrijfsomgevingen of bedrijfsculturen;	Ja	• In verschillende landen gelden verschillende regels voor de heffing en terugvordering van btw. Dit kan leiden tot complicaties in de btw-administratie en mogelijk tot onjuiste aangiften, wat resulteert in boetes of naheffingen door de belastingautoriteiten. • Fluctuaties in wisselkoersen kunnen invloed hebben op de waarde van de transacties, wat kan resulteren in onverwachte kosten of verliezen.	M 😐	H ☹	Het is belangrijk dat GGDrU zich bewust is van deze risico's en passende maatregelen neemt om ze te beheersen, zoals het verbeteren van interne controles, regelmatig overleg met belastingadviseurs en het ontwikkelen van duidelijke richtlijnen voor grensoverschrijdende transacties.	M 😐	Ja
Acties voor verbetering GGDrU kan de risico's van grensoverschrijdende transacties met crediteuren minimaliseren door duidelijke contracten te hanteren, uitgebreide due diligence uit te voeren en medewerkers op te leiden in internationale handelspraktijken. Due diligence is het proces van zorgvuldige inspectie en beoordeling dat wordt uitgevoerd door individuen of organisaties voordat ze een zakelijke transactie of overeenkomst aangaan. Daarnaast is het essentieel om te voldoen aan lokale wet- en regelgeving en veilige betalingsstructuren te implementeren om financiële risico's en compliance-issues te beheersen.							
• De inschakeling van zakelijke tussenpersonen zonder duidelijke zakelijke redenen kan voor GGDrU een risicofactor zijn. Dit kan leiden tot ondoorzichtige transacties en een gebrek aan verantwoordelijkheid, wat de integriteit van de organisatie in gevaar kan brengen. Het is essentieel	Ja	Het is van belang dat GGDrU een grondige evaluatie uitvoert van de rol en noodzaak van dergelijke tussenpersonen om risico's te minimaliseren en transparantie te waarborgen. Het inschakelen van professionals die advies geven zonder duidelijke reden of toegevoegde waarde kan een risico vormen voor GGDrU. Dit kan leiden tot ondoorzichtige uitgaven, inefficiëntie en zelfs reputatieschade.	M 😐	M 😐	• **Duidelijke criteria voor inschakeling**: Strikte richtlijnen voor het inschakelen van externe adviseurs, waaronder de noodzaak voor een duidelijke zakelijke reden en de verwachte toegevoegde waarde; • **Grondige evaluatie en due diligence**: Gedetailleerde beoordeling van de kwalificaties en de reputatie van de adviseurs. Dit kan helpen om te bevestigen dat	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
dat GGDrU de noodzaak van tussenpersonen goed evalueert en ervoor zorgt dat hun rol transparant en gerechtvaardigd is, om risico's van corruptie of misbruik te minimaliseren;		Naast de risicofactoren die voortkomen uit de inschakeling van zakelijke tussenpersonen, bestaat in deze context ook een aanzienlijk risico met betrekking tot de handhaving op schijnzelfstandigheid. **Risico van handhaving op Schijnzelfstandigheid**: Met de invoering van de volledige handhaving door de Belastingdienst op schijnzelfstandigheid per 1 januari 2025, lopen bedrijven en organisaties het risico op boetes en naheffingen wanneer zij zzp'ers inschakelen voor werk dat zij niet zelfstandig uitvoeren. Hoewel er een overgangsperiode van één jaar is waarin werkgevers en werkenden geen vergrijpboete krijgen als ze kunnen aantonen dat ze actie ondernemen tegen schijnzelfstandigheid, blijft er een risico bestaan dat de handhaving leidt tot financiële gevolgen en juridische complicaties voor de betrokken partijen. Deze maatregel, onderdeel van de kabinetsinitiatieven om schijnconstructies te bestrijden, kan invloed hebben op de zekerheid binnen de arbeidsmarkt en de manier waarop bedrijven hun arbeidsrelaties vormgeven.			hun expertise relevant en noodzakelijk is; • **Transparante documentatie**: Duidelijke en gedetailleerde documentatie van alle besluiten om externe adviseurs in te schakelen, inclusief de specifieke reden en verwachte resultaten; • **Regelmatige audits en beoordelingen**: Regelmatig audits op de uitgaven voor adviesdiensten en beoordeling van de resultaten van hun bijdragen aan de organisatie. Dit helpt bij het identificeren van onnodige of ineffectieve uitgaven; • **Stakeholderbetrokkenheid**: Relevante belanghebbenden, zoals team financiën en de operationele teams, bij de besluitvorming over het inschakelen van externe adviseurs betrekken om ervoor te zorgen dat er consensus is over de noodzaak en waarde; • **Training en bewustwording**: Medewerkers die betrokken zijn bij het proces van het inschakelen van externe adviseurs zijn op de hoogte van de risico's en de juiste procedures om potentiële risico's te vermijden.		
Acties voor verbetering GGDrU kan de risico's van het inschakelen van externe professionals minimaliseren door duidelijke selectiecriteria te hanteren en due diligence uit te voeren om hun waarde te verifiëren. Daarnaast is het belangrijk om contractuele afspraken te maken over verwachte resultaten en om regelmatig de effectiviteit van hun diensten te evalueren. Door transparante communicatie en training voor interne medewerkers te implementeren, kan GGDrU de samenwerking met professionals optimaliseren en de risico's beter beheersen. Door deze **aanvullende acties** te implementeren, kan GGDrU het risico van boetes en naheffingen als gevolg van schijnzelfstandigheid effectief verminderen:							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
1. **Opstellen van duidelijke Contracten**: Zorg voor heldere contracten met zzp'ers waarin de aard van de werkzaamheden en hun zelfstandigheid expliciet worden vastgelegd; 2. **Regelmatige evaluatie van werkzaamheden**: Voer periodieke evaluaties uit van de werkzaamheden van ingehuurde zzp'ers om te bevestigen dat zij zelfstandig opereren en niet onder directe leiding van de opdrachtgever werken; 3. **Bieden van training en boorlichting**: Organiseer trainingen en voorlichtingssessies voor medewerkers en management over de regels rondom zelfstandigheid en schijnzelfstandigheid om het bewustzijn te vergroten en risico's te minimaliseren; 4. **Documenteren van acties**: Houd gedetailleerde documentatie bij van de stappen die zijn ondernomen om schijnzelfstandigheid tegen te gaan, zoals het verstrekken van contracten en de evaluatie van zzp'ers; 5. **Raadplegen van experts**: Schakel juridische en fiscale experts in voor advies over het correct inhuren van zzp'ers en het beoordelen van contracten; 6. **Benutten van de overgangsperiode**: Maak actief gebruik van de overgangsperiode door stappen te ondernemen tegen schijnzelfstandigheid en deze acties goed te documenteren, zodat compliance kan worden aangetoond; 7. **Herzien van het inhuurbeleid**: Evalueer en herzie het inhuurbeleid om ervoor te zorgen dat het voldoet aan de nieuwe richtlijnen en wetgeving met betrekking tot zelfstandigheid; 8. **Ontwikkelen van een risicomanagementplan**: Stel een risicomanagementplan op dat specifiek gericht is op het risico van schijnzelfstandigheid, inclusief procedures voor identificatie, beoordeling en mitigatie van deze risico's.						
• Bankrekeningen of activiteiten met dochterondernemingen of nevenvestigingen waarvoor geen duidelijke zakelijke rechtvaardiging bestaat.	Er zijn geen potentiële risico's te melden.	GGDrU heeft geen dochtermaatschappijen of nevenvestigingen. Dit minimaliseert de kans op ongebruikelijke transacties of het ontbreken van duidelijke zakelijke rechtvaardigingen, wat de integriteit van de organisatie versterkt.					
1.2.2 De monitoring van het management is niet effectief om verschillende redenen: 1. **Ontbreken van duidelijke procedures**: Het gebrek aan gestandaardiseerde procedures voor het toezicht op managementactiviteiten kan leiden tot inconsistentie en verwarring over verantwoordelijkheden; 2. **Inadequate rapportagesystemen**: Als		Wanneer deze monitoring niet effectief is, kunnen er verschillende risico's ontstaan, zoals: 1. **Onvoldoende toezicht**: Een gebrek aan adequate controlemechanismen kan leiden tot ongewenste of onethische beslissingen. Als GGDrU niet in staat is om haar management effectief te monitoren, kunnen er risico's ontstaan, zoals fraude of ongepaste uitgaven; 2. **Onvoldoende rapportage**: Zonder effectieve monitoring kunnen belangrijke financiële en operationele rapportages					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
de rapportagesystemen niet betrouwbaar of transparant zijn, kan dit resulteren in onvolledige of onnauwkeurige informatie, waardoor belangrijke besluiten niet goed gefundeerd zijn; 3. **Onvoldoende toegang tot Informatie**: Een gebrek aan toegang tot relevante gegevens voor de toezichthouders kan hen verhinderen om weloverwogen beoordelingen van het management uit te voeren; 4. **Beperkte feedback-mechanismen**: Als er geen effectieve feedbackkanalen zijn, kan het management niet adequaat worden aangemoedigd om prestaties te verbeteren of om te leren van fouten; 5. **Communicatiehinder-nissen**: Een organisatiecultuur die niet openstaat voor feedback of waar medewerkers zich niet vrij voelen om zorgen te uiten, kan de effectiviteit van de monitoring ondermijnen;		onvolledig of onnauwkeurig zijn. Dit kan resulteren in misleidende informatie voor belanghebbenden en een gebrek aan vertrouwen in de organisatie; 3. **Weinig verantwoording**: Een tekortkoming in het toezicht kan leiden tot een cultuur waarin medewerkers zich niet verantwoordelijk voelen voor hun acties, wat kan resulteren in onethisch gedrag of nalatigheid; 4. **Risico op slechte besluitvorming**: Als het management niet effectief wordt gemonitord, kan dit leiden tot slechte strategische keuzes, gebaseerd op incomplete of onbetrouwbare informatie.					
• Het management kan worden gedomineerd door één persoon of een kleine groep individuen, zonder	Er zijn geen potentiële risico's voor GGDrU met	De situatie waarbij het management gedomineerd wordt door één persoon of een kleine groep individuen, zonder dat er adequate interne					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
dat er adequate interne beheersmaatregelen zijn getroffen om deze situatie te compenseren;	betrekking tot de dominantie van het management door één persoon of een kleine groep.	beheersmaatregelen zijn genomen, is niet relevant voor GGDrU.					
• Het toezicht door de personen, die verantwoordelijk zijn voor governance op het proces van financiële verslaggeving en de interne beheersmaatregelen, is niet effectief.	Potentiële risico's nihil voor GGDrU. Het toezicht op het proces van financiële verslaggeving en de interne beheersmaatregelen, uitgevoerd door de verantwoordelijken voor governance, lijkt effectief te zijn. Toch is het van belang om regelmatig evaluaties uit te voeren om mogelijke risico's tijdig te signaleren en te mitigeren. Hierdoor kan de organisatie zich beter beschermen tegen potentiële problemen en de effectiviteit	Adequate structuren en processen zorgen voor een effectieve monitoring en rapportage. Dit waarborgt dat financiële verslaggeving op een transparante en betrouwbare manier plaatsvindt, waardoor risico's op onregelmatigheden worden geminimaliseerd. De P&C-cyclus bij GGDrU omvat een systematische benadering voor planning, uitvoering, monitoring en evaluatie van gezondheidsdoelstellingen en -middelen. De cyclus bestaat uit belangrijke activiteiten, zoals: • **Kaderbrief**: Dit document dient als richtlijn voor de begrotingscyclus; • **Begrotingen**: Zowel de voorlopige als de definitieve begroting worden opgesteld en ingediend volgens vastgestelde procedures; • **Jaarrekening**: De financiële jaarrekening wordt opgesteld en opgeleverd, met een bijbehorende rapportage; • **Tussentijdse Rapportages**: Deze rapportages worden regelmatig uitgevoerd om de					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
	van haar controles en toezicht waarborgen.	voortgang en prestaties te monitoren. Een goed uitgevoerde P&C-cyclus helpt potentiële risico's te beheersen, zoals budgetoverschrijdingen, onvoldoende monitoring of onjuiste financiële verslaglegging. Zonder tijdige en zorgvuldige uitvoering van deze processen kunnen er risico's ontstaan, zoals een gebrek aan financiële transparantie, inefficiënt gebruik van middelen of het niet behalen van doelstellingen.					
1.2.3 Er is sprake van een complexe of instabiele organisatiestructuur, zoals blijkt uit de volgende punten:		Een complexe of instabiele organisatiestructuur verwijst naar een organisatie met meerdere lagen van management, verschillende afdelingen of teams die moeilijk te coördineren zijn, en waar processen niet altijd duidelijk zijn. Dit kan leiden tot verwarring, inefficiëntie en een gebrek aan duidelijke verantwoordelijkheden.					
• Er is een uitdaging bij het identificeren van welke personen een overheersende invloed uitoefenen binnen GGDrU;	De uitdaging bij het identificeren van welke organisaties of personen een overheersende invloed hebben binnen GGDrU vormt geen potentieel risico.	GGDrU heeft een heldere en transparante organisatiestructuur, waardoor het gemakkelijk is om de betrokken belanghebbenden en hun invloed te identificeren. Dit minimaliseert de kans op belangenconflicten en bevordert een effectieve besluitvorming, omdat verantwoordelijkheden en bevoegdheden duidelijk zijn gedefinieerd.					
• Een overmatig complexe organisatiestructuur die gebruikmaakt van	Er is geen potentieel risico voor GGDrU met	Complexe of instabiele organisatiestructuur verwijst naar een bedrijfsstructuur die moeilijk te					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
ongebruikelijke rechtspersonen of verwarrende hiërarchische gezagslijnen;	betrekking tot een overmatige complexe organisatie-structuur die ongebruikelijke rechtspersonen of verwarrende hiërarchische gezagslijnen gebruikt.	begrijpen of te navigeren is, vaak vanwege een teveel aan lagen, functies, en ongebruikelijke rechtspersonen. Dergelijke structuren kunnen leiden tot verwarring over verantwoordelijkheden, hiërarchie, en besluitvorming. Dit kan het management bemoeilijken om effectief toezicht te houden en kan leiden tot inefficiëntie, gebrek aan transparantie, en een verhoogd risico op fraude of miscommunicatie.					
• Er is sprake van een hoog personeelsverloop binnen het senior management, de juridische adviseurs of de personen die verantwoordelijk zijn voor governance.	Ja	Er is een potentieel risico voor GGDrU bij een hoog verloop onder het senior management, juridische adviseurs of personen die verantwoordelijk zijn voor governance. Dit kan leiden tot verlies van belangrijke kennis, inconsistenties in besluitvorming en een verzwakte interne controle. Dergelijk verloop kan ook het vertrouwen van belanghebbenden ondermijnen en zorgen voor een gebrek aan continuïteit in de organisatie, wat uiteindelijk de effectiviteit van de governance en risicobeheersing in gevaar kan brengen.	M 	H 	• **Personeelsontwikkelings-programma's:** Programma's voor loopbaanontwikkeling en training om medewerkers te ondersteunen in hun groei binnen de organisatie; • **Cultuur van open communicatie:** Cultuur waarin medewerkers hun zorgen kunnen delen en waar hun stem gehoord wordt, om zo de werkplek positief te beïnvloeden; • **Wervings- en behoudstrategieën:** Strategieën voor het werven en behouden van talent, met focus op diversiteit en inclusie.	L 	Ja
Acties voor verbetering Mogelijke acties voor GGDrU omvatten het implementeren van een strategisch wervings- en opleidingsprogramma, het bevorderen van een sterke organisatiecultuur ter ondersteuning van continuïteit, en het waarborgen van een gestructureerd kennisoverdrachtsysteem om de impact van verloop te minimaliseren.							
1.2.4 Elementen van de interne beheersing zijn onvoldoende effectief, als gevolg van:		Volgens het COSO-raamwerk, dat veel gebruikt wordt als referentie voor interne beheersingssystemen, omvatten de belangrijkste elementen: • **Bestuur**: Duidelijke richtlijnen en					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		verantwoordelijkheden voor het management en bestuur; • **Risicobeheer**: Identificatie, beoordeling en prioritering van risico's die de organisatie kunnen beïnvloeden; • **Controle-activiteiten**: Procedures en beleid die zijn ontworpen om risico's te beheersen en doelstellingen te behalen; • **Informatie en communicatie**: Effectieve communicatie van informatie binnen de organisatie, zodat alle betrokkenen op de hoogte zijn van hun verantwoordelijkheden; • **Toezicht en monitoring**: Continue evaluatie van de effectiviteit van de interne beheersingssystemen en de noodzakelijke aanpassingen.					
• Onvoldoende toezicht op interne beheersingsmaatregelen, waaronder geautomatiseerde systemen en maatregelen voor tussentijdse financiële verslaglegging, kan de effectiviteit en betrouwbaarheid hiervan ondermijnen;	Ja	Als het toezicht niet goed wordt uitgevoerd, ontstaat er een verhoogd risico op fouten, onregelmatigheden of zelfs fraude in de financiële rapportages en operationele processen. Dit kan leiden tot verkeerde beslissingen, inefficiënt gebruik van middelen en mogelijk verlies van vertrouwen in de organisatie. Tijdig toezicht en adequate controlemechanismen zijn daarom essentieel om deze risico's te beperken: • **Fouten in financiële rapportages**: Onvoldoende	H ☹	H ☹	• **Regelmatige audits:** Periodieke interne en externe audits uit om de effectiviteit van de beheersmaatregelen te beoordelen en om eventuele tekortkomingen te identificeren; • **Geautomatiseerde controles**: Geautomatiseerde systemen voor financiële rapportage en gegevensverwerking om de nauwkeurigheid en transparantie te verhogen; • **Training en bewustwording**: Trainingen aan medewerkers over de belangrijke rol van interne	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		monitoring kan leiden tot onjuiste financiële gegevens, waardoor de betrouwbaarheid van rapportages in het gedrang komt. Dit kan invloed hebben op beslissingen van het management en stakeholders; • **Fraude of onregelmatigheden**: Zonder adequate controles kunnen medewerkers geneigd zijn om frauduleuze activiteiten uit te voeren, omdat de kans op detectie laag is; • **Non-compliance met regelgeving**: Als de interne beheersmaatregelen niet goed worden gemonitord, kunnen er wettelijke en reglementaire voorschriften worden overtreden, wat kan leiden tot juridische consequenties en reputatieschade; • **Operationele inefficiëntie**: Het ontbreken van toezicht kan resulteren in inefficiënte processen, die zowel tijd als middelen verspillen, en kan leiden tot een slechte dienstverlening; • **Verlies van vertrouwen**: Afnemers en stakeholders kunnen het vertrouwen in de organisatie verliezen als blijkt dat financiële gegevens onbetrouwbaar zijn of als er schandalen aan het licht komen.			beheersmaatregelen en de noodzaak van naleving; • **Rapportagesystemen**: Duidelijke rapportagesystemen waarmee medewerkers afwijkingen en problemen in realtime kunnen melden; • **Risicobeheerteam:** Team dat verantwoordelijk is voor het toezicht op risico's en de effectiviteit van beheersmaatregelen, met regelmatige evaluaties van processen; • **Feedbackmechanismen**: feedbacksysteem waarmee medewerkers suggesties kunnen doen voor verbeteringen in de interne controles en processen; • **Documentatie en procedures**: Gedetailleerde documentatie van alle interne procedures en beheersmaatregelen, zodat deze gemakkelijk toegankelijk zijn voor alle medewerkers.		
Acties voor verbetering Voor GGDrU zijn de volgende aanvullende acties te overwegen om de interne beheersing en monitoring te verbeteren: 1. **Versterking van opleiding**: Regelmatige training en bewustwordingsprogramma's voor personeel over interne controles en rapportageprocessen om ervoor te zorgen dat iedereen goed geïnformeerd is;							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
2. **Technologische tools**: Implementatie van geavanceerde software voor het monitoren van financiële processen en rapportages om automatisering en realtime feedback te waarborgen; 3. **Regelmatige evaluatie**: Voer periodieke interne audits en evaluaties uit om de effectiviteit van de interne beheersingsmaatregelen te beoordelen en aan te passen waar nodig; 4. **Feedback mechanismen**: Creëer kanalen voor medewerkers om problemen of tekortkomingen in de interne beheersing anoniem te rapporteren, zodat deze tijdig kunnen worden aangepakt; 5. **Stakeholder betrokkenheid**: Betrek relevante belanghebbenden bij het proces van interne controle en rapportage om diverse perspectieven en ervaringen te integreren.							
• Een hoog personeelsverloop of de inzet van ineffectieve medewerkers voor administratieve taken, interne audits of informatietechnologie;	Ja	• **Verminderde efficiëntie**: Onervaren of slecht presterende medewerkers kunnen leiden tot vertragingen in administratieve processen en een lagere kwaliteit van de dienstverlening; • **Verhoogde foutenlast**: Ineffectieve medewerkers kunnen meer fouten maken, wat kan resulteren in onjuiste financiële verslaglegging of compliance-issues; • **Verlies van kennis**: Hoog personeelsverloop kan leiden tot het verlies van waardevolle kennis en ervaring binnen de organisatie, wat de continuïteit van processen in gevaar kan brengen; • **Moeilijkheden bij interne audits**: Slechte prestaties van medewerkers die verantwoordelijk zijn voor interne audits kunnen het risico op frauduleuze activiteiten verhogen en de effectiviteit van de interne controle verminderen; • **Verhoogde kosten**: Het continu aannemen en opleiden van nieuw personeel kan leiden tot hogere operationele kosten.	M 	H 	• **Wervings- en Selectiebeleid**: Wervingsproces dat zich richt op het aantrekken van gekwalificeerde en competente medewerkers. Dit omvat gedetailleerde functieomschrijvingen en gestructureerde interviews om de beste kandidaten te selecteren; • **Opleidingsprogramma's**: Uitgebreide trainingen en ontwikkelingsmogelijkheden aan voor nieuwe en bestaande medewerkers. Dit helpt om vaardigheden te verbeteren en zorgt ervoor dat personeel goed voorbereid is op hun taken; • **Mentorschap en coaching**: Ervaren Medewerkers begeleiden nieuwe collega's begeleiden. Dit kan de integratie vergemakkelijken en bijdragen aan kennisoverdracht; • **Feedback en evaluatie**: Regelmatig prestatie-evaluaties om het functioneren van medewerkers te beoordelen en te zorgen voor continue feedback. Dit helpt bij het identificeren van ontwikkelingsbehoeften en bevordert een cultuur van verbetering; • **Tevredenheidsonderzoeken**: Regelmatige onderzoeken om de medewerkerstevredenheid te meten en inzicht te krijgen in de redenen voor verloop. Dit kan helpen om problemen tijdig aan te pakken;	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					• **Flexibele werkstructuren**: Flexibele werkregelingen om de werk-privébalans van medewerkers te verbeteren en zo het verloop te verminderen.		
Acties voor verbetering Om het risico van hoog personeelsverloop en ineffectieve medewerkers bij GGDrU te verminderen, kunnen verschillende acties worden ondernomen. Dit omvat het verbeteren van wervingsprocessen, het aanbieden van training en ontwikkeling, het implementeren van mentorschap, en het creëren van feedbackmechanismen. Daarnaast kunnen personeelsbehoudstrategieën, prestatie-evaluaties en gezondheidsprogramma's bijdragen aan een stabiele en effectieve organisatie. Door deze maatregelen te nemen, kan GGDrU de effectiviteit van haar personeel verhogen en een positieve werkcultuur bevorderen.							
• Ineffectieve systemen voor administratieve verwerking en informatiemanagement, inclusief gevallen waarin significante tekortkomingen in de interne controlestructuren aanwezig zijn;	Ja	• **Fouten in gegevensverwerking**: Wanneer administratieve systemen niet effectief zijn, kunnen ze onnauwkeurige of onvolledige informatie genereren, wat de kwaliteit van financiële rapportages en beslissingen beïnvloedt; • **Tekortkomingen in interne beheersing**: Significante tekortkomingen in de interne controlemaatregelen kunnen leiden tot een verhoogd risico op fraude, mismanagement of inefficiënte processen, wat de integriteit van de organisatie in gevaar kan brengen; • **Verlies van efficiëntie**: Ineffectieve systemen kunnen de werklast van medewerkers verhogen, waardoor tijd en middelen verloren gaan aan handmatige processen of het corrigeren van fouten; • **Compliance risico's**: Als systemen niet adequaat zijn, kan de organisatie moeite hebben om	M 	H 	• **Regelmatige systeemaudits:** Periodieke audits op administratieve en informatiesystemen om eventuele tekortkomingen vroegtijdig te identificeren; • **Training en opleiding:** Continue training van medewerkers om hen bewust te maken van de juiste procedures en systemen die ze moeten gebruiken; • **Geïntegreerde informatiesystemen:** Geïntegreerde software-oplossingen die alle administratieve processen stroomlijnen en de datakwaliteit verbeteren; • **Documentatie en procedures:** Duidelijke documentatie en werkprocedures voor het gebruik van systemen, zodat medewerkers weten hoe ze deze effectief kunnen inzetten; • **Monitoring en rapportage:** Real-time monitoring van systemen en rapportagesystemen om afwijkingen snel op te sporen en aan te pakken. • **Feedbackmechanismen:** Kanalen voor medewerkers om feedback te geven over inefficiënties of problemen	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		te voldoen aan wettelijke en regelgevende vereisten, wat kan resulteren in juridische problemen of sancties.			met de systemen, zodat deze snel kunnen worden opgelost.		
Acties voor verbetering Het is noodzakelijk om regelmatig de effectiviteit van de systemen en beheersmaatregelen te evalueren en bij te stellen, om ervoor te zorgen dat ze blijven voldoen aan de behoeften van de organisatie en risico's continu worden gemonitord.							
• Het management kan interne beheersmaatregelen omzeilen of negeren;	Ja	Het management heeft de unieke mogelijkheid om fraude te plegen, omdat het de administratieve registraties kan manipuleren en valse financiële rapportages kan opstellen door effectieve interne beheersingsmaatregelen te omzeilen	H 	H 	• **Versterking van de interne controlemechanismen**: Set van interne controles die regelmatig worden geëvalueerd en bijgewerkt om fraude te voorkomen. Dit omvat zowel geautomatiseerde als handmatige controles; • **Onafhankelijke audit**: Regelmatig interne en externe audits om de effectiviteit van de interne controles te beoordelen en mogelijke tekortkomingen tijdig te identificeren; • **Scheiding van taken**: Verantwoordelijkheden binnen de organisatie zijn zo verdeeld dat geen enkele persoon de volledige controle heeft over financiële transacties. Dit helpt om de kans op frauduleuze handelingen te verkleinen; • **Toezicht en rapportage**: Structuur van toezicht die ervoor zorgt dat alle belangrijke financiële beslissingen worden gerapporteerd aan algemeen bestuur (AB) en een dagelijks bestuur (DB); • **Training en bewustwording**: Trainingen aan medewerkers en management over ethisch gedrag en de gevolgen van fraude, en creëer een cultuur waarin integriteit en transparantie worden bevorderd;	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					• **Anonieme meldsystemen**: Meldsysteem waar medewerkers anoniem vermoedens van fraude of ongepast gedrag kunnen melden zonder angst voor repercussies.		
Acties voor verbetering: De volgende acties zijn relevant voor GGDrU: 1. **Versterken van de onafhankelijke toezichtstructuur**: Zorg voor een auditcommissie die het management effectief controleert en verantwoording aflegt; 2. **Implementeren van strikte controlemechanismen**: Ontwikkel en implementeer gedetailleerde procedures voor financiële verslaglegging en interne audits die regelmatig worden geëvalueerd en bijgewerkt; 3. **Ontwikkeln van een cultuur van integriteit**: Bevorder een organisatiecultuur die integriteit en transparantie waardeert, waarbij medewerkers worden aangemoedigd om onregelmatigheden of zorgen te melden zonder angst voor repercussies; 4. **Regelmatige training en bewustwording**: Bied regelmatig trainingen aan voor zowel het management als medewerkers over ethische normen, compliance en de gevolgen van fraude; 5. **Evalueren van beheersmaatregelen**: Voer periodieke evaluaties uit van de effectiviteit van interne beheersingsmaatregelen en pas deze aan op basis van veranderende risico's en omstandigheden; 6. **Toepassen van anomaliedetectie**: Gebruik technologieën en software die afwijkingen in financiële gegevens kunnen detecteren, wat kan helpen bij het vroegtijdig signaleren van potentiële fraude.							
1.3 Rationalisatie	**Rationalisatie is het proces waarbij iemand een logische of redelijke verklaring zoekt voor gedrag dat in werkelijkheid emotioneel of moreel problematisch is. Dit stelt de persoon in staat om zichzelf te overtuigen dat hun acties**	Rationaliseren gebeurt wanneer individuen proberen hun gedrag, beslissingen of gevoelens te rechtvaardigen, vooral als die gedragspatronen moreel of ethisch twijfelachtig zijn. Dit proces kan optreden in verschillende situaties, waaronder: • Morele dilemma's: Mensen kunnen hun acties rationaliseren wanneer ze geconfronteerd worden met situaties waarin ze tegen hun morele waarden ingaan, zoals fraude of bedrog. Ze kunnen bijvoorbeeld zeggen dat "iedereen het doet" of "dat de regels niet eerlijk zijn;"					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
	acceptabel zijn, ondanks eventuele tegenstrijdige gevoelens.	• Stressvolle omstandigheden: In situaties van hoge druk of stress kunnen individuen rationaliseren om zichzelf te beschermen tegen de emotionele gevolgen van hun keuzes. Dit kan hen helpen om beter met de situatie om te gaan en om te gaan met de gevolgen van hun acties; • Sociale acceptatie: Mensen rationaliseren vaak hun gedrag om zich aan te passen aan de normen of verwachtingen van hun sociale omgeving. Dit kan voorkomen bij groepsdruk, waar individuen gedrag goedpraten om erbij te horen; • Fouten of mislukkingen: Wanneer iemand een fout maakt of faalt in een taak, kan hij of zij rationaliseren door te stellen dat de omstandigheden buiten hun controle lagen of dat de verwachtingen onrealistisch waren; • Zelfbescherming: Rationalisatie kan ook een mechanisme zijn om de zelfwaardering te behouden. Door hun gedrag te rechtvaardigen, kunnen mensen zich beter voelen over hun beslissingen, zelfs als deze verkeerd zijn.					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• Ineffectieve communicatie, Deze zin verwijst naar de situatie waarin het management niet effectief is in het communiceren, implementeren, ondersteunen of handhaven van de waarden en ethische normen binnen een organisatie, of wanneer het management zelfs ongepaste waarden of normen promoot. In het kader van rationalisatie van fraude betekent dit dat medewerkers de gebrekkige ethiek of waarden van het management kunnen gebruiken om hun eigen frauduleuze gedrag te rechtvaardigen. Met andere woorden, als het management geen sterke morele en ethische standaarden uitdraagt, kan dit een cultuur creëren waarin fraude wordt getolereerd of goedgepraat.	Ja	Voor GGDrU kunnen de volgende potentiële risico's spelen wanneer er sprake is van ineffectieve communicatie, implementatie, ondersteuning of handhaving van ethische waarden door het management: 1. **Fraude en Onregelmatigheden**: Als ethische normen niet duidelijk worden gecommuniceerd of gehandhaafd, kunnen medewerkers makkelijker frauduleuze handelingen rationaliseren, zoals het misbruik van middelen, vervalsen van gegevens of onrechtmatige toekennen van contracten; 2. **Integriteitsrisico**: Een gebrek aan duidelijke ethische standaarden kan de integriteit van GGDrU ondermijnen, wat kan leiden tot reputatieschade en	M 	H 	1. **Strikte aanbestedingsprocedures**: Duidelijke en formele aanbestedingsregels voor het selecteren van leveranciers volgens Europese aanbestedingsrichtlijnen. Doel: Zorgen voor eerlijke concurrentie en trasparantie bij het toekennen van contracten; 2. **Vier-ogen-principe**: Het splitsen van verantwoordelijkheden zodat één persoon niet alle stappen in het aanbestedingsproces beheert. Dit betekent dat meerdere medewerkers betrokken moeten zijn bij het beoordelen en toekennen van contracten. Doel: Verminderen van de kans op belangenverstrengeling, fouten of fraude door de betrokkenheid van meerdere partijen; 3. **Transparante selectiecriteria**: Heldere en vooraf vastgelegde criteria voor het beoordelen van offertes en leveranciers, inclusief objectieve scoremodellen en documentatie van de beslissingen. Doel: Waarborgen dat contracten worden toegekend op basis van eerlijke, meetbare criteria en niet op basis van persoonlijke voorkeuren; 4. **Interne en externe audit**: Regelmatig audits door interne of externe partijen om te controleren of de aanbestedings- en contracttoewijzingsprocessen correct	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		verminderde publieke en politieke steun; 3. **Gebrekkige verantwoording**: Zonder goed vastgelegde waarden kunnen er problemen ontstaan in de verantwoording van beslissingen en acties, wat leidt tot ondoorzichtige processen en een gebrek aan transparantie. 4. **Minder doeltreffende beheersingsmaatregelen**: Het niet strikt naleven van ethische richtlijnen kan leiden tot een afname van de effectiviteit van interne controlesystemen, zoals de financiële verslaglegging en compliance; 5. **Verminderde medewerkersmoraal**: Werknemers die zien dat ethiek niet wordt nageleefd of dat onethisch gedrag ongestraft blijft, kunnen			worden gevolgd en voldoen aan de geldende wet- en regelgeving. Doel: Vroegtijdig opsporen van onregelmatigheden en afwijkingen van het beleid; 5. **Training en bewustwording:** Regelmatig training voor medewerkers over ethische normen, aanbestedingsregels en het herkennen van belangenverstrengeling of corruptie. Doel: Zorgen dat alle medewerkers zich bewust zijn van de risico's en verantwoordelijkheden rondom het toekennen van contracten; • **Gedragscode en integriteitsbeleid**: Een gedragscode die duidelijk aangeeft wat wel en niet acceptabel is met betrekking tot het gebruik van zakelijke tussenpersonen en het toewijzen van contracten. Doel: Stimuleren van een cultuur van ethisch gedrag en verantwoordelijkheid binnen GGDrU; • **Meldpunt en Klokkenluidersregeling**: Een anoniem meldpunt en/of klokkenluidersregeling waar medewerkers en derden vermoedens van onrechtmatigheden of misstanden kunnen melden zonder angst voor represailles. Doel: Bevorderen van transparantie en het snel signaleren van mogelijke onrechtmatige toekenning van contracten;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		gedemotiveerd raken, wat de algehele werksfeer en productiviteit negatief beïnvloedt. 6. **Toename van klachten of misstanden**: Een cultuur waarin ethische waarden niet duidelijk worden uitgedragen kan leiden tot een toename van meldingen van misstanden of klachten, zoals ongewenst gedrag, wat het functioneren van GGDrU schaadt.			• **Belangenverstrengeling registreren en beheren**: Verplichte registratie van mogelijke conflicten van belangen voor iedereen die betrokken is bij aanbestedingen, inclusief leveranciers. Het voeren van een register en beleid om hiermee om te gaan. • **Contractbeheer en nazorg:** Strakke controle op de uitvoering van toegekende contracten, met regelmatige evaluatie en monitoring van prestaties van leveranciers. Doel: Zorgen dat contracten correct worden uitgevoerd en dat eventuele afwijkingen of onregelmatigheden vroegtijdig worden gesignaleerd en aangepakt.		

Acties voor verbetering
Door deze aanvullende maatregelen te implementeren, kan de GGD het risico op onrechtmatige toekenning van contracten verder verlagen en de algehele integriteit van het aanbestedingsproces verbeteren:

1. Data-analyse en monitoring:
- **Actie**: Implementeer systemen voor data-analyse om patronen en trends in aanbestedingen en contracttoewijzingen te monitoren;
- **Doel**: Vroegtijdig signaleren van ongewone transacties of afwijkingen die kunnen wijzen op fraude of onregelmatigheden;

2. Regelmatige risico-evaluaties:
- **Actie**: Voer periodieke risico-evaluaties uit om potentiële risico's binnen het aanbestedingsproces te identificeren en te beoordelen;
- **Doel**: Proactief omgaan met opkomende risico's en de effectiviteit van bestaande maatregelen te beoordelen;

3. Communicatie- en rapportagestructuur:
- **Actie**: Ontwikkel een duidelijke communicatie- en rapportagestructuur over aanbestedingen, inclusief wie verantwoordelijk is voor welke informatie;
- **Doel**: Zorgen voor transparantie in het proces en dat belangrijke informatie tijdig wordt gedeeld met alle betrokken partijen;

4. Klankbordgroep:
- **Actie**: Stel een klankbordgroep in dat toeziet op de naleving van ethische normen en aanbestedingsprocedures;
- **Doel**: Bieden van een onafhankelijk platform dat verantwoordelijk is voor het monitoren en waarborgen van integriteit binnen het proces;

5. Feedback mechanismen:

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• **Actie**: Implementeer mechanismen voor het verzamelen van feedback van medewerkers en stakeholders over de aanbestedingsprocessen; • **Doel**: Continu verbeteren van processen door input van betrokkenen en het oplossen van eventuele knelpunten; **6. Externe inbreng en advies:** • **Actie**: Raadpleeg externe experts of adviseurs voor het evalueren van aanbestedingsprocessen en het geven van aanbevelingen voor verbetering; • **Doel**: Profiteren van externe kennis en ervaringen om de processen te versterken; **7. Verplichtings- en prestatiecontracten:** • **Actie**: Gebruik van prestatiecontracten waarin specifieke verwachtingen en verplichtingen voor leveranciers zijn vastgelegd; • **Doel**: Zorg ervoor dat leveranciers verantwoordelijk zijn voor het leveren van kwaliteit en dat er gevolgen zijn bij tekortkomingen; **8. Evaluatie van leveranciers:** • **Actie**: Voer regelmatig beoordelingen uit van leveranciers op basis van hun prestaties, compliance en ethisch gedrag; • **Doel**: Zorgen voor de voortdurende geschiktheid van leveranciers en het voorkomen van herhaalde tekortkomingen; **9. Openbare verslaggeving:** • **Actie**: Zorg voor regelmatige publicatie van rapportages over aanbestedingsprocessen en contracttoewijzingen in TenderNed, zodat deze op een toegankelijke manier voor het publiek beschikbaar zijn; • **Doel**: Verhoogde transparantie en verantwoording naar de samenleving toe, wat kan helpen om publieke vertrouwen te vergroten; **10. Technologische innovaties:** • **Actie**: Onderzoek de mogelijkheden innovatieve digitale oplossingen voor transparantie en traceerbaarheid in het aanbestedingsproces; • **Doel**: Versterken van de integriteit van het proces en het verminderen van het risico op fraude door ongewijzigde, transparante transacties; **11**. **Nevenfunctieregister**: • **Actie**: Een nevenfunctieregister is een openbaar register waarin medewerkers van GGDrU hun nevenfuncties (bijbanen of andere werkzaamheden buiten hun hoofdtaken) dienen te registreren. Dit register heeft als doel om transparantie te waarborgen en belangenverstrengeling te voorkomen; • **Doel**: Het voorkomen van persoonlijke belangen die de objectiviteit en integriteit van het toekenningsproces kunnen beïnvloeden.							
• De intensieve betrokkenheid van leden van het management zonder directe financiële verantwoordelijkheden bij het kiezen van grondslagen voor financiële verslaggeving of het maken van belangrijke schattingen kan een risico vormen voor de integriteit van de financiële rapportage;	Potentiële risico's zijn beperkt	Hoewel de betrokkenheid van niet-financiële managers in financiële zaken potentieel risico's met zich meebrengt, zijn de specifieke omstandigheden binnen GGDrU, zoals strikte regelgeving (waaronder Gemeentewet, de Financieringswet, de Wet maatschappelijke ondersteuning, de Jeugdwet, en het Besluit begroting en verantwoording (BBV), specialisatie					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		van personeel, en interne controlemaatregelen, belangrijke factoren die bijdragen aan een minimalisatie van deze risico's.					
• Een geschiedenis van overtredingen van de effectenwet of andere wetgeving, of aanklachten tegen de organisatie, het senior management of verantwoordelijke personen over fraude of het niet naleven van regels	De potentiële risico's als minimaal worden beschouwd.	Het feit dat GGDrU geen geschiedenis van overtredingen heeft, is positief en duidt op een goed functionerend systeem van naleving en governance. Desondanks is het belangrijk om waakzaam te blijven en ervoor te zorgen dat er adequate processen en procedures zijn om ook in de toekomst risico's te minimaliseren.			Het treasurystatuut is het beleidsdocument dat de regels en richtlijnen vastlegt voor financieel beheer en treasury binnen GGDrU.		
• Bovenmatige belangstelling van het management voor het handhaven of verhogen van het resultaatontwikkeling. Resultaatontwikkeling verwijst naar de groei en verbetering van de financiële prestaties van GGDrU, inclusief: • **Financiële groei**: Het streven naar hogere inkomsten en winstgevendheid. • **Efficiëntieverbetering**: Optimaliseren van processen om kosten te	De focus op resultaatontwik-keling kan, als deze te ver doorschiet, leiden tot aanzienlijke risico's voor de integriteit en de operationele effectiviteit van GGDrU.	Een sterke focus van het management op resultaatontwikkeling kan de kans op rationalisatie van onethisch gedrag vergroten, omdat medewerkers onder druk gezet kunnen worden om onrealistische resultaten te behalen. Enkele van de belangrijkste risico's zijn: 1. **Fraude en onethisch gedrag**: De druk om financiële doelstellingen te	M 	H 	Om de risico's van een te sterke focus op resultaatontwikkeling binnen GGDrU te beheersen, kunnen verschillende maatregelen worden genomen. Een duidelijke ethische code en regelmatige training bevorderen een cultuur van ethisch gedrag. Transparante communicatie en feedbackmechanismen zorgen ervoor dat medewerkers zich vrij voelen om zorgen te uiten. Het gebruik van een balanced scorecard, interne en externe audits, en het vier-ogen-principe helpen om financiële en	L tot M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
verlagen en middelen beter te benutten. • **Kwaliteitsverbetering van diensten**: Verhogen van de kwaliteit van geleverde diensten om klanttevredenheid te verbeteren. • **Prestatie-indicatoren**: Gebruik van KPI's om voortgang en effectiviteit te meten. • **Strategische doelen**: Bereiken van doelstellingen die zijn vastgesteld in het beleidsplan van de organisatie. In deze context betekent dit dat het management misschien te veel druk uitoefent om financiële doelstellingen te bereiken.		behalen kan medewerkers aanmoedigen om onethische praktijken of zelfs fraude te rationaliseren om de gewenste resultaten te presenteren; 2. **Verlies van integriteit**: Wanneer medewerkers zich onder druk gezet voelen om resultaten te behalen, kunnen ze geneigd zijn om de waarheid te verdraaien of onjuiste informatie te verstrekken in financiële rapportages; 3. **Afname van kwaliteit**: De nadruk op cijfers kan ertoe leiden dat de kwaliteit van de geleverde diensten in het gedrang komt, omdat medewerkers zich meer richten op het behalen van financiële doelen dan op het leveren van waardevolle zorg; 4. **Negeren van risico's**: Er kan een neiging zijn om			kwaliteitsaspecten in evenwicht te houden. Daarnaast zijn een belangenverstrengelingregister en een klokkenluidersregeling cruciaal voor het waarborgen van integriteit en transparantie in de organisatie.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		financiële risico's en andere belangrijke indicatoren van de organisatie te negeren, zolang de financiële resultaten positief lijken; 5. **Belemmering van feedback**: Een cultuur waarin resultaatontwikkeling prioriteit krijgt, kan leiden tot een gebrek aan open communicatie en feedback, waardoor problemen niet tijdig worden gesignaleerd; 6. **Belangenverstrengeling**: Er kunnen situaties ontstaan waarin persoonlijke belangen van medewerkers de objectiviteit in besluitvorming beïnvloeden, vooral als ze worden aangemoedigd om resultaten te behalen ten koste van ethische normen.					
Acties voor verbetering Om het restrisico van onethisch gedrag of fraude binnen GGDrU verder te beheersen, kunnen aanvullende acties worden ondernomen. Dit omvat het versterken van de organisatiecultuur door leiderschapsprogramma's en integratie van kernwaarden in de prestatiecriteria. Regelmatige evaluaties van de effectiviteit van beheersmaatregelen, samen met transparante communicatie en feedbackrondes, zijn cruciaal. Daarnaast kunnen innovatieve technologieën zoals data-analyse en compliance software worden ingezet om verdachte transacties te detecteren. Tot slot is continue monitoring en transparante rapportage over audits en bevindingen essentieel voor het waarborgen van integriteit en verantwoordelijkheid.							
• Het management heeft de neiging om aan schuldeisers en andere	Ja	• **Verlies van vertrouwen**: Wanneer de werkelijke resultaten	M	M	1. **Realistische Prognoseprocessen**:	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
externe partijen ambitieuze of onrealistische prognoses te presenteren.		niet overeenkomen met de gepresenteerde prognoses, kan dit leiden tot een verlies van vertrouwen van schuldeisers, investeerders en andere belanghebbenden in de organisatie; • **Financiële risico's**: Onrealistische prognoses kunnen leiden tot verkeerde financiële beslissingen, zoals het aangaan van onnodige schulden of het maken van te hoge uitgaven, wat de financiële stabiliteit van de organisatie kan ondermijnen; • **Reputatieschade**: De presentatie van onrealistische verwachtingen kan de reputatie van de organisatie schaden, vooral als het bekend wordt dat de prognoses niet worden gehaald, wat kan leiden tot negatieve publiciteit en een verminderd imago; • **Juridische gevolgen**: Als stakeholders zich misleid voelen door de gepresenteerde	😐	😐	○ Duidelijke richtlijnen voor het opstellen van prognoses, waarbij historische gegevens, marktanalyses en realistische groeipercentages worden gebruikt. Dit zorgt ervoor dat prognoses zijn gebaseerd op haalbare verwachtingen; 2. **Inbreng van meerdere afdelingen**: ○ Financiën, bedrijfsvoering en strategische beleidsvorming zijn betrokken bij het opstellen van prognoses. Dit kan zorgen voor een breder perspectief en een betere afstemming van doelstellingen; 3. **Regelmatige evaluatie van prognoses**: ○ Periodieke evaluaties uit van de prognoses en vergelijk deze met de		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		prognoses, kan dit leiden tot juridische claims of geschillen, wat verdere financiële en reputatieschade kan veroorzaken; • **Interne demotivatie**: Medewerkers kunnen demotivatie ervaren als ze het gevoel hebben dat de doelen die door het management zijn gesteld onrealistisch zijn, wat kan leiden tot verminderde productiviteit en werktevredenheid; • **Risico op fraude**: Een sterke druk om ambitieuze doelstellingen te behalen kan sommige medewerkers ertoe aanzetten om onethische of frauduleuze praktijken toe te passen om de prognoses te halen.			werkelijke resultaten. Dit kan helpen om tijdig afwijkingen te identificeren en bij te sturen; 4. **Transparante communicatie**: o Open communciatie over de aannames en onzekerheden die aan de prognoses ten grondslag liggen. Dit helpt om het vertrouwen van belanghebbenden te behouden, zelfs als de werkelijke resultaten afwijken van de verwachtingen; 5. **Training en opleiding**: o Trainingen voor medewerkers die betrokken zijn bij het opstellen van prognoses, zodat zij beter begrijpen hoe ze realistische en onderbouwde schattingen kunnen maken; 6. **Onafhankelijke toetsing**:		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					○ Prognoses toetsen door een onafhankelijke derde, zoals een interne audit of een externe adviseur, om objectiviteit en nauwkeurigheid te waarborgen. 7. **Risicobeheerprocessen**: ○ Risicobeheerproces dat specifiek gericht is op het identificeren en mitigeren van de risico's die voortkomen uit onrealistische prognoses; 8. **Gedragscode en ethische normen**: ○ Een gedragscode waarin de verwachtingen omtrent integriteit en transparantie met betrekking tot prognoses worden beschreven;		
Acties voor verbetering Ondanks het lage restrisico is het belangrijk om regelmatig trainingen te organiseren voor medewerkers over het belang van realistische prognoses en de impact daarvan op de organisatie.							
• Het management is er niet in geslaagd om bekend zijnde aanzienlijke tekortkomingen in de	Ja	• **Financiële onregelmatigheden**: Onjuiste financiële rapportages of misbruik van middelen;	M 	H 	• **Regelmatige interne audits**: Audits om de effectiviteit van interne controles en processen te evalueren en	L tot M 	

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
interne controle tijdig aan te pakken. In de context van interne beheersing kunnen aanzienlijke tekortkomingen bijvoorbeeld omvatten: 1. **Onvoldoende controle-maatregelen**: Gebrek aan effectieve procedures of systemen om risico's te beheersen, zoals een gebrek aan toezicht of monitoring. 2. **Inconsistenties in rapportage**: Fouten of onnauwkeurigheden in financiële rapportages die de betrouwbaarheid van de informatie in gevaar brengen. 3. **Beperkingen in toegang tot informatie**: Gebrek aan adequate toegang tot noodzakelijke informatie voor het nemen van geïnformeerde beslissingen. 4. **Onvoldoende training en bewustwording**: Medewerkers zijn niet goed opgeleid of op de hoogte van hun		• **Compliance-issues**: Niet-naleving van wetten en regelgeving, wat kan leiden tot boetes of juridische problemen; • **Operationele verstoringen**: Inefficiënte processen of systemen die leiden tot vertragingen of fouten; • **Reputatieschade**: Negatieve publiciteit of verlies van vertrouwen door onethisch gedrag of mismanagement; • **Cybersecurity-bedreigingen**: Risico's van datalekken of hacking die vertrouwelijke informatie in gevaar kunnen brengen.			eventuele tekortkomingen te identificeren; • **Compliance-programma's**: Programma's die medewerkers bewust maken van wettelijke vereisten en ethische normen; • **Training en ontwikkeling**: Training aan medewerkers over risicobeheer, financiële verslaglegging en compliance om kennis en bewustzijn te vergroten; • **Strikte procedures**: Duidelijke en gedocumenteerde processen voor financiële transacties en aanbestedingen om transparantie en verantwoordelijkheid te waarborgen; • **Cybersecurity-maatregelen**: Informatiesystemen met firewalls, antivirussoftware en regelmatige updates om datalekken en cyberaanvallen te voorkomen; • **Klokkenluidersregelingen**: Een veilige en anonieme manier voor medewerkers om onregelmatigheden of zorgen te melden zonder angst voor repercussies.	😐	

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
verantwoordelijkheden en de procedures, wat leidt tot fouten. 5. **Gebrek aan naleving van wet- en regelgeving**: Niet voldoen aan relevante wetten of richtlijnen, wat kan leiden tot juridische en financiële gevolgen. 6. **Inadequate IT-systemen**: Technologische systemen die verouderd of niet goed beveiligd zijn, waardoor gegevensverlies of inbreuken kunnen optreden;							

Acties voor verbetering

Door deze acties te implementeren, kan GGDrU haar risicobeheerprocessen verder versterken en een hogere mate van integriteit en transparantie waarborgen:

1. **Regelmatige evaluatie van beheersmaatregelen**:
   - Voer periodieke beoordelingen uit van de bestaande beheersmaatregelen om hun effectiviteit te waarborgen en aan te passen aan nieuwe risico's of omstandigheden;
2. **Cultuur van openheid en verantwoording**:
   - Stimuleer een organisatiecultuur waar medewerkers zich vrij voelen om zorgen en ideeën te uiten, wat kan helpen bij het vroegtijdig signaleren van potentiële problemen;
3. **Verbeterde communicatie**:
   - Zorg voor duidelijke en effectieve communicatiekanalen tussen management en medewerkers over risicobeheer en ethische normen;
4. **Externe adviesdiensten**:
   - Overweeg het inschakelen van externe experts om een onafhankelijke beoordeling van de interne processen en risicobeheerstrategieën uit te voeren;
5. **Versterken van cybersecurity**:
   - Investeer in geavanceerdere technologieën en trainingen voor personeel om de beveiliging van informatiesystemen te verbeteren en de kans op cyberaanvallen te verkleinen.
6. **Feedbackmechanismen**:
   - Implementeer mechanismen voor feedback van zowel medewerkers als externe belanghebbenden om continue verbeteringen in de processen te stimuleren;
7. **Noodplannen**:
   - Ontwikkel en test noodplannen voor verschillende scenario's, zodat de organisatie snel kan reageren op onverwachte gebeurtenissen of crises.

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• Een laag moraal onder het senior management. Dit kan zich uiten in verschillende signalen, zoals een gebrek aan betrokkenheid bij belangrijke beslissingen, negatieve communicatie en een hoge mate van personeelsverloop. Daarnaast kunnen conflicten binnen het team, een lage medewerkerstevredenheid en terughoudendheid om nieuwe ideeën te omarmen ook wijzen op onvrede. Wanneer het management de waarden van de organisatie niet naleeft, leidt dit tot wantrouwen en kritiek op hun besluitvorming, wat de effectiviteit en integriteit van de organisatie schaadt.	Geen potentieel risico voor GGDrU.	Er zijn geen duidelijke aanwijzingen voor een laag moraal onder het senior management. De betrokkenheid bij belangrijke beslissingen, de communicatie en de samenwerking binnen het team lijken adequaat te zijn, wat duidt op een gezonde organisatiecultuur. Bovendien is er geen sprake van significante personeelsverloop of onvrede onder medewerkers, wat de integriteit en effectiviteit van de organisatie waarborgt.					
• Het bestuur maakt geen onderscheid tussen transacties van publieke en private aard. Dit houdt in dat het bestuur zowel private als publieke transacties op dezelfde manier behandelt, zonder rekening te houden met de specifieke regels, verantwoordelijkheden en transparantievereisten die aan elk type transactie zijn verbonden.	Ja	GGDrU lijkt adequaat om te gaan met haar verantwoordelijkheden en voldoet aan de geldende wet- en regelgeving, wat het vertrouwen van het publiek en andere stakeholders waarborgt. Deze risico's benadrukken het belang van duidelijke richtlijnen en procedures om publieke en private transacties effectief van elkaar te scheiden:	L 	L 	• **Regelmatige compliance controle**: Regelmatig interne audits om de naleving van de Besluit begroting en verantwoording (BBV) te waarborgen. Dit helpt om afwijkingen tijdig op te sporen en te corrigeren; • **Training en Opleiding**: Trainingen voor medewerkers en management over de vereisten van de BBV en de betekenis ervan voor financiële verslaggeving en besluitvorming;	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Publieke transacties zijn financiële handelingen die worden uitgevoerd met publiek geld en die onderhevig zijn aan specifieke wet- en regelgeving. Private transacties zijn financiële handelingen die niet direct verband houden met de publieke functie van GGDrU.		• **Onvoldoende transparantie**: Het ontbreken van een duidelijke scheiding tussen publieke en private transacties kan leiden tot onduidelijkheid over financiële stromen en de besteding van publieke middelen. Dit kan het vertrouwen van burgers en andere stakeholders ondermijnen; • **Belangenverstrengeling**: Wanneer privé- en publieke belangen niet van elkaar worden gescheiden, kunnen er situaties ontstaan waarin persoonlijke of zakelijke belangen van bestuurders of medewerkers de besluitvorming beïnvloeden. Dit kan leiden tot onethische beslissingen en mogelijk juridische gevolgen; • **Compliance risico's**: Publieke transacties zijn vaak onderworpen aan specifieke wet- en regelgeving. Het niet naleven van deze regels kan resulteren in juridische sancties, boetes of andere consequenties voor de gemeente. • **Verlies van publiek vertrouwen**: Als inwoners het gevoel hebben dat er geen duidelijke scheiding is tussen publieke en private belangen, kan dit leiden tot wantrouwen en ontevredenheid over het bestuur. Dit kan zich uiten in protesten,			• **Implementatie van controlemechanismen**: Controlemechanismen die zorgen voor transparantie en verantwoordingsplicht in financiëletransacties; • **Risicobeoordeling**: Regelmatig risicobeoordelingen om potentiële risico's in de uitvoering van de BBV te identificeren en te evalueren; • **Documentatie en rapportage**: Gedegen documentatie van financiële transacties en rapportages, zodat alle activiteiten traceerbaar zijn en voldoen aan de eisen van de BBV; • **Verantwoordelijkheid en toezicht**: Duidelijke verantwoordelijkheden en toezichtmechanismen voor het bestuur en management om ervoor te zorgen dat financiële beslissingen in lijn zijn met de BBV. • **Verantwoordelijkheid en toezicht**: Duidelijke verantwoordelijkheden en toezichtmechanismen voor het bestuur en management om ervoor te zorgen dat financiële beslissingen in lijn zijn met de BBV. externe auditors die de naleving van de BBV toetsen en onafhankelijke feedback geven over de financiële verslaggeving en processen.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		negatieve publiciteit of lagere participatie bij gemeentelijke activiteiten; • **Financiële risico's**: Onjuiste of ondoorzichtige transacties kunnen leiden tot inefficiënt gebruik van middelen, wat de financiële gezondheid van de gemeente kan ondermijnen en kan resulteren in onvoorziene uitgaven; • **Schade aan de reputatie**: Wanneer publieke en private transacties door elkaar lopen, kan dit leiden tot schandalen of negatieve media-aandacht, wat de reputatie van de gemeente kan schaden.					
Acties voor verbetering Deze acties dragen bij aan verbeterde transparantie, efficiëntie en naleving van het BBV binnen GGDrU: • **Trainingen**: Regelmatig medewerkers trainen over BBV-richtlijnen en financiële verslaggeving; • **Interne communicatie**: Een duidelijke communicatiestructuur opzetten om medewerkers op de hoogte te houden van procedures; • **Interne audits**: Regelmatig interne audits uitvoeren om de naleving van de BBV te controleren; • **Beleidsherziening**: Regelmatig het interne beleid herzien om te voldoen aan de laatste BBV-regelgeving.							
• Onenigheid tussen toezichthouders in een entiteit met weinig toezichthouders;	Geen potentieel risico.	Het toezichtteam bestaat uit meerdere toezichthouders, wat zorgt voor diversiteit in perspectieven en expertise. Deze brede samenstelling helpt om onenigheden beter te beheren en bevordert een constructieve dialoog. Daarnaast kan de aanwezigheid van verschillende toezichthouders bijdragen aan een meer robuuste en effectieve controle over de organisatie,					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		waardoor de kans op conflicten aanzienlijk wordt verminderd					
• Het management probeert herhaaldelijk administratieve handelingen te rechtvaardigen die niet helemaal voldoen aan de geldende normen. Het is cruciaal dat het management aandacht besteedt aan de rechtmatigheid van administratieve handelingen, omdat niet-naleving kan leiden tot financiële sancties, verlies van vertrouwen bij stakeholders en negatieve auditbevindingen.	Ja	Er bestaat een risico dat de GGD in strijd met wet- en regelgeving handelt, vooral als administratieve handelingen worden uitgevoerd die niet voldoen aan het normenkader. Dit kan leiden tot juridische consequenties en financiële sancties. Het feit dat het management herhaaldelijk administratieve handelingen probeert te rechtvaardigen die niet helemaal voldoen aan de geldende normen, kan zeker worden beschouwd als een potentieel risico. Hier zijn enkele redenen waarom: • **Integriteit van de rapportage**: Het rechtvaardigen van niet-conforme handelingen kan leiden tot onjuiste of misleidende financiële rapportages, wat de integriteit van de organisatie ondermijnt; • **Compliance risico**: Als het management afwijkingen van normen niet op een correcte manier aanpakt, kan dit resulteren in een schending van wet- en regelgeving, met mogelijke juridische gevolgen; • **Verlies van vertrouwen**: Herhaaldelijk afwijken van normen kan het vertrouwen van belanghebbenden (zoals medewerkers, klanten en	H 	M 	• **Training en Voorlichting**: Regelmatig training voor het management en medewerkers over geldende normen, wetgeving en ethische richtlijnen om bewustzijn en naleving te vergroten; • **Strikte toezichtmechanismen**: Interne controles en auditprocedures om afwijkingen van normen tijdig op te sporen en aan te pakken; • **Duidelijke gedragscode**: Gedragscode waarin de normen en verwachtingen voor administratieve handelingen helder worden uiteengezet; • **Meldpunten voor onregelmatigheden**: Anoniem meldpunt waar medewerkers vermoedens van onregelmatigheden of niet-conforme handelingen kunnen rapporteren zonder angst voor repercussies; • **Periodieke evaluaties**: Regelmatig evalueren van administratieve processen en handelingen om te	L tot M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		toezichthouders) in de organisatie en het management verminderen; • **Frauderisico**: Dit gedrag kan wijzen op een cultuur waarin het accepteren van risico's en het negeren van regels wordt gestimuleerd, wat de kans op fraude kan vergroten; • **Operationele risico's**: Dit kan ook leiden tot inefficiënties en fouten in de operationele processen, waardoor de prestaties van de organisatie in gevaar komen.			waarborgen dat ze voldoen aan de geldende normen en wetgeving; • **Verantwoordelijkheidsstructuur**: Duidelijke toewijzing van verantwoordelijkheden voor naleving van normen aan specifieke teamleden of afdelingen binnen de organisatie.		
Acties voor verbetering Door deze aanvullende acties te implementeren, kan GGDrU niet alleen het restrisico verlagen, maar ook een sterke basis creëren voor een cultuur van naleving en integriteit binnen de organisatie: 1. **Regelmatige risicoanalyse**: Voer periodiek risicoanalyses uit om nieuwe of veranderende risico's te identificeren, zodat tijdig passende maatregelen kunnen worden genomen; 2. **Feedbackmechanismen**: Creëer mogelijkheden voor medewerkers om feedback te geven over administratieve processen en de effectiviteit van de beheersmaatregelen, zodat verbeteringen kunnen worden doorgevoerd; 3. **Cultuur van transparantie**: Stimuleer een organisatiecultuur waarin transparantie en open communicatie over administratieve handelingen worden aangemoedigd, om het vertrouwen te vergroten en zorgen aan te pakken; 4. **Externe evaluaties**: Betrek externe auditors of deskundigen om de interne processen en naleving van normen te beoordelen en aanbevelingen te doen voor verbetering; 5. **Bewustwordingscampagnes**: Organiseer campagnes om het bewustzijn over de geldende normen en de gevolgen van niet-naleving te vergroten, zowel binnen het management als onder medewerkers; 6. **Versterking van leiderschap**: Zorg ervoor dat het senior management actief betrokken is bij het bevorderen van naleving en dat zij het goede voorbeeld geven in het naleven van normen; 7. **Implementatie van technologische oplossingen**: Overweeg het gebruik van software of systemen die helpen bij het monitoren van administratieve handelingen en het automatisch signaleren van afwijkingen van normen; 8. **Verantwoordingsstructuren**: Stel duidelijke verantwoordelijkheden en verantwoording vast voor alle medewerkers met betrekking tot administratieve handelingen, zodat er een cultuur van verantwoordelijkheid ontstaat.						
2. Het oneigenlijk toe-eigenen van bedrijfsmiddelen		Wanneer bedrijfsmiddelen worden toegeëigend voor persoonlijk gebruik, verliest de organisatie waardevolle middelen. Dit kan variëren van kleine bedrijfsmiddelen, zoals kantoorbenodigdheden, tot grote					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		bedrijfsmiddelen, zoals geld of eigendommen.					
2.1 Druk		Druk, zoals persoonlijke financiële problemen en de noodzaak om prestaties te leveren, kan medewerkers aanzetten tot frauduleus gedrag met betrekking tot bedrijfsmiddelen. Deze druk vergroot het risico op ongeoorloofde toe-eigening of misbruik van liquide middelen en kwetsbare bezittingen.					
2.1.1 Persoonlijke financiële verplichtingen kunnen druk uitoefenen op het management of medewerkers met toegang tot liquide middelen of kwetsbare bedrijfsmiddelen, wat hen kan aanzetten tot ongeoorloofde toe-eigening. Daarnaast kan een slechte verstandhouding tussen medewerkers van GGDrU bijdragen aan deze situatie, bijvoorbeeld door conflicten of gebrek aan samenwerking door:		Persoonlijke financiële verplichtingen kunnen aanzienlijke druk uitoefenen op het management of medewerkers met toegang tot liquide middelen of kwetsbare bedrijfsmiddelen. Deze druk kan hen verleiden tot ongeoorloofde toe-eigening van bedrijfsmiddelen, wat de integriteit van de organisatie in gevaar kan brengen. Daarnaast kan een slechte verstandhouding tussen medewerkers deze situatie verergeren. Conflicten of gebrek					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		aan samenwerking kunnen leiden tot wantrouwen en onduidelijkheid in de verantwoordelijkheden, waardoor het risico op ongeoorloofd gedrag met betrekking tot bedrijfsmiddelen toeneemt.					
• Aangekondigde of verwachte toekomstige ontslagen onder werknemers	Geen potentieel risico	Momenteel zijn er geen aangekondigde of verwachte toekomstige ontslagen onder medewerkers, wat de kans op spanning en onrust binnen de organisatie vermindert. In een stabiele werkomgeving is de motivatie om ongeoorloofd gedrag te vertonen daardoor lager, wat bijdraagt aan een positieve en samenwerkende cultuur.					
• Recente of verwachte wijzigingen in de beloningen van de werknemers of in toegezegde pensioenrechten	Geen poteniteel risico	Stabiliteit in beloningen draagt bij aan een positieve werksfeer en verhoogt de betrokkenheid van medewerkers, wat juist een mitigatie van risico's inhoudt in plaats van een toename.					
• Interne promoties, vergoeding of andere beloningen die afwijken van wat werd verwacht	Geen potentieel risico	GGDrU hanteert duidelijke en transparante criteria voor beloningsstructuren en het toekennen van promoties. Bovendien zijn de besluitvormingsprocessen goed gedocumenteerd en goedgekeurd					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		door het management en bestuur, wat zorgt voor consistentie en rechtmatigheid in de uitvoering. Dit voorkomt de mogelijkheid van willekeurige of ongepaste toekenningen die zouden kunnen leiden tot onvrede of wantrouwen onder medewerkers.					
2.2 Gelegenheid		Gelegenheid verwijst naar situaties waarin medewerkers toegang hebben tot bedrijfsmiddelen zonder adequate controle of toezicht, wat de kans op ongeoorloofde toe-eigening vergroot. Dit kan gebeuren in omgevingen met onvoldoende interne controles of waar de verantwoordelijkheden en procedures niet duidelijk zijn, waardoor medewerkers de kans krijgen om frauduleus gedrag te vertonen.					
2.2.1 Bepaalde kenmerken of omstandigheden kunnen de vatbaarheid van het oneigenlijk toe-eigenen van bedrijfsmiddelen vergroten.		Wanneer er onvoldoende interne controles of toezicht zijn, hebben medewerkers meer gelegenheid om misbruik te maken van hun					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Zo kan meer gelegenheid daartoe wordt gecreëerd in de volgende situaties:		toegang tot bedrijfsmiddelen. Ook in situaties met een gebrek aan duidelijke verantwoordelijkheden en procedures kunnen medewerkers sneller onethisch gedrag vertonen, omdat de kans op ontdekking kleiner is.					
• Grote hoeveelheden contant geld in kas of frequent kasverkeer: Contant geld is vervangen door pinbetalingen, maar ook pintransacties kunnen fraudegevoelig zijn, zoals bij ongeautoriseerde betalingen of manipulatie van pinautomaten.	Ja	Contante transacties binnen GGDrU zijn situaties waarin betalingen of financiële handelingen plaatsvinden met fysiek geld, zoals bankbiljetten en munten. Dit kan bijvoorbeeld het geval zijn bij: 1. **Kleine aankopen**: Bij het betalen voor diensten of goederen die op locatie worden geleverd, zoals catering of materialen voor evenementen; 2. **Betalingen aan klanten**: Wanneer klanten contant betalen voor bepaalde diensten of producten die door GGDrU worden aangeboden; 3. **Onkostenvergoedingen**: Wanneer medewerkers contant geld ontvangen voor onkosten, zoals reiskosten of andere uitgaven; 4. **Evenementen en activiteiten**: Bij evenementen waar direct contante betalingen worden gedaan, zoals voor toegang	M 	H 	Door deze beheersmaatregelen te implementeren, kan GGDrU de kans op fraude verminderen en de impact van eventuele incidenten beperken. Het bevorderen van een cultuur van veiligheid en bewustzijn is cruciaal voor het beschermen van zowel de organisatie als de klanten: • **Versterkte cyberbeveiliging**: Firewalls, antivirussoftware en intrusion detection systems (IDS) om ongeautoriseerde toegang te voorkomen. Regelmatige beveiligingsupdates en patchbeheer zijn ook essentieel om systemen te beschermen tegen kwetsbaarheden; • **Transactie monitoring**: Real-time monitoring van pintransacties om verdachte activiteiten onmiddellijk te identificeren. Dit kan helpen bij het detecteren van ongebruikelijke patronen of hoge transactiebedragen die op fraude kunnen duiden; • **Beveiliging van betaalterminals**: Betaalterminals worden regelmatig gecontroleerd op skimming-apparaten. Dit omvat	L tot M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		of aankopen van consumpties. In deze situaties is het belangrijk dat er goede controles en procedures zijn om de risico's van fraude of ongeoorloofd gebruik van contanten te minimaliseren. GGDrU voert geen contante transacties uit of deze zijn minimaal, en opereert in volledig met digitale betalingen, waaronder creditcard- en andere elektronische betalingen. Dit minimaliseert het risico op diefstal, fraude en onregelmatigheden die vaak samenhangen met de omgang met contant geld. Contant geld is vervangen door pinbetalingen. Hier zijn enkele overwegingen: 1. **Beveiliging**: Pinbetalingen zijn doorgaans veiliger dan contante transacties, omdat ze digitaal worden geregistreerd en makkelijker te traceren zijn. Dit vermindert het risico op fysieke diefstal of verlies van geld; 2. **Efficiëntie**: Het gebruik van pinbetalingen maakt het eenvoudiger en sneller om transacties af te handelen. Klanten kunnen hun betalingen snel en			ook het trainen van medewerkers in het herkennen van verdachte apparaten; • **klantbewustzijn en educatie**: Klanten worden bewust gemaakt van risico's van fraude en hoe ze zichzelf kunnen beschermen, zoals het controleren van bankafschriften en het rapporteren van verdachte transacties; • **authenticatieprocessen**: Extra authenticatiemethoden, zoals tweefactorauthenticatie (2FA) voor online betalingen en transacties, om de veiligheid te verhogen; • **Incidentenmanagement**: Incidentenbeheerplan op om snel te reageren op fraude-incidenten, inclusief contactinformatie voor de betrokken instanties, zoals de bank en autoriteiten; • **Training en bewustwording van medewerkers**: Zorg ervoor dat medewerkers getraind zijn in het herkennen van fraude-signalen en hoe te handelen in geval van een vermoeden van fraude. • **Interne controlemechanismen**: Procedures en controles waarborgen dat transacties correct worden uitgevoerd en bedrijfsmiddelen goed worden beheerd. Dit omvat scheiding van taken, autorisatieprocedures en verificaties; • **Beveiligingsmaatregelen**: Fysieke en digitale beveiligingssystemen, zoals toegangscontroles, encryptie en		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		gemakkelijk doen, wat de klantervaring verbetert; 3. **Risico's**: Ondanks de voordelen van pinbetalingen, blijven er risico's bestaan, zoals fraude, technische storingen en cyberbeveiligingsproblemen. Deze risico's zijn voornamelijk gerelateerd aan de digitale aspecten van het betalingsproces; 4. **Financieel beheer**: Pinbetalingen vereisen een goede administratieve controle om ervoor te zorgen dat alle transacties correct worden verwerkt en dat er geen fouten optreden in de boekhouding; 5. **Klantenservice**: Klanten kunnen ook vragen of problemen ervaren met pinbetalingen, zoals terugboekingen of onterechte afschrijvingen. Dit vereist dat medewerkers goed getraind zijn in het omgaan met dergelijke situaties. Hoewel GGDrU geen contante transacties heeft en volledig digitaal werkt, zijn er nog steeds risico's verbonden aan digitale betalingen. Enkele mogelijke risico's zijn: 1. **Technische storingen**: Problemen met betaalsoftware of hardware			beveiligingscamera's, beschermen tegen ongeoorloofde toegang en datalekken; • **Audit en monitoring**: Regelmatige audits en continue monitoring van processen en systemen helpen afwijkingen op te sporen en corrigerende maatregelen te nemen; • **Risicoanalyse**: Het systematisch identificeren, beoordelen en prioriteren van risico's zorgt ervoor dat passende maatregelen worden genomen ter vermindering van die risico's; • **Documentatie en rapportage**: Het bijhouden van gedetailleerde documentatie van processen, transacties en controles waarborgt transparantie en legt verantwoordelijkheden vast.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		kunnen leiden tot fouten in transacties of vertragingen, wat financiële verliezen kan veroorzaken; 2. **Onrechtmatige terugboekingen**: Klanten kunnen onterecht een terugboeking aanvragen, wat financiële complicaties voor de organisatie met zich meebrengt; 3. **Interne fraude**: Medewerkers kunnen misbruik maken van hun toegang tot financiële systemen, bijvoorbeeld door valse transacties te registreren of klantgegevens te manipuleren; 4. **Onbeveiligde netwerken**: Pinbetalingen via onbeveiligde netwerken kunnen leiden tot datalekken en andere beveiligingsincidenten. Daarnaast zijn er andere risico's bij digitale betalingen, zoals: 5. **Cybercriminaliteit**: Hacking en ongeautoriseerde toegang tot gevoelige informatie kunnen leiden tot gegevensdiefstal; 6. **Phishing**: Medewerkers kunnen doelwit worden van aanvallen die gericht zijn op het verkrijgen van vertrouwelijke informatie;					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		7. **Technische fouten**: Systeemuitval of betalingsfouten kunnen leiden tot gegevensverlies of onjuiste transacties; 8. **Fraude met betalingen**: Ondanks beveiligingsmaatregelen bestaat er een risico op creditcardfraude; 9. **Interne risico's**: Medewerkers kunnen frauduleus handelen zonder adequate controles; 10. **Compliance**: Het niet naleven van regelgeving kan resulteren in juridische problemen en boetes. Deze risico's benadrukken het belang van sterke beveiligingsmaatregelen en interne controles binnen een digitale omgeving.					

Acties voor verbetering

Voor GGDrU zijn er verschillende acties voor verbetering die de beheersing van frauderisico's verder kunnen versterken, met name gezien de focus op digitale processen en pinbetalingen in plaats van contante transacties. Hier zijn enkele suggesties:

1. **Verbeterde monitoring en auditing**:
   - **Regelmatige controle van transacties**: Zorg voor frequente audits en monitoring van digitale betalingen om verdachte transacties snel te detecteren;
   - **Fraude-detectiesystemen**: Investeer in systemen die afwijkingen in het betalingsverkeer automatisch detecteren, zoals ongebruikelijke transactiepatronen of verdachte bedragen;
2. **Training en bewustwording**:
   - **Medewerkerstraining**: Regelmatig trainen van medewerkers over het herkennen van frauderisico's, zoals phishing en andere cyberaanvallen;
   - **Bewustzijnscampagnes**: Zorg ervoor dat iedereen binnen de organisatie op de hoogte is van potentiële gevaren en weet hoe ze moeten reageren;
3. **Versterking van cybersecurity**:
   - **Informatiebeveiliging**: Verbeter de beveiliging van digitale systemen met up-to-date software, firewalls, en encryptietechnologie om cyberfraude te voorkomen;
   - **Twee-factor-authenticatie (2FA)**: Vereis 2FA voor alle gevoelige digitale transacties en toegang tot financiële systemen;
4. **Strengere interne controles**:
   - **Scheiding van taken**: Zorg ervoor dat verschillende medewerkers verantwoordelijk zijn voor verschillende stappen in het betalingsproces om interne fraude te beperken;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ **Controle op toegang**: Beperk de toegang tot financiële systemen tot geautoriseerd personeel, met regelmatige herziening van toegangsrechten; 5. **Incident response plannen**: ○ **Snelle reactie op fraudegevallen**: Zorg voor een robuust plan voor hoe de organisatie moet reageren als fraude wordt ontdekt, inclusief schadebeperking en herstelmaatregelen; ○ **Rapportageprotocollen**: Zorg voor een duidelijk en eenvoudig rapportageproces voor verdachte activiteiten.							
• Voorraaditems die klein van formaat zijn, maar een hoge waarde vertegenwoordigen of waarvoor grote vraag is; Voor GGDrU kunnen de volgende voorbeelden van voorraaditems die klein van formaat zijn, maar een hoge waarde vertegenwoordigen of waarvoor grote vraag is, worden genoemd: 1. **Medische Apparatuur**: Kleine maar kostbare apparaten zoals thermometers, bloedglucosemeters en ECG-monitoren. Deze items zijn cruciaal voor diagnose en behandeling, en de vraag naar hen kan fluctueren, afhankelijk van seizoensgebonden ziekte-uitbraken of epidemieën; 2. **Geneesmiddelen**: Farmaceutische producten, zoals injecties of zeldzame medicijnen, die in	Ja	• **Diefstal of verlies**: Door de kleine omvang kunnen deze items gemakkelijk gestolen of ongezien verloren raken; • **Fraude bij voorraadbeheer**: Werknemers of leveranciers kunnen voorraadverplaatsingen of aantallen manipuleren zonder dat dit direct opvalt, wat kan leiden tot onregelmatigheden; • **Verkoop of vervalsing**: Producten van hoge waarde kunnen vervalst worden of onrechtmatig verkocht aan derden, wat moeilijker te traceren is; • **Omvangrijke vraag en voorraadtekort**: Door de grote vraag kunnen tekorten ontstaan, wat kan leiden tot druk om sneller te leveren zonder strikte controles, waardoor fouten of misbruik kunnen optreden; • **Hoge verzekeringskosten**: Vanwege hun hoge waarde kunnen dergelijke items duurder zijn om te verzekeren, wat extra kosten met zich meebrengt.	M 	H 	Voor GGDrU kunnen de volgende beheersmaatregelen worden getroffen om risico's te minimaliseren bij kleine maar waardevolle voorraaditems: 1. **Strikte voorraadregistratie**: Gedetailleerde en up-to-date registratie van alle voorraaditems, vooral die met een hoge waarde. Gebruik van barcode- of RFID-technologie om de voorraadniveaus automatisch bij te houden en afwijkingen snel te identificeren; 2. **Frequente inventarisaties**: Regelmatig fysieke controles van de voorraad om discrepanties tussen de werkelijke en geregistreerde aantallen snel op te sporen; 3. **Toegangscontrole en beveiliging**: Beperkte toegang tot opslagruimtes alleen tot geautoriseerd personeel en implementeer beveiligingssystemen zoals cameratoezicht, alarmsystemen en elektronische toegangskaarten; 4. **Functiescheiding**: Gescheide taken van medewerkers die betrokken zijn bij het beheer van de voorraad, zoals inkoop, opslag en registratie, om de kans op	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
kleine verpakkingen komen maar vaak zeer hoge prijzen hebben. De beschikbaarheid en vraag naar deze middelen kunnen sterk variëren, vooral bij plotselinge uitbraken van ziekten; 3. **Vaccins**: Vaccins tegen infectieziekten zijn vaak klein van formaat, maar de waarde en vraag naar deze items kunnen enorm zijn, vooral in tijden van pandemieën of gezondheidscrises; 4. **Desinfectie-middelen**: Kleine flacons met handdesinfectiemiddelen of ontsmettingsmiddelen zijn zeer waardevol, vooral in de context van volksgezondheid en hygiëne. De vraag naar deze producten is toegenomen in de nasleep van de COVID-19-pandemie; 5. **Medische verbruiksartikelen**: Voorwerpen zoals steriele naalden, handschoenen en verbandmiddelen zijn klein en goedkoop in					fraude door één persoon te verminderen; 5. **Rapportage en monitoring**: Gebruik van systemen die automatisch rapporteren wanneer er afwijkingen of verdachte activiteiten worden gedetecteerd, zoals onverwachte wijzigingen in de voorraad; 6. **Beheer van inkoop- en bestelsystemen**: Limieten voor bestellingen en controleer regelmatig de afstemming tussen bestellingen, ontvangsten en uitgiften van voorraaditems om fouten of fraude te voorkomen.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
aanschaf, maar ze zijn essentieel voor de dagelijkse operaties in de gezondheidszorg en hebben daardoor een constante vraag.							
Acties voor verbetering Om de risico's voor GGDrU met betrekking tot waardevolle voorraaditems en mogelijke verliezen te minimaliseren, zijn de volgende acties vereist: 3. **Strengere toegangscontroles**: Beperking van de toegang tot de opslagruimten waar waardevolle en gewilde voorraaditems worden bewaard. Alleen bevoegde medewerkers mogen toegang hebben, en elke toegang moet worden gelogd; 4. **Regelmatige voorraadcontroles en audits**: Voer periodieke controles uit om de daadwerkelijke voorraad af te stemmen met de geregistreerde voorraad in het systeem. Dit helpt om eventuele discrepanties vroegtijdig op te sporen; 5. **Gebruik van technologie**: Overweeg het gebruik van technologie zoals RFID (Radio Frequency Identification) of barcodesystemen om voorraadbewegingen nauwkeuriger bij te houden en verlies of diefstal te detecteren; 6. **Strikte functiescheiding**: Zorg ervoor dat er een duidelijke scheiding is tussen medewerkers die verantwoordelijk zijn voor het registreren van de voorraad, het beheren van de fysieke voorraad, en het uitvoeren van de controles; 7. **Training en bewustzijn**: Zorg ervoor dat medewerkers goed getraind zijn in het naleven van interne procedures en zich bewust zijn van de risico's en gevolgen van fraude of verlies; 8. **Cameratoezicht en beveiliging**: Installeer camera's in magazijnen en opslagruimten om toezicht te houden op de toegang en beweging van voorraad; 9. **Snelle opvolging van afwijkingen**: Zorg voor een heldere procedure waarbij afwijkingen tussen de fysieke voorraad en de administratie snel worden opgevolgd en opgelost.							
• Recente of verwachte veranderingen in het salaris van werknemers of in hun beloofde pensioenrechten;	Ja	• **Financiële Belastingen**: Veranderingen in salarissen of pensioenrechten kunnen leiden tot hogere personeelskosten, wat invloed kan hebben op het budget van de organisatie. Dit kan vooral riskant zijn als de organisatie niet adequaat is voorbereid op deze extra uitgaven; • **Werknemersmotivatie en retentie**: Als wijzigingen in beloningen niet goed worden	M 	H 	• **Transparante Communicatie**: Duidelijke communicatie met medewerkers over eventuele wijzigingen in salaris en pensioen. Dit kan helpen om onduidelijkheid en ontevredenheid te voorkomen; • **Financiële Planning**: Regelmatige financiële analyses om de impact van salaris- en pensioenveranderingen op het totale budget van de organisatie te beoordelen. Dit helpt bij het	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		gecommuniceerd of als werknemers het gevoel hebben dat ze niet eerlijk worden behandeld, kan dit leiden tot een afname van de motivatie en een verhoogd personeelsverloop. Dit kan op lange termijn de effectiviteit van de organisatie beïnvloeden; • **Compliance en juridische risico's**: Wijzigingen in salarissen of pensioenregelingen moeten voldoen aan arbeidswetgeving en andere regelgeving. Onjuiste implementatie kan leiden tot juridische problemen of boetes; • **Verhoogde verwachtingen**: Als werknemers op basis van recente wijzigingen hogere verwachtingen ontwikkelen over toekomstige beloningen, kan dit leiden tot teleurstelling en ontevredenheid als deze			identificeren van eventuele financiële risico's vroegtijdig; • **Marktonderzoek**: Marktonderzoeken om te begrijpen hoe de beloningen en pensioenrechten van GGDrU zich verhouden tot vergelijkbare organisaties. Dit kan helpen bij het bepalen van eerlijke en competitieve beloningsstructuren; • **Flexibele Beloningsstructuren**: Flexibele beloningsstructuren die kunnen worden aangepast aan de behoeften van de organisatie en de werknemers. Dit kan bijvoorbeeld het aanbieden van keuzemogelijkheden in secundaire arbeidsvoorwaarden inhouden; • **Opleiding en Ontwikkeling**: Training en ontwikkeling voor personeel, zodat zij beter voorbereid zijn op veranderingen in hun rol en verantwoordelijkheden, wat kan bijdragen aan een betere acceptatie van salarisveranderingen;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		verwachtingen niet worden waargemaakt; • **Impact op Pensioenvoorzieningen**: Als pensioenrechten veranderen, kunnen er implicaties zijn voor de financiële planning van de organisatie. Dit kan leiden tot problemen als werknemers besluiten hun pensioen eerder op te nemen of als de waarde van pensioenvoorzieningen fluctueert.			• **Monitoring en Evaluatie**: Systeem voor het monitoren van de tevredenheid van medewerkers en de effecten van salarisveranderingen. Dit kan bijvoorbeeld door middel van enquêtes of feedbacksessies.		

Acties voor verbetering

Voor GGDrU zijn er verschillende acties voor verbetering te overwegen met betrekking tot recente of verwachte wijzigingen in de salarissen en pensioenrechten van werknemers:

1. **Transparante communicatie**:
   - Zorg voor open en duidelijke communicatie met medewerkers over veranderingen in salarissen en pensioenregelingen. Dit kan helpen om onduidelijkheden en ontevredenheid te verminderen;
2. **Feedback mechanismen**:
   - Implementeer systemen voor het verzamelen van feedback van medewerkers over hun compensatie en voordelen. Dit kan door middel van enquêtes of regelmatige gesprekken, zodat medewerkers zich gehoord voelen en hun zorgen kunnen delen;
3. **Marktonderzoek**:
   - Voer regelmatig marktonderzoek uit om ervoor te zorgen dat de salarissen en voordelen concurrerend zijn met andere organisaties in de sector. Dit helpt om talent aan te trekken en te behouden;
4. **Flexibele beloningsstructuren**:
   - Overweeg het implementeren van flexibele beloningsstructuren die het mogelijk maken om tegemoet te komen aan de verschillende behoeften en voorkeuren van medewerkers, zoals keuzemogelijkheden in secundaire arbeidsvoorwaarden;
5. **Training en ontwikkeling**:
   - Bied medewerkers mogelijkheden voor professionele ontwikkeling en training. Dit kan bijdragen aan hun tevredenheid en motivatie, zelfs wanneer salarisveranderingen plaatsvinden;
6. **Regelmatige beoordelingen**:
   - Voer periodieke beoordelingen uit van de beloningsstructuren en pensioenregelingen om ervoor te zorgen dat ze blijven voldoen aan de behoeften van zowel de organisatie als de werknemers;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
7. **Risicoanalyse**: ○ Voer een gedetailleerde risicoanalyse uit om potentiële impact en kans op ontevredenheid te beoordelen. Dit kan helpen bij het ontwikkelen van gerichte strategieën om deze risico's te mitigeren.							
• Interne promoties en vergoedingen of andere beloningen die afwijken van de oorspronkelijke verwachtingen.	Ja	1. **Ontevredenheid onder medewerkers**: Als medewerkers zich niet erkend voelen of als de beloningen niet in lijn zijn met hun verwachtingen, kan dit leiden tot onvrede en een slechte werksfeer. Dit kan ook de motivatie en productiviteit negatief beïnvloeden; 2. **Ontevredenheid onder medewerkers**: Als medewerkers zich niet erkend voelen of als de beloningen niet in lijn zijn met hun verwachtingen, kan dit leiden tot onvrede en een slechte werksfeer. Dit kan ook de motivatie en productiviteit negatief beïnvloeden; 3. **Hogere personeelsverloop**: Afwijkingen in beloningen kunnen leiden tot een hogere turnover van personeel, vooral als medewerkers het gevoel	M tot H 	M tot H 	• **Duidelijke beleidslijnen**: Heldere richtlijnen voor interne promoties en beloningsstructuren, zodat alle medewerkers weten wat ze kunnen verwachten en hoe beslissingen worden genomen; • **Transparante communicatie**: Open communicatie over de criteria voor promoties en beloningen. Dit helpt om misverstanden en onzekerheid te verminderen; • **Regelmatige audits**: Periodieke controles om ervoor te zorgen dat het beloningsbeleid wordt nageleefd en dat er geen afwijkingen zijn van de vastgestelde richtlijnen; • **Training voor leidinggevenden**: Training voor managers en leidinggevenden over de juiste procedures en best practices voor het toekennen van beloningen en promoties; • **Feedbackmechanismen**: Mechanismen waarmee medewerkers feedback kunnen geven over het	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		hebben dat hun inzet niet wordt gewaardeerd. Dit kan extra kosten met zich meebrengen voor wervings- en opleidingsprocessen; 4. **Implicaties voor teamdynamiek**: Wanneer interne promoties of beloningen als oneerlijk worden ervaren, kan dit de samenwerking binnen teams verstoren. Dit kan leiden tot een lagere algehele effectiviteit en cohesie binnen de organisatie; 5. **Reputatierisico**: Negatieve percepties over interne promoties en beloningsstructuren kunnen de reputatie van GGDrU schaden, zowel intern als extern. Dit kan invloed hebben op de aantrekkelijkheid als werkgever en de relatie met belanghebbenden. 6. **Compliance-risico**: Afwijkingen in vergoedingen of			beloningsbeleid en promotiebeslissingen, zodat er ruimte is voor verbetering; • **Benchmarking**: Beloningsstructuren en promoties vergelijken met die van vergelijkbare organisaties om ervoor te zorgen dat ze concurrerend en eerlijk zijn.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		beloningen kunnen ook leiden tot juridische of compliance-issues, vooral als deze niet in overeenstemming zijn met arbeidswetgeving of interne richtlijnen.					
Acties voor verbetering Door deze acties te implementeren, kan GGDrU niet alleen de interne processen verbeteren, maar ook het vertrouwen en de tevredenheid van medewerkers vergroten: 1. **Transparante communicatie**: Zorg voor duidelijke communicatie over de criteria voor promoties en beloningen. Dit kan door middel van informatiebijeenkomsten of een interne nieuwsbrief waarin de processen worden uitgelegd; 2. **Feedback mechanismen**: Implementeer systemen waarmee medewerkers feedback kunnen geven over het belonings- en promotieproces. Dit helpt bij het identificeren van mogelijke onvrede of misverstanden; 3. **Training en opleiding**: Bied trainingen aan voor managers en HR-medewerkers over het voeren van eerlijke en transparante beoordelingsgesprekken. Dit zorgt ervoor dat iedereen goed voorbereid is en dat de processen eerlijk worden uitgevoerd; 4. **Regelmatige evaluatie van beleid**: Evalueer regelmatig de beloningsstructuren en promotiecriteria om ervoor te zorgen dat ze blijven aansluiten bij de behoeften van de organisatie en de verwachtingen van de medewerkers; 5. **Creëren van eerlijke beoordelingscriteria**: Ontwikkel duidelijke en meetbare criteria voor prestaties die voor iedereen toegankelijk zijn. Dit kan helpen om subjectiviteit uit het beoordelingsproces te verwijderen; 6. **Betrekken van medewerkers**: Betrek medewerkers bij het proces van het ontwikkelen of herzien van belonings- en promotiebeleid. Dit vergroot de betrokkenheid en het gevoel van eigenaarschap; 7. **Monitoring van medewerkerstevredenheid**: Voer regelmatig enquêtes uit om de tevredenheid van medewerkers te meten over beloningen en promoties. Dit kan helpen bij het identificeren van gebieden die verbetering behoeven.						
• Bedrijfsmiddelen die klein van formaat zijn, eenvoudig te verkopen, of waarvan de eigendom niet duidelijk is vastgesteld. • **Medische apparatuur**: Apparaten zoals bloeddrukmeters, glucosemeters of kleine diagnostische tools zijn vaak klein, maar hebben een hoge waarde en zijn	Ja	• **Diefstal of verlies**: Kleine apparaten zijn gemakkelijk te stelen of te verliezen, wat kan leiden tot verlies van gevoelige patiëntgegevens en vertrouwelijke informatie; • **Databeveiliging**: Als deze apparaten niet goed beveiligd zijn, kunnen ze kwetsbaar zijn voor hacking of malware, wat kan resulteren in datalekken of ongeoorloofde toegang tot vertrouwelijke informatie; • **Onvoldoende beheer**: Het gebrek aan een duidelijk	H ☹	H ☹	**1. Beveiligingsmaatregelen voor apparaten** • **Fysieke beveiliging**: Veilige opslag en gebruik van apparaten, bijvoorbeeld door ze op slot te bewaren of te gebruiken met beveiligde kabels; • **Diefstalpreventie**: Gebruik van labels of GPS-tracking om apparaten te kunnen volgen in geval van verlies of diefstal; **2. Databeveiliging** • **Encryptie**: Versleutelde gegevens op apparaten om gevoelige	M tot H 😐 ☹	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
essentieel voor medische zorg; • **Medicijnen en vaccins**: Kleine verpakkingen van medicijnen of vaccins kunnen waardevol zijn, vooral in tijden van een gezondheidscrisis; • **Persoonlijke beschermingsmiddelen**: Items zoals mondkapjes, handschoenen en gezichtsschermen zijn klein, maar essentieel en van hoge waarde, vooral tijdens pandemieën; • **Computerhardware**: Dit omvat kleine elektronische apparaten zoals laptops, tablets en mobiele devices, die worden ingezet voor telewerken of voor het registreren van patiëntgegevens; • **Diagnostische testkits**: Kits voor COVID-19-tests of andere infectieziekten zijn klein van formaat maar hebben een hoge waarde, vooral bij uitbraken.		eigendomsregister of een goed beheer van deze bedrijfsmiddelen kan leiden tot verwarring over wie verantwoordelijk is voor het onderhoud en de beveiliging van de apparatuur; • **Verouderde technologie**: Apparaten die niet regelmatig worden bijgewerkt of vervangen, kunnen verouderd raken, wat de efficiëntie en effectiviteit van het werk kan verminderen; • **Inadequate training**: Gebrek aan training voor medewerkers over hoe ze veilig en effectief gebruik moeten maken van deze apparaten kan leiden tot onbedoelde fouten of beveiligingslekken.			informatie te beschermen in het geval van diefstal of verlies; • **Firewall en antivirus**: Installatie en onderhoud firewalls en antivirussoftware om apparaten te beschermen tegen ongeautoriseerde toegang en malware; **3. Actief beheer van apparaten** • **Eigendomsregistratie**: Gedetailleerd register van alle apparaten, inclusief wie verantwoordelijk is voor elk apparaat en de bijbehorende onderhoudsverplichtingen; • **Periodieke inventarisatie**: Regelmatig inventarisatie van de apparaten om te zorgen dat alles goed beheerd wordt en dat verloren of gestolen apparaten worden gerapporteerd; **4. Regelmatige updates en vervangingen** • **Software-updates**: Alle apparaten worden regelmatig bijgewerkt met de nieuwste software en beveiligingspatches; • **Vervangingsschema**: Een schema voor het vervangen van verouderde apparatuur om ervoor te zorgen dat medewerkers beschikken over up-to-date technologie; **5. Training en bewustwording** • **Training voor Medewerkers**: Bied training aan over het veilig gebruik van apparatuur, inclusief hoe te reageren bij verlies of		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					diefstal, en het herkennen van beveiligingsrisico's; • **Bewustwordingscampagnes**: Campagnes om medewerkers te informeren over het belang van databeveiliging en het veilig omgaan met apparaten; **6. Incident management** • **Incident response plan**: Een plan voor het omgaan met incidenten, zoals diefstal of verlies van apparaten, inclusief communicatierichtlijnen en procedures voor het rapporteren van incidenten; **7. Beleid en procedures** • **Beveiligingsbeleid**: Beleid voor het gebruik van informatichardware en databeveiliging, en zorg ervoor dat alle medewerkers hiervan op de hoogte zijn; • **Audit en toezicht**: Voer regelmatig audits uit om de naleving van beveiligingsbeleid en -procedures te controleren en om zwakke plekken in de beveiliging te identificeren.		

Acties voor verbetering
Door deze acties voor verbetering toe te passen, kan GGDrU de risico's die verband houden met bedijfsmiddelen beter beheersen en zorgen voor een efficiënter beheer van waardevolle middelen:

1. **Beveiligingsmaatregelen versterken**:
    - **Fysieke Beveiliging**: Verbeter de beveiliging van opslagruimtes voor bedrijfsmiddelen, bijvoorbeeld door cameratoezicht en toegangsbeperkingen in te voeren;
    - **Beveiliging tegen diefstal**: Implementeer sloten of andere fysieke beveiligingsoplossingen om diefstal te voorkomen;
2. **Duidelijke eigendomsregistratie**:
    - **Registratie van bedrijfsmiddelen**: Houd een gedetailleerd register bij van alle bedrijfsmiddelen, inclusief informatie over eigendom, locatie en gebruik;
    - **Regelmatige controle**: Voer periodieke controles uit om te bevestigen dat de gegevens in het register correct zijn en dat alle bedrijfsmiddelen worden beheerd;
3. **Bewustwording en training**:

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ **Training voor medewerkers**: Bied trainingen aan om medewerkers bewust te maken van het belang van het veilig beheren van bedrijfsmiddelen en het volgen van procedures; ○ **Informatie over protocollen**: Zorg ervoor dat medewerkers op de hoogte zijn van de juiste procedures voor het omgaan met en het rapporteren van bedrijfsmiddelen; 4. **Onderhoud en vervanging**: ○ **Onderhoudsplan**: Stel een plan op voor regelmatig onderhoud van bedrijfsmiddelen om ervoor te zorgen dat ze in goede staat blijven; ○ **Vervangingsbeleid**: Ontwikkel een beleid voor het tijdig vervangen van bedrijfsmiddelen die verouderd of niet meer functioneel zijn; 5. **Beheer van incidenten**: ○ **Protocol voor diefstal of verlies**: Stel een protocol op voor het omgaan met diefstal of verlies van bedrijfsmiddelen, inclusief rapportage en follow-up; ○ **Evaluatie van incidenten**: Voer na elk incident een evaluatie uit om te leren van de situatie en toekomstige risico's te verminderen.							
2.2.2 Onvoldoende interne beheersingsmaatregelen met betrekking tot bedrijfsmiddelen kunnen leiden tot een verhoogd risico op oneigenlijk gebruik of toe-eigening van deze bedrijfsmiddelen. Dit kan gebeuren door verschillende factoren, zoals:							
• Onvoldoende scheiding van taken of onafhankelijke controles, zowel voor de verwerking van informatie als voor beheertaken; Een goede scheiding van functies en onafhankelijke controles zijn essentieel voor de bescherming van bedrijfsmiddelen en het waarborgen van de nauwkeurigheid en integriteit van informatie binnen GGDrU. Dit verwijst naar het gebrek aan duidelijke scheidingen in verantwoordelijkheden binnen	Ja	• **Fraude en misbruik**: Wanneer dezelfde persoon verantwoordelijk is voor zowel informatieverwerking als beheer, kunnen ze gemakkelijker frauduleuze handelingen uitvoeren zonder dat dit wordt opgemerkt. Dit kan leiden tot het ongeoorloofd toe-eigenen van bedrijfsmiddelen of het manipuleren van gegevens; • **Verlies van gegevensintegriteit**: Zonder onafhankelijke controles is er een verhoogd risico op fouten in de gegevensverwerking. Dit kan resulteren in onjuiste of onbetrouwbare informatie, wat	H ☹	H ☹	• **Functiescheiding**: Belangrijke taken, zoals autorisatie, uitvoering en controle, door verschillende personen worden uitgevoerd. Dit helpt om de kans op frauduleuze handelingen te verkleinen en verhoogt de transparantie; • **Onafhankelijke controles**: Regelmatige onafhankelijke controles en audits uit om de effectiviteit van de interne controles te waarborgen. Dit kan interne of externe auditors omvatten die de processen en procedures beoordelen; • **Toegangscontrole**:	M tot H 😐 ☹	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
de organisatie en kan leiden tot risico's, zoals: • **Fraude**: Wanneer één persoon zowel de verantwoordelijkheid heeft voor het verwerken van informatie als het beheer ervan, kan dat de kans op oneigenlijk gedrag verhogen, zoals diefstal of manipulatie van gegevens; • **Fouten**: Het ontbreken van onafhankelijke controles kan ervoor zorgen dat fouten niet tijdig worden opgemerkt, wat kan leiden tot aanzienlijke problemen binnen de organisatie; • **Verlies van vertrouwen**: Onvoldoende scheiding van functies kan ook de transparantie en integriteit van de organisatie ondermijnen, wat kan resulteren in een verminderd vertrouwen van stakeholders, zoals klanten of toezichthouders.		schadelijk kan zijn voor beslissingen op alle niveaus van de organisatie; • **Beveiligingslekken**: Inadequate controlemaatregelen kunnen ook leiden tot datalekken. Persoonlijke of gevoelige gegevens van patiënten kunnen in gevaar komen, wat kan resulteren in ernstige juridische en financiële gevolgen voor de organisatie; • **Verlies van vertrouwen**: Wanneer stakeholders (zoals inwoners, medewerkers of gemeentes) merken dat er onvoldoende controles zijn, kan dit het vertrouwen in de organisatie ondermijnen. Dit kan gevolgen hebben voor de reputatie van GGDrU en kan de samenwerking met andere organisaties bemoeilijken; • **Onvoldoende naleving van regelgeving**: Als er geen onafhankelijke controles zijn, kan het zijn dat GGDrU niet voldoet aan relevante wet- en regelgeving, wat kan leiden tot juridische sancties of boetes.			Strikte toegangscontroles voor systemen en bedrijfsmiddelen, zodat alleen bevoegde medewerkers toegang hebben tot gevoelige informatie en belangrijke functies; • **Documentatie en rapportage**: Duidelijke documentatie van alle processen en verantwoordelijkheden. Regelmatige rapportages kunnen helpen bij het identificeren van afwijkingen en het waarborgen van verantwoordingsplicht; • **Training en bewustwording**: Medewerkers trainen in de juiste procedures en het belang van functiescheiding. Dit vergroot hun inzicht in de noodzaak van controles en draagt bij aan een cultuur van naleving; • **Beleid en procedures**: Duidelijke beleidslijnen en procedures voor het beheer van beleidsmiddelen en informatie. Dit kan helpen om richtlijnen te bieden voor het handelen in overeenstemming met de vastgestelde controles; • **Monitoring en evaluatie**: Continue monitoring uit van processen en controles om tijdig problemen te identificeren. Regelmatige evaluaties helpen om de effectiviteit van de maatregelen te waarborgen en aanpassingen te maken waar nodig.		
Acties voor verbetering Door deze acties te implementeren, kan GGDrU de interne controle verbeteren en de risico's van inadequate scheiding van taken minimaliseren:							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• **Duidelijke taakverdeling:** Zorg voor een heldere verdeling van taken binnen teams, zodat verantwoordelijkheden voor verschillende processen gescheiden zijn. Dit voorkomt dat één persoon te veel controle heeft over belangrijke taken; • **Implementatie van controlesystemen:** Stel controlesystemen in die onafhankelijke verificatie van belangrijke handelingen vereisen, zoals financiële transacties of gegevensinvoer. Dit kan ook inhouden dat verschillende personen verantwoordelijk zijn voor het goedkeuren en uitvoeren van processen; • **Regelmatige training:** Bied training aan medewerkers over het belang van functiescheiding en de risico's van onvoldoende controle. Dit vergroot het bewustzijn en begrip van de procedures die gevolgd moeten worden; • **Interne audits:** Voer periodieke interne audits uit om te controleren op naleving van de scheiding van taken en om eventuele tekortkomingen in de controlesystemen te identificeren; • **Monitoring en rapportage:** Implementeer een systeem voor voortdurende monitoring dat afwijkingen of ongebruikelijke activiteiten in real-time kan signaleren en rapporteren aan het management; • **Feedback mechanismen:** Zorg voor feedbackmechanismen waarin medewerkers hun zorgen kunnen delen over onvoldoende scheiding van taken of andere controlekwesties zonder angst voor repercussies; • **Gebruik van technologie:** Maak gebruik van technologie en software om processen te automatiseren, zodat handmatige fouten en het risico op fraude door menselijke interactie worden verminderd; • **Evaluatie en verbetering:** Evalueer regelmatig de effectiviteit van de scheiding van taken en controles, en pas waar nodig het beleid en de procedures aan om de effectiviteit te verbeteren.							
• Onvoldoende toezicht op de uitgaven van het management, waaronder reiskosten en andere vergoedingen. Dit zijn vaak kosten die medewerkers maken om hun werk effectief te kunnen uitvoeren, zoals vergoedingen voor maaltijden, lunch en overnachtingen.	Ja	• **Fraude en misbruik**: Gebrek aan controle kan leiden tot misbruik van vergoedingen. Medewerkers kunnen valse declaraties indienen voor kosten die niet zijn gemaakt of overdrijven wat ze hebben uitgegeven; • **Verlies van vertrouwen**: Als medewerkers het gevoel hebben dat er geen adequate controle is over uitgaven, kan dit leiden tot wantrouwen in het management. Dit kan de motivatie en samenwerking binnen het team negatief beïnvloeden; • **Onjuiste financiële Rapportage**: Onvoldoende toezicht kan leiden tot onnauwkeurigheden in financiële rapportages, waardoor het moeilijk wordt om de werkelijke	M 	H 	• **Duidelijke richtlijnen en beleid**: Heldere richtlijnen voor het indienen van onkostenvergoedingen, inclusief welke kosten wel en niet vergoed worden. Dit helpt om verwachtingen te verduidelijken en voorkomt misbruik; • **Tweede Controle**: Een systeem waarbij alle onkostenvergoedingen een tweede goedkeuring vereisen van een leidinggevende of financiën. Dit kan helpen om onterecht ingediende declaraties te identificeren en te voorkomen; • **Regelmatige audit en monitoring**: Regelmatig audits van de ingediende onkostenvergoedingen om afwijkingen of onregelmatigheden te identificeren. Dit kan ook helpen om trends in uitgaven te	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		financiële positie van de organisatie te begrijpen; • **Overmatige kosten**: Zonder goed toezicht kunnen uitgaven hoger uitvallen dan nodig is. Dit kan leiden tot onnodige kosten voor de organisatie, waardoor budgetten overschreden worden; • **Compliance risico's**: Als GGDrU niet voldoet aan interne of externe richtlijnen voor kostenbeheer, kan dit leiden tot juridische problemen of sancties; • **Onvoldoende verantwoording**: Het ontbreken van adequate controlemechanismen kan de verantwoordelijkheid van medewerkers en management verminderen, wat leidt tot een cultuur waarin men zich niet verantwoordelijk voelt voor het beheer van publieke middelen.			analyseren en eventuele misbruiken op te sporen; • **Training en bewustwording**: Trainingen voor medewerkers en management over het beleid en de procedures rondom onkostenvergoedingen. Dit kan helpen om bewustzijn te creëren over de gevolgen van misbruik en het belang van transparantie**;** • **Gebruik van software voor kostenbeheer**: Digitaal systeem voor het indienen en goedkeuren van onkosten. Dit maakt het makkelijker om gegevens te volgen, rapportages te genereren en afwijkingen op te merken; • **Feedback mechanisme**: Een anoniem feedbackmechanisme waarin medewerkers zorgen of misstanden met betrekking tot onkostenvergoedingen kunnen rapporteren. Dit kan helpen om een cultuur van verantwoordelijkheid en transparantie te bevorderen; • **Regelmatige rapportage aan het management**: Rapporten worden gepresenteerd aan het management over uitgaven en trends in onkostenvergoedingen. Dit houdt het management verantwoordelijk en bewust van de uitgavenpatronen.		

Acties voor verbetering
Door deze acties te implementeren, kan GGDrU de controle over de uitgaven verbeteren, het risico op fraude en misbruik minimaliseren, en een cultuur van financiële verantwoordelijkheid bevorderen:

1. **Implementeren van strikte declaratieprocedures**:

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
o Ontwikkel duidelijke richtlijnen voor het indienen van onkosten, inclusief wat wel en niet vergoed wordt. Zorg ervoor dat deze richtlijnen goed gecommuniceerd worden naar alle medewerkers; 2. **Regelmatige training en bewustwording**: o Bied regelmatig trainingen aan over de procedures voor het indienen van onkosten en het belang van financiële integriteit. Dit helpt medewerkers te begrijpen wat van hen verwacht wordt en de gevolgen van onjuiste declaraties; 3. **Invoeren van een goedkeuringsproces**: o Stel een systeem in waarbij alle uitgaven door meerdere niveaus van management goedgekeurd moeten worden. Dit kan helpen om onterecht ingediende declaraties te voorkomen; 4. **Gebruik van Technologie voor Transparantie**: o Maak gebruik van software en digitale systemen om uitgaven te registreren en te controleren. Dit kan helpen bij het automatiseren van het proces en het vergroten van de transparantie; 5. **Periodieke audits**: o Voer regelmatig interne audits uit op uitgaven en vergoedingen om eventuele onregelmatigheden tijdig te signaleren en te corrigeren; 6. **Cultuur van verantwoordelijkheid**: o Stimuleer een organisatiecultuur waarin medewerkers zich verantwoordelijk voelen voor het correct indienen van onkosten en het beheren van middelen. Dit kan bijdragen aan een grotere betrokkenheid bij de integriteit van financiële processen; 7. **Feedbackmechanismen**: o Stel een systeem in waar medewerkers anoniem feedback kunnen geven over de processen en controles. Dit kan helpen om zwakke plekken in het systeem te identificeren en te verbeteren.							
• Onvoldoende toezicht door het management op medewerkers die verantwoordelijk zijn voor bedrijfsmiddelen van andere locaties, waaronder het gebrek aan adequate controle of monitoring;	Ja	• **Fraude en diefstal**: Medewerkers kunnen de kans grijpen om bedrijfsmiddelen toe te eigenen of ongeoorloofd gebruik te maken van middelen zonder ontdekking; • **Fouten en onregelmatigheden**: Een gebrek aan controle kan leiden tot administratieve fouten, verkeerde registratie van bedrijfsmiddelen of ongepaste uitgaven; • **Inconsistentie in procedures**: Onvoldoende toezicht kan resulteren in variaties in de naleving van procedures, wat leidt tot onbetrouwbare gegevens en processen**;**	L 	M 	• **Interne Controlemechanismen**: Strikte procedures voor autorisatie en controle van bedrijfsmiddelen, inclusief dienstauto's; • **Regelmatig audits**: Periodieke audits van bedrijfsmiddelen en gebruik van middelen om onregelmatigheden en fouten tijdig te identificeren; • **Documentatie en rapportage**: Gedetailleerde registratie van het gebruik van bedrijfsmiddelen, zoals dienstauto's, inclusief kilometerregistratie en doeleinden van gebruik; • **Training en voorlichting**: Trainingen voor medewerkers over het juiste gebruik van bedrijfsmiddelen • en de gevolgen van misbruik;	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		• **Verlies van bedrijfsmiddelen**: Het risico op verlies of beschadiging van bedrijfsmiddelen neemt toe wanneer er geen adequate monitoring is; • **Slecht medewerkersmoraal**: Het gevoel dat er geen toezicht is, kan leiden tot een gebrek aan verantwoordelijkheid en betrokkenheid onder medewerkers. • **Reputatieschade**: Onregelmatigheden of frauduleuze activiteiten kunnen schadelijk zijn voor de reputatie van de organisatie als deze aan het licht komen. Het gebruik van een dienstauto valt ook onder de risico's die gepaard gaan met onvoldoende toezicht op medewerkers die verantwoordelijk zijn voor bedrijfsmiddelen van andere locaties. Hier zijn enkele specifieke risico's met betrekking tot het gebruik van dienstauto's: 1. **Misbruik van de dienstauto**: Medewerkers kunnen de dienstauto voor persoonlijke doeleinden gebruiken zonder toestemming, wat leidt tot onterecht gebruik van bedrijfsmiddelen; 2. **Ongevallen en Aansprakelijkheid**: Onvoldoende toezicht kan resulteren in een verhoogd			• **Toezicht en monitoring**: Real-time monitoring van het gebruik van dienstauto's en andere middelen, met duidelijke verantwoordelijkheden voor toezicht; • **Onderhoudsprogramma**: Een regulier onderhoudsprogramma voor dienstauto's om de veiligheid en betrouwbaarheid te waarborgen; • **Feedbackmechanismen**: Kanalen waar medewerkers anoniem feedback kunnen geven over onregelmatigheden of onethisch gedrag, waardoor een cultuur van verantwoordelijkheid en transparantie wordt bevorderd; • **Duidelijke Richtlijnen**: Heldere richtlijnen voor het gebruik van dienstauto's, inclusief beperkingen en vereisten voor toestemming voor persoonlijk gebruik; • **Consequenties bij overtredingen**: Duidelijke consequenties voor medewerkers die de regels overtreden, zodat er een sterkere motivatie is om zich aan de richtlijnen te houden.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		risico op ongevallen of schade aan de auto, waarvoor de organisatie aansprakelijk kan zijn; 3. **Slechte onderhoudspraktijken**: Een gebrek aan controle kan ertoe leiden dat voertuigen niet regelmatig worden onderhouden, wat hun veiligheid en betrouwbaarheid in gevaar brengt; 4. **Verhoogde kosten**: Ongeoorloofd gebruik kan leiden tot hogere brandstof- en onderhoudskosten, die niet worden verantwoord; 5. **Beveiligingsrisico's**: Dienstauto's kunnen waardevolle bedrijfsinformatie bevatten (zoals laptops of documenten), en een gebrek aan toezicht kan het risico op diefstal of verlies vergroten.					
• Onvoldoende screening van sollicitanten die, na hun aanstelling, toegang hebben gekregen tot bedrijfsmiddelen; Onvoldoende screening van sollicitanten kan leiden tot het aannemen van medewerkers met een verhoogd risico op	Ja	• **Fraude en diefstal**: Aangenomen medewerkers kunnen bedrijfsmiddelen misbruiken of verduisteren zonder dat dit direct wordt opgemerkt • **Integriteitsproblemen**: Medewerkers met een twijfelachtige achtergrond kunnen onethisch gedrag vertonen, wat	L 	M 	1. **Grondige achtergrondcontroles**: Uitgebreide achtergrondcontroles, inclusief het verifiëren van referenties, werkervaring en eventuele strafrechtelijke verleden van kandidaten, voordat ze toegang krijgen tot bedrijfsmiddelen;	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
frauduleus gedrag. Wanneer deze medewerkers toegang hebben tot waardevolle bedrijfsmiddelen, vergroot dit de kans op misbruik of diefstal. Het is cruciaal om grondige achtergrondcontroles en referentiechecks uit te voeren voordat iemand wordt aangesteld, vooral voor functies die toegang tot bedrijfsmiddelen vereisen.		leidt tot schending van vertrouwen binnen de organisatie**;** • **Reputatieschade**: Onregelmatigheden kunnen leiden tot negatieve publiciteit en verlies van vertrouwen van klanten en partners; • **Financiële verliezen**: Frauduleuze activiteiten kunnen aanzienlijke financiële schade toebrengen aan de organisatie; • **Verhoogde Risico's**: Een gebrek aan controle bij de aanwervingsprocedure kan leiden tot een hogere kans op misbruik van bedrijfsmiddelen.			2. **Verklaring Omtrent Gedrag (VOG)**: VOG voor nieuwe medewerkers, zodat je inzicht krijgt in eventuele strafbare feiten die relevant kunnen zijn voor de functie en toegang tot bedrijfsmiddelen; 3. **Identiteitsverificatie**: Strikte identificatieprocedure om te bevestigen dat kandidaten de juiste kwalificaties en identificatie hebben; 4. **Screening op integriteit**: Psychologische tests of assessments om de integriteit en betrouwbaarheid van sollicitanten te beoordelen; 5. **Beleid voor toegang tot bedrijfsmiddelen**: Duidelijke richtlijnen op over wie toegang heeft tot welke bedrijfsmiddelen, gebaseerd op hun rol en verantwoordelijkheden binnen de organisatie; 6. **Training voor wervingspersoneel**: Trainingen voor HR- en wervingspersoneel om hen bewust te maken van het belang van screening en de bijbehorende risico's; 7. **Audits van wervingsprocessen**: Regelmatig audits van het wervings- en screeningproces om te waarborgen dat procedures effectief worden nageleefd; 8. **Feedbackmechanismen**: Systeem waar medewerkers anoniem zorgen of verdachte gedragingen kunnen melden met		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					betrekking tot nieuwe aanstellingen; 9. **Tijdelijke toegang**: Beperkte toegang tot bedrijfsmiddelen voor nieuwe medewerkers tot zij volledig zijn gescreend en goedgekeurd.		
Acties voor verbetering Door deze aanvullende acties voor verbetering te implementeren, kan GGDrU de effectiviteit van hun beheersmaatregelen verder verhogen en het risico op fraude en misbruik van bedrijfsmiddelen verder verkleinen: 1. **Periodieke herbeoordeling van VOG's**: Voer regelmatig herbeoordelingen uit van de VOG's van medewerkers die toegang hebben tot bedrijfsmiddelen, vooral na belangrijke wijzigingen in hun rol of na incidenten; 2. **Cultuur van integriteit**: Stimuleer een cultuur van integriteit en ethisch gedrag binnen de organisatie door regelmatig workshops of seminars te organiseren over de impact van fraude en de waarde van transparantie; 3. **Mentorprogramma's**: Implementeer mentorprogramma's waarbij ervaren medewerkers nieuwe medewerkers begeleiden, wat kan helpen bij het bevorderen van een verantwoordelijkheidsgevoel; 4. **Preventieve communicatie**: Zorg voor duidelijke communicatie over de verwachtingen met betrekking tot gedrag en ethiek, en de gevolgen van het overtreden van deze normen; 5. **Risicobeoordeling**: Voer regelmatig risicobeoordelingen uit met betrekking tot de aanwervingsprocedures en het beheer van bedrijfsmiddelen om nieuwe risico's te identificeren en aan te pakken; 6. **Benchmarking**: Vergelijk de screening- en wervingspraktijken met die van andere organisaties in de sector om best practices te identificeren en implementeren; 7. **Meldsysteem**: Ontwikkel een vertrouwelijk meldsysteem voor medewerkers om onregelmatigheden of ongepast gedrag te rapporteren zonder angst voor repercussies; 8. **Feedbacksessies**: Organiseer regelmatig feedbacksessies met medewerkers om hun ervaringen met het wervingsproces te bespreken en verbeterpunten te identificeren; 9. **Technologische ondersteuning**: Investeer in technologieën die de screening en monitoring van medewerkers kunnen ondersteunen, zoals software voor achtergrondcontroles en integriteitsbeoordelingen.							
• Inadequate administratie met betrekking tot bedrijfsmiddelen Dit betekent dat de documentatie, registratie en het beheer van bedrijfsmiddelen niet op een juiste of voldoende manier worden uitgevoerd.	Ja	• **Financiële verliezen**: Onjuiste of ontbrekende administratie kan leiden tot verkeerde financiële rapportages, wat kan resulteren in financiële verliezen of fouten in budgettering; • **Fraude en diefstal**: Een gebrek aan toezicht op de administratie kan medewerkers de mogelijkheid bieden om bedrijfsmiddelen toe te eigenen of misbruik te maken van middelen zonder ontdekking;	M 	H 	**Strikte Administratieve Procedures**: Duidelijke richtlijnen en procedures voor de administratie van bedrijfsmiddelen om fouten te minimaliseren en consistentie te waarborgen; **Regelmatig audits**: Periodieke interne audits om de nauwkeurigheid van de administratie te controleren en eventuele onregelmatigheden vroegtijdig op te sporen; **Opleiding en Training**: Trainingen voor medewerkers over het belang van goede	M tot L  	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		• **Verlies van bedrijfsmiddelen**: Niet goed bijgehouden bedrijfsmiddelen kunnen verloren gaan of beschadigd raken zonder dat dit op tijd wordt opgemerkt, wat leidt tot een verlies van waarde; • **Compliance risico's**: Inadequate documentatie kan ervoor zorgen dat GGDrU niet voldoet aan wet- en regelgeving, wat kan leiden tot juridische problemen en boetes; • **Slechte besluitvorming**: Onvolledige of onnauwkeurige gegevens kunnen leiden tot slechte strategische beslissingen met betrekking tot investeringen of de inzet van middelen; • **Onvoldoende ondersteuning van te leveren diensnten**: Gebrek aan inzicht in de beschikbare bedrijfsmiddelen kan GGDrU belemmeren in het effectief en efficiënt leveren van diensten aan cliënten, wat kan leiden tot inadequate zorgverlening en verspilling van middelen. Dit resulteert in vertragingen, beperkte innovatie en een negatieve impact op de tevredenheid van cliënten; • **Reputatieschade**: Onregelmatigheden of schandalen die voortkomen uit een slechte administratie kunnen schadelijk zijn voor de reputatie van de gemeenschappelijke regeling; • **Personeelsmoraal**: Medewerkers kunnen gefrustreerd			administratieve praktijken en de gevolgen van fouten of fraude; **Toegangscontrole**: Beperkte toegang tot administratieve systemen en bedrijfsmiddelen tot geautoriseerde medewerkers, en autorisatieprocedures voor belangrijke transacties**;** **Monitoring en rapportage**: Real-time monitoring van bedrijfsmiddelen en gebruik een systeem voor rapportage van onregelmatigheden of afwijkingen; **Gebruik van technologie**: Geavanceerde softwareoplossingen voor het beheer van bedrijfsmiddelen, inclusief automatische rapportages en meldingen bij onregelmatigheden; **Documentatie en archivering**: Gedetailleerde en georganiseerde documentatie van alle transacties en activiteiten met betrekking tot bedrijfsmiddelen om transparantie en traceerbaarheid te waarborgen; **Feedbackmechanismen**: Anonieme kanalen voor medewerkers om feedback te geven over administratieve processen en mogelijke onregelmatigheden te melden. **Compliance Beleid**: Voldoen aan alle relevante wet- en regelgeving door regelmatige compliance checks en training van medewerkers. **Incidentenmanagement**: Plan voor het omgaan met administratieve incidenten, inclusief duidelijke procedures voor het melden en oplossen van problemen.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		raken door een inefficiënte administratie, wat kan leiden tot een gebrek aan motivatie en betrokkenheid.					
Acties voor verbetering • **Strikte Administratieve Procedures**: Duidelijke richtlijnen en procedures helpen fouten te minimaliseren en consistentie in de administratie van bedrijfsmiddelen te waarborgen; • **Regelmatige audits**: Periodieke interne audits controleren de nauwkeurigheid van administratieve gegevens en stellen GGDrU in staat om onregelmatigheden tijdig te identificeren; • **Opleiding en training**: Trainingen over goede administratieve praktijken verhogen het bewustzijn van medewerkers over de risico's van fouten en fraude; • **Toegangscontrole**: Beperk de toegang tot administratieve systemen en bedrijfsmiddelen tot geautoriseerde medewerkers, en implementeer autorisatieprocedures voor belangrijke transacties; • **Monitoring en rapportage**: Real-time monitoring van bedrijfsmiddelen en een rapportagesysteem helpen bij het onmiddellijk detecteren van afwijkingen en onregelmatigheden; • **Gebruik van technologie**: Geavanceerde softwareoplossingen automatiseren het beheer van bedrijfsmiddelen en verbeteren de controle via automatische rapportages; • **Documentatie en archivering**: Gedetailleerde en georganiseerde documentatie van transacties waarborgt transparantie en traceerbaarheid van bedrijfsmiddelen; • **Feedbackmechanismen**: Anonieme feedbackkanalen moedigen medewerkers aan om onregelmatigheden te melden, wat een open cultuur bevordert; • **Compliance Beleid**: Regelmatige compliance checks en medewerkerstraining waarborgen de naleving van relevante wet- en regelgeving; • **Incidentenmanagement**: Een incidentenmanagementplan stelt GGDrU in staat om effectief te reageren op administratieve incidenten met duidelijke procedures voor rapportage en oplossing.							
• Inadequate registratie en autorisatie van gewerkte uren Verwijst naar een situatie waarbij de vastlegging van de tijd die medewerkers hebben gewerkt, niet zorgvuldig of nauwkeurig wordt gedaan.	Ja	• **Ongeoorloofd gebruik van uren**: Medewerkers kunnen geneigd zijn om meer uren te registreren dan daadwerkelijk gewerkt, of om uren te claimen voor niet-gewerkte dagen, wat leidt tot onterecht ontvangen betalingen. • **Fraude door samenspanning**: Als de registratie en autorisatie niet goed gecontroleerd worden, kan er een mogelijkheid ontstaan voor medewerkers om samen te werken om onterecht gewerkte uren goedgekeurd te krijgen; • **Beperkte transparantie**: Een gebrek aan goede registratie kan het moeilijk maken om een duidelijk	H ☹	M tot H 😐 ☹	**Strikte Registratieprocedures** • Duidelijke en gedetailleerde richtlijnen voor het registreren van gewerkte uren, inclusief de verplichting om een reden op te geven voor uitzonderlijke of overuren; **2. Toegangsbeheer** • Toegang tot het urenregistratiesysteem tot geautoriseerde medewerkers. Autorisatieprocedures voor het goedkeuren van gewerkte uren; **3. Regelmatige audits** • Periodieke interne audits van de urenregistratie om afwijkingen en onregelmatigheden op te sporen. Dit houdt in dat er steekproeven worden genomen van geregistreerde uren; **4. Training en voorlichting**	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		overzicht te krijgen van de gewerkte uren, wat leidt tot onvoldoende toezicht en daarmee verhoogde kansen op frauduleuze activiteiten; • **Verhoogde risico's bij audits**: Inadequate registratie kan tijdens audits tot moeilijkheden leiden, omdat onregelmatigheden moeilijk te traceren zijn, waardoor fraude moeilijker te identificeren is; • **Impact op budgettering en planning**: Onjuiste registratie van gewerkte uren kan ook leiden tot onjuiste financiële rapportages en planningsproblemen, wat het vertrouwen in de organisatie kan schaden.			• Trainingen aan medewerkers over de juiste procedures voor urenregistratie, de gevolgen van fraude en het belang van transparantie in de administratie; **5. Monitoring en rapportage** • Real-time monitoring van geregistreerde uren om verdachte patronen of afwijkingen tijdig te signaleren. Gebruik van rapportagetools voor een beter overzicht; **6. Feedback mechanismen** • Anonieme kanalen waar medewerkers eventuele onregelmatigheden of fraude kunnen melden zonder angst voor repercussies; **7. Beleid voor werktijden en overuren** • Duidelijk beleid op met betrekking tot werktijden, overuren en compensatie, en communiceer dit naar alle medewerkers; **8. Controle door twee personen** • Systeem waarbij belangrijke transacties of goedkeuringen (zoals urenregistratie) door twee verschillende personen moeten worden gecontroleerd en goedgekeurd; **9. Gebruik van technologie** • Software die automatische waarschuwingen en rapporten genereert bij onregelmatigheden in de urenregistratie. **10. Regelmatige evaluatie van procedures**		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					• Regelmati evaluatie van administratieve procedures en controles om ervoor te zorgen dat ze effectief blijven in het voorkomen van fraude.		

Acties voor verbetering
Deze acties kunnen helpen om de administratieve processen te optimaliseren, de kans op fraude te verkleinen en een cultuur van verantwoordelijkheid en transparantie binnen GGDrU te bevorderen:

- **Versterking van de cultuur van transparantie**: Creëer een open communicatieklimaat waarin medewerkers zich vrij voelen om zorgen te uiten over onregelmatigheden zonder angst voor repercussies;
- **Continue training**: Zorg voor regelmatige training en bijscholing van medewerkers over de procedures voor urenregistratie en de gevolgen van fraude, met nadruk op ethisch gedrag;
- **Integratie van geavanceerde technologie**: Implementeer moderne softwareoplossingen die automatische rapportages, waarschuwingen bij verdachte activiteiten en gebruiksvriendelijke interfaces bieden voor urenregistratie;
- **Regelmatig evaluatie van procedures**: Voer systematische evaluaties van de registratiesystemen en procedures uit om hun effectiviteit te waarborgen en verbeterpunten te identificeren;
- **Feedback mechanismen**: Implementeer anonieme feedbackkanalen en onderzoeken om continu inzicht te krijgen in mogelijke zwakheden in de huidige processen;
- **Versterking van toezicht**: Verhoog het aantal interne audits en steekproeven om de naleving van registratieprocedures te waarborgen en eventuele onregelmatigheden tijdig op te sporen;
- **Betere communicatie van beleid**: Zorg ervoor dat alle medewerkers goed op de hoogte zijn van het beleid met betrekking tot werktijden, overuren en de procedures voor urenregistratie;
- **Onafhankelijke toezicht**: Overweeg het inschakelen van externe auditors of consultants om een objectieve beoordeling van de administratieve processen en controles te geven;
- **Evaluatie van technologische innovaties**: Blijf op de hoogte van technologische ontwikkelingen en evalueer regelmatig of nieuwe tools of systemen de administratieve processen kunnen verbeteren;
- **Strategische planning en analyse**: Gebruik data-analyse om trends en patronen in urenregistratie te identificeren, wat kan helpen bij het verbeteren van de besluitvorming en planning.

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• Onvoldoende toezicht op afvalstromen;	Ja	• **Milieuvervuiling:** Slechte afvalverwerking kan leiden tot vervuiling van lucht, water en bodem; • **Regelgeving:** Overtredingen van wet- en regelgeving kunnen leiden tot boetes en juridische problemen; • **Financiële verliezen:** Onvoldoende controle kan leiden tot hogere kosten door inefficiënte afvalverwerking of herstelmaatregelen; • **Reputatieschade:** Negatieve publiciteit kan het vertrouwen van stakeholders schaden.	M 	H 	• **Toezicht door omgevingsdienst:** ○ De omgevingsdienst houdt toezicht op de afvalstromen en de verwerking ervan. Dit omvat regelmatige inspecties en controles om ervoor te zorgen dat alle meldingen voldoen aan de wet- en regelgeving; ○ Er wordt een rapportagesysteem gebruikt om de naleving en eventuele afwijkingen bij te houden, zodat tijdig actie kan worden ondernomen; • **Strikte inzamelingsprocedures:** ○ Medische afvalstoffen worden ingezameld en vervoerd volgens strikte bepalingen die voldoen aan de geldende milieu- en gezondheidsnormen; ○ GGDrU schakelt gespecialiseerde afvalverwerkingsbedrijven in die gecertificeerd zijn voor de verwerking van medische en gevaarlijke afvalstoffen; ○ Trainingen voor personeel over de juiste procedures voor afvalinzameling en -verwerking worden regelmatig georganiseerd	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					om bewustzijn en naleving te waarborgen; • **Documentatie en Rapportage:** ○ Alle afvalstromen worden gedocumenteerd en er worden rapporten opgesteld over de hoeveelheid en het type afval dat wordt ingezameld en verwerkt; ○ Deze documentatie helpt bij het monitoren van de efficiëntie van het afvalbeheer en zorgt voor transparantie richting stakeholders; • **Risicobeoordeling:** ○ Regelmatige risicobeoordelingen om potentiële risico's in verband met afvalstromen te identificeren en passende maatregelen te nemen; ○ Dit omvat het beoordelen van de samenwerking met afvalverwerkingsbedrijven en het actualiseren van procedures indien nodig.		

Acties voor verbetering

Door deze acties te implementeren, kan GGDrU de effectiviteit van het toezicht op afvalstromen verder verbeteren:

1. **Versterking van training en voorlichting:** Regelmatige trainingen voor medewerkers over de juiste procedures voor afvalverwerking en -inzameling kunnen het bewustzijn en de naleving verbeteren;
2. **Verbeterde documentatie:** Het implementeren van een gestandaardiseerd systeem voor het bijhouden van afvalstromen kan de traceerbaarheid en controle vergemakkelijken;
3. **Uitbreiding van controlemaatregelen:** Het vergroten van het aantal controles door de omgevingsdienst en het uitvoeren van onregelmatige audits kan helpen om naleving van de regels te waarborgen;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
4. **Feedbackmechanismen:** Het instellen van een systeem voor feedback van medewerkers over afvalverwerkingsprocessen kan waardevolle inzichten opleveren en bijdragen aan continue verbetering; 5. **Samenwerking met externe experts:** Regelmatig overleg met externe afvalverwerkingsbedrijven kan zorgen voor actuele kennis over beste praktijken en nieuwe regelgeving.							
• Onvoldoende controle op het gebruik van ruimtes en apparatuur;	Ja	Bij onvoldoende controle op het gebruik van ruimtes en apparatuur kunnen medewerkers ongeoorloofd toegang krijgen tot waardevolle middelen, wat leidt tot gelegenheidsfraude en het onrechtmatig toe-eigenen van bedrijfsmiddelen. Dit vergroot het risico op diefstal, misbruik en verlies van belangrijke informatie of apparatuur.	M 	H 	1. **Toegangsbeheer**: Beperke toegang tot gevoelige ruimtes en apparatuur tot bevoegde medewerkers om ongeoorloofd gebruik te voorkomen; 2. **Registratiesysteem**: Registratiesysteem voor het gebruik van ruimtes en apparatuur, zodat het gebruik kan worden gemonitord en geëvalueerd; 3. **Regelmatige audits**: Periodieke controles en audits om te waarborgen dat ruimtes en apparatuur correct worden gebruikt en dat eventuele afwijkingen tijdig worden opgespoord; 4. **Training en bewustwording**: Trainingen voor medewerkers over het juiste gebruik van ruimtes en apparatuur en het belang van naleving van de richtlijnen; 5. **Procedures en richtlijnen**: Duidelijke procedures en richtlijnen voor het gebruik van ruimtes en apparatuur, inclusief meldingssystemen voor onregelmatigheden of misbruik.	M 	Ja
Acties voor verbetering Deze acties kunnen helpen om de controle te verbeteren en het restrisico op fraude en toeeigening van bedrijfsmiddelen te verminderen: 1. **Toegangsbeheer**: Beperk de toegang tot gevoelige ruimtes en apparatuur tot bevoegde medewerkers om ongeoorloofd gebruik te voorkomen. 2. **Registratiesysteem**: Implementeer een registratiesysteem voor het gebruik van ruimtes en apparatuur, zodat het gebruik kan worden gemonitord en geëvalueerd; 3. **Regelmatige audits**: Voer periodieke controles en audits uit om te waarborgen dat ruimtes en apparatuur correct worden gebruikt en dat eventuele afwijkingen tijdig worden opgespoord;							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
4. **Training en bewustwording**: Bied trainingen aan medewerkers over het juiste gebruik van ruimtes en apparatuur en het belang van naleving van de richtlijnen; 5. **Procedures en richtlijnen**: Ontwikkel duidelijke procedures en richtlijnen voor het gebruik van ruimtes en apparatuur, inclusief meldingssystemen voor onregelmatigheden of misbruik.							
• De fysieke bewaking van dure geneesmiddelen en opiaten binnen GGDrU is onvoldoende; Dit houdt in dat er geen adequate maatregelen zijn om deze waardevolle en gevoelige producten te beschermen tegen diefstal of ongeoorloofd gebruik. GDrU richt zich met name op de verstrekking van vaccinaties en andere preventieve geneesmiddelen als onderdeel van haar preventieprogramma's. Daarnaast biedt de organisatie ondersteuning en behandeling aan patiënten met infectieziekten en verslavingsproblemen, en monitort zij het gebruik van geneesmiddelen binnen de bevolking voor gezondheidsstatistieken en rapportages.	Ja	1. **Diefstal of misbruik**: Onvoldoende toezicht kan de kans op diefstal van dure geneesmiddelen en opiaten vergroten, wat leidt tot financieel verlies en risico's voor cliënten; 2. **Ongeoorloofde toegang**: Onbevoegden kunnen toegang krijgen tot opiaten en dure geneesmiddelen, met het risico op ongepast gebruik of misbruik, wat schade kan toebrengen aan zowel individuen als de bredere gemeenschap; 3. **Verlies van vertrouwen**: Een gebrek aan adequate beveiliging kan het vertrouwen van de gemeenschap in GGDrU ondermijnen, vooral als het gaat om verslavingsbehandeling en de veiligheid van preventieve geneesmiddelen, zoals vaccins; 4. **Impact op vaccinatieprogramma's**: Inadequate controle kan de effectiviteit van vaccinatieprogramma's aantasten, waardoor er een risico bestaat dat patiënten niet tijdig of niet correct gevaccineerd worden, wat	M 	H 	1. **Versterking van toezicht:** Strikte controles en toezichtsystemen om diefstal van geneesmiddelen en opiaten te voorkomen en financiële verliezen te minimaliseren; 2. **Toegangscontrole:** Rolgebaseerde toegang en fysieke beveiliging van opslagruimten voor opiaten en geneesmiddelen om ongeoorloofde toegang en misbruik te voorkomen; 3. **Communicatie en transparantie:** Communicatie over de veiligheid van geneesmiddelen en verslavingsbehandeling om het vertrouwen te behouden; 4. **Monitoring van vaccinaties:** Protocollen voor de controle en monitoring van vaccinatieprogramma's om te waarborgen dat cliënten tijdig en correct worden gevaccineerd. 5. **Naleving van regelgeving:** Compliance met wettelijke vereisten voor de opslag en bewaking van geneesmiddelen om juridische gevolgen te voorkomen; 6. **Evaluatie van behandelprogramma's:** Regelmatig evaluaties van behandelprogramma's voor verslavingsproblematiek om hun effectiviteit te waarborgen en aanpassingen te doen waar nodig.	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		hun gezondheid in gevaar kan brengen; 5. **Regelgeving en sancties**: Het niet naleven van wettelijke vereisten voor de opslag en bewaking van geneesmiddelen kan leiden tot juridische gevolgen voor GGDrU; 6. **Effect op behandelprogramma's**: Een slechte controle kan de effectiviteit van behandelingsprogramma's voor verslavingsproblematiek ondermijnen, wat negatieve gevolgen heeft voor de volksgezondheid.					
Acties voor verbetering Om de veiligheid van dure geneesmiddelen en opiaten te waarborgen, moeten fysieke beveiliging en toegangscontrole naar een hoger niveau worden getild. Dit omvat het versterken van cameratoezicht, het implementeren van striktere toegangseisen, en het bieden van trainingen aan personeel over het veilig omgaan met deze middelen. Regelmatige audits en monitoring van de voorraad zijn essentieel om onregelmatigheden tijdig te signaleren.							
• Inadequate fysieke beveiliging van medische apparatuur en hulpmiddelen Onvoldoende fysieke beveiliging van medische apparatuur en hulpmiddelen verhoogt het risico op diefstal, misbruik en beschadiging. Dit kan leiden tot financiële verliezen voor GGDrU en mogelijk ook de kwaliteit van zorg aantasten, omdat essentiële hulpmiddelen niet beschikbaar zijn wanneer dat nodig is.	Ja	1. **Diefstal en misbruik:** Onvoldoende beveiliging kan leiden tot diefstal van waardevolle medische apparatuur en hulpmiddelen, resulterend in financiële verliezen en verstoring van zorgprocessen; 2. **Verlies van essentiële hulpmiddelen:** Onbevoegd gebruik of beschadiging kan de beschikbaarheid van medische hulpmiddelen beïnvloeden, wat kan leiden tot vertraging in zorgverlening;	H ☹	H ☹	1. **Toegangscontrole:** Strikte toegangscontroles tot ruimtes waar medische apparatuur en hulpmiddelen zijn opgeslagen, zodat alleen bevoegde medewerkers toegang hebben; 2. **Fysieke beveiliging:** Beveiligingssystemen, zoals camera's en alarmsystemen, om ongeoorloofde toegang of diefstal te voorkomen; 3. **Inventarisatie:** Regelmatig inventarisatie van medische apparatuur en hulpmiddelen om te	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		3. **Verminderde zorgkwaliteit:** Gebrek aan adequate beveiliging kan het vertrouwen van cliënten in de zorgverlening van GGDrU ondermijnen; 4. **Juridische en financiële consequenties:** Niet-naleving van regelgeving rondom de beveiliging van medische apparatuur kan leiden tot juridische problemen en mogelijke sancties.			controleren op ontbrekende items en om te zorgen dat alle apparatuur correct is geregistreerd; 4. **Opleiding van personeel:** Training aan medewerkers over het belang van de beveiliging van medische apparatuur en de procedures voor het veilig opslaan en gebruiken ervan; 5. **Beveiligingsprocedures:** Duidelijke procedures op voor het omgaan met en rapporteren van onregelmatigheden of verdachte activiteiten met betrekking tot medische apparatuur; 6. **Monitoring en audits:** Regelmatig audits om de effectiviteit van de beveiligingsmaatregelen te evalueren en aan te passen waar nodig.		

Acties voor verbeteringen

Door deze acties te implementeren, kan GGDrU de kans op incidenten verlagen en de algehele beveiliging van medische apparatuur en hulpmiddelen verbeteren:

1. **Regelmatig trainingen:** Organiseer trainingen voor personeel over het belang van beveiliging van medische apparatuur en hulpmiddelen, inclusief procedures voor het melden van verdachte activiteiten;
2. **Versterken van toezicht:** Verhoog de frequentie en de grondigheid van toezicht op de opslag en het gebruik van medische apparatuur om eventuele afwijkingen vroegtijdig te signaleren;
3. **Implementatie van technologie:** Maak gebruik van moderne technologieën zoals camerabewaking en alarmsystemen om ongeoorloofde toegang tot belangrijke ruimtes te monitoren;
4. **Toegangscontrole:** Implementeer strikte toegangscontroles tot ruimtes waar medische apparatuur en hulpmiddelen zijn opgeslagen, bijvoorbeeld door gebruik te maken van toegangspassen of biometrische identificatie;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
5. **Regelmatig audits:** Voer periodieke audits uit van de beveiligingsmaatregelen en het gebruik van medische apparatuur om naleving van de procedures te waarborgen. 6. **Verbeteren van Documentatie:** Zorg voor duidelijke documentatie en registratie van het gebruik, de locatie en de status van medische apparatuur, om eventuele verloren of beschadigde items te traceren; 7. **Feedbackmechanismen:** Implementeer mechanismen waarbij personeel incidenten of zorgen kan melden zonder angst voor repercussies, zodat verbeterpunten in de beveiliging kunnen worden vastgesteld; 8. **Beleid en Procedures Herzien:** Evalueer en actualiseer regelmatig het beveiligingsbeleid en de procedures met betrekking tot medische apparatuur om deze af te stemmen op de nieuwste normen en technologieën.							
• Inadequate monitoring van fysieke en digitale gegevens, waardoor er mogelijkheden voor fraude kunnen ontstaan; Onvoldoende bewaking van zowel fysieke als digitale gegevens vergroot de kans op fraude doordat kwetsbaarheden niet tijdig worden opgemerkt. Dit kan leiden tot ongeoorloofde toegang tot gevoelige informatie, manipulatie van gegevens of misbruik van middelen, waardoor de integriteit van de organisatie in gevaar komt. Effectieve controles zijn essentieel om deze risico's te minimaliseren.	Ja	1. **Datalekken:** Onvoldoende beveiliging van persoonlijke en medische gegevens kan leiden tot datalekken, waardoor vertrouwelijke informatie van burgers en patiënten openbaar wordt; 2. **Fraude met medische gegevens:** Gebrek aan controle kan leiden tot manipulatie van medische gegevens, bijvoorbeeld voor onterecht verkrijgen van vergoedingen of diensten; 3. **Ongeoorloofde toegang:** Het niet effectief monitoren van fysieke locaties en digitale systemen kan resulteren in ongeautoriseerde toegang tot vertrouwelijke gegevens en faciliteiten; 4. **Verlies van vertrouwelijkheid:** Onvoldoende bescherming van gegevens kan het vertrouwen van inwoners in GGDrU schaden, met gevolgen voor de samenwerking en informatieverstrekking;	H tot M 	M tot H 	1. **Informatiebeveiligingsbeleid:** Ontwikkeling en implementatie van een uitgebreid beleid waarin de verantwoordelijkheden van de ISO (Informatiebeveiligings-functionaris), PO (Privacy Officer) en FG (Functionaris Gegevensbescherming) worden vastgelegd, inclusief procedures voor databeveiliging en privacybescherming; 2. **Toegangscontrole:** Rolgebaseerde toegangscontroles voor zowel fysieke als digitale gegevens, zodat alleen bevoegde medewerkers toegang hebben tot gevoelige informatie; 3. **Training en bewustwording:** Regelmatig trainingen voor medewerkers over gegevensbeveiliging en privacy, met nadruk op de rol van de FG en PO in het waarborgen van de privacy van gegevens; 4. **Monitoring en audit:** Regelmatige audits van systemen en processen om de naleving van de Algemene Verordening Gegevensbescherming (AVG) te waarborgen en eventuele tekortkomingen in de	M tot H 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		5. **Nalevingsrisico's:** Niet voldoen aan wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), kan leiden tot juridische sancties en reputatieschade; 6. **Operationele verstoringen:** Inadequate bescherming kan leiden tot storingen in de dienstverlening, zoals het niet kunnen verwerken van vaccinatiegegevens of andere cruciale informatie; 7. **Impact op gezondheidsmonitoring:** Onvoldoende gegevensbewaking kan invloed hebben op de effectiviteit van gezondheidsmonitoring en -interventies, wat kan leiden tot onjuiste conclusies of aanbevelingen.			gegevensbescherming te identificeren; 5. **Incidentbeheer:** Procedures voor het melden en reageren op datalekken of beveiligingsincidenten, waarbij de rollen van de ISO, PO en FG duidelijk zijn gedefinieerd; 6. **Documentatie en registratie:** Gedetailleerde documentatie van gegevensverwerkingen en incidenten, wat essentieel is voor compliance met de AVG en helpt bij audits; 7. **Risicobeheer:** Risicoanalyse om potentiële bedreigingen voor gegevensbeveiliging in kaart te brengen en ontwikkel maatregelen om deze risico's te mitigeren.		

Acties voor verbetering

Door deze acties te implementeren, kan GGDrU de kans op risico's verder verminderen en de impact van eventuele incidenten beperken:

1. **Regelmatige trainingen en bewustwording:**
   - Voer frequent trainingen uit voor medewerkers over gegevensbeveiliging, AVG-compliance en fraudepreventie. Dit helpt medewerkers bewust te maken van de risico's en hen te leren hoe ze veilig moeten omgaan met fysieke en digitale gegevens;
2. **Versterking van toegangscontroles:**
   - Implementeer strengere rolgebaseerde toegangscontroles en multi-factor authenticatie voor gevoelige systemen en gegevens om ongeoorloofde toegang te voorkomen;
3. **Audits en monitoring:**
   - Voer regelmatig interne en externe audits uit om de effectiviteit van de beheersmaatregelen te beoordelen. Implementeer continue monitoring van systemen en transacties om afwijkingen of verdachte activiteiten tijdig te detecteren;
4. **Documentatie en registratie:**

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ Zorg voor een gedetailleerde documentatie van alle processen met betrekking tot de registratie van fysieke en digitale gegevens, inclusief afspraken met functionarissen zoals de Informatiebeveiligingsfunctionaris (ISO) en de Functionaris Gegevensbescherming (FG); 5. **Verbeterde incidentresponsprocedures:** ○ Ontwikkel en test procedures voor incidentrespons die gericht zijn op het snel reageren op datalekken of andere beveiligingsincidenten om de impact te minimaliseren; 6. **Evaluatie van beheersmaatregelen:** ○ Evalueer regelmatig de effectiviteit van bestaande beheersmaatregelen en pas deze aan op basis van nieuwe risico's, technologieën of veranderingen in de organisatie; 7. **Samenwerking met externe experts:** ○ Overweeg samen te werken met externe beveiligingsspecialisten om advies te krijgen over best practices en om eventuele kwetsbaarheden in de systemen te identificeren.							
• Inadequate administratie en registratie van ICT- en telefonieapparatuur;	Ja	• **Verlies van apparatuur**: Onvoldoende registratie kan leiden tot het verlies of de diefstal van apparatuur, zonder dat dit wordt opgemerkt of geregistreerd. Dit kan leiden tot het gebruik van verloren apparatuur voor frauduleuze activiteiten; • **Onrechtmatige toegang**: Zonder duidelijke administratie is het moeilijk te bepalen wie toegang heeft tot bepaalde apparaten, waardoor onbevoegden toegang kunnen krijgen tot gevoelige informatie of systemen; • **Verkeerde inventarisatie**: Een inadequate administratie kan resulteren in onjuiste gegevens over de aanwezige apparatuur, wat kan leiden tot het bestellen van onnodige apparatuur of het niet opmerken van verdwenen of defecte apparatuur; • **Fraude met apparatuur**: Medewerkers kunnen mogelijk apparatuur verduisteren of vervalsen door gebruik te maken	M 😐	M tot H 😐☹	• **Centraal Registratiesysteem**: ○ Centraal systeem voor de registratie van alle ICT- en telefonieapparatuur. Dit systeem moet toegankelijk zijn voor alle relevante afdelingen en regelmatig worden bijgewerkt; • **Regelmatige Inventarisaties**: ○ Periodieke inventarisaties van alle apparatuur om ervoor te zorgen dat de geregistreerde gegevens overeenkomen met de fysieke apparatuur. Dit helpt om verloren of niet-geregistreerde apparatuur te identificeren; • **Duidelijke Verantwoordelijkheden**: ○ Specifieke medewerkers of teams zijn verantwoordelijk voor het beheer van ICT- en telefonieapparatuur. Duidelijke verantwoordelijkheden zijn gedefinieerd in functieomschrijvingen; • **Trainingsprogramma's**: ○ Trainingen voor medewerkers over het belang van correcte administratie en registratie van apparatuur, inclusief richtlijnen over hoe apparatuur correct moet	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		van gebrekkige registratie, wat leidt tot financiële verliezen; • **Beperkingen bij audits**: Een slechte registratie bemoeilijkt interne en externe audits, waardoor het moeilijk is om de integriteit van de administratie te waarborgen en risico's op fraude te identificeren**;** • **Compliance-risico's**: Onvoldoende administratie kan leiden tot niet-naleving van wet- en regelgeving met betrekking tot de registratie van bedrijfsmiddelen, wat kan resulteren in juridische gevolgen en boetes; • **Financiële verlies**: Het gebrek aan controle kan leiden tot financiële verliezen door niet-geautoriseerde of ongeregistreerde aankopen van apparatuur.			worden geregistreerd en onderhouden; • **Procedures voor aanschaf en afvoer**: ○ Duidelijke procedures voor de aanschaf, registratie en afvoer van apparatuur. Dit omvat het registreren van nieuwe apparatuur bij aanschaf en het documenteren van de afvoer van oude apparatuur; • **Monitoring en rapportage**: ○ Monitoring- en rapportagesysteem om afwijkingen in de registratie te identificeren en aan te pakken. Dit kan helpen bij het tijdig signaleren van onregelmatigheden; • **Integratie met Financiële Systemen**: ○ Het registratiesysteem voor apparatuur is geïntegreerd met het financiële systeem van GGDrU, zodat kosten en investeringen in apparatuur gemakkelijk kunnen worden bijgehouden en gecontroleerd; • **Audits en evaluaties**: ○ Regelmatig interne audits om de effectiviteit van de administratie- en registratieprocessen te evalueren. Deze audits worden gebruikt om verbeterpunten te identificeren en te implementeren.		

Acties voor verbetering
Door deze acties te implementeren, kan GGDrU het restrisico van inadequate administratie en registratie van ICT- en telefonieapparatuur verder minimaliseren en de algehele financiële en operationele integriteit verbeteren:

1. **Regelmatige inventarisatie**:
   - Voer regelmatig een volledige inventarisatie uit van alle ICT- en telefonieapparatuur om ervoor te zorgen dat alle items correct zijn geregistreerd en gedocumenteerd;
2. **Standaardisatie van procedures**:

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ Ontwikkel en implementeer gestandaardiseerde procedures voor de registratie en administratie van apparatuur, inclusief duidelijke richtlijnen voor in- en uitschrijvingen; 3. **Training en bewustwording**: ○ Bied trainingen aan voor medewerkers over het belang van correcte registratie en administratie van apparatuur. Zorg ervoor dat zij op de hoogte zijn van de procedures en verantwoordelijkheden; 4. **Digitale registratiesystemen**: ○ Implementeer geautomatiseerde systemen voor het registreren van ICT- en telefonieapparatuur, die real-time updates en meldingen mogelijk maken om onregelmatigheden snel te detecteren; 5. **Toezicht en controle**: ○ Stel regelmatig toezicht en controles in, zoals interne audits en reviews van de administratie, om ervoor te zorgen dat de procedures worden nageleefd; 6. **Verantwoordelijkheden duidelijk definiëren**: ○ Wijs specifieke verantwoordelijkheden toe aan teamleden voor het beheren van de administratie en registratie van apparatuur, zodat er een duidelijk aanspreekpunt is; 7. **Incidentenregistratie**: ○ Implementeer een systeem voor het registreren van incidenten met betrekking tot apparatuur (zoals verlies of schade) en evalueer deze regelmatig om verbeteringen door te voeren; 8. **Compliance monitoring**: ○ Houd toezicht op naleving van wet- en regelgeving omtrent apparatuurbeheer en pas processen aan indien nodig om te voldoen aan nieuwe eisen; 9. **Feedbackmechanismen**: ○ Creëer mogelijkheden voor medewerkers om feedback te geven over de administratieprocessen, zodat onregelmatigheden kunnen worden gemeld en aangepakt; 10. **Evaluatie en aanpassing van beheersmaatregelen**: ○ Evalueer regelmatig de effectiviteit van de huidige beheersmaatregelen en pas deze aan op basis van nieuwe risico's of veranderingen in de organisatie.							
• Inadequate interne beheersingsmaatregelen voor contante opbrengsten; Hoewel inadequate interne beheersingsmaatregelen met betrekking tot de volledige verantwoording van contante opbrengsten in andere organisaties problematisch kunnen zijn, is dit voor GGDrU minder relevant. De organisatie heeft contante opbrengsten geminimaliseerd door processen volledig digitaal te maken. Dit betekent dat de financiële transacties van	Ja, er zijn potentiële risico's verbonden aan onvoldoende interne beheersingsmaatregelen bij digitale opbrengsten.	Potentiële risico's verbonden aan interne beheersingsmaatregelen met betrekking tot **contante opbrengsten** omvatten de mogelijkheid van fraude en misbruik, waarbij medewerkers contante transacties kunnen manipuleren of vervalsen. Daarnaast is er een verhoogd risico op fouten door menselijke interactie bij de verwerking van contante betalingen, wat kan leiden tot onjuiste boekingen. Ook ontbreekt vaak een adequate controle en monitoring van contante stromen, waardoor afwijkingen niet tijdig worden opgemerkt. Dit kan resulteren in financiële verliezen en reputatieschade voor de organisatie.	M 	H 	**Rolgebaseerde toegang**: Alleen bevoegde medewerkers hebben toegang tot digitale betalingssystemen; **Accountbeheer**: Accounthouders stellen doelen, verwachtingen en financiële verantwoordelijkheden vast in samenwerking met gemeentes; **Duidelijke procedures en richtlijnen**: • **Documentatie**: Richtlijnen voor verwerking van digitale opbrengsten, inclusief goedkeurings- en registratieprocedures; • **Betalingsvoorwaarden**: Duidelijke communicatie van betalingsvoorwaarden voor	L 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
bijvoorbeeld Reisvaccinaties, worden beheerd via een efficiënt digitaal systeem, waardoor het risico op fouten en fraude aanzienlijk is verminderd. Hierdoor zijn de verantwoording en controle van opbrengsten transparanter en beter traceerbaar. **Digitale opbrengsten**: In tegenstelling tot contante opbrengsten, verwijzen digitale opbrengsten naar inkomsten die zijn gegenereerd via digitale betalingssystemen, zoals bankoverschrijvingen, pinbetalingen en online betalingsplatforms. Deze methoden bieden een efficiënter en veiliger betalingsproces, wat de transparantie en traceerbaarheid van financiële transacties bevordert. Door te kiezen voor digitale opbrengsten wordt het risico op fouten en fraude, die vaak gepaard gaan met contante transacties, aanzienlijk verminderd. Dit versterkt niet alleen de financiële integriteit van de organisatie, maar zorgt ook voor een betrouwbaarder en geordend financieel beheer;		In het kader van de relevantie zal daarom hier de focus liggen op **digitale opbrengsten**. Potentiële risico's verbonden aan interne beheersingsmaatregelen met betrekking tot digitale opbrengsten zijn: 1. **Fraude en misbruik**: Zonder sterke controles kunnen medewerkers of externe partijen frauduleuze handelingen uitvoeren, zoals het manipuleren van betalingsgegevens of het creëren van valse transacties, wat kan leiden tot aanzienlijke financiële verliezen voor de organisatie; 2. **Technologische risico's**: Digitale betalingssystemen zijn kwetsbaar voor cyberaanvallen, waaronder phishing en ransomware. Onvoldoende beveiliging kan resulteren in datalekken of ongeoorloofde toegang tot gevoelige financiële informatie, waardoor de organisatie in een kwetsbare positie komt te verkeren; 3. **Fouten bij verwerking**: Gebrek aan adequate controles kan leiden tot menselijke fouten tijdens het invoeren of verwerken van digitale betalingen, wat resulteert in verkeerde boekingen en financiële inconsistenties; 4. **Onvoldoende monitoring**: Zonder regelmatige controles en audits kan het management			transparantie en minder geschillen; **Monitoring en audit**: • **Interne audits**: Regelmatig audits om de effectiviteit van controlemechanismen te beoordelen; • **Opbrengsten**: nauwkeurige registratie door de opbrengsten continu te monitoren; **Training en Bewustwording**: • **Opleidingsprogramma's**: Training voor medewerkers over fraudepreventie en interne controles; • **Bewustwordingscampagnes**: Medewerkers informeren over fraudegevaren bij digitale opbrengsten. **Fraudepreventiesystemen**: • **Automatische signalering**: Detecteren transacties, zoals ongebruikelijke bedragen. • **Controle opbrengsten**: Overeenkomsten en facturen controleren om fouten te voorkomen en leveringen correct te verifiëren; **Verificatieprocessen**: • **Authenticatie**: Gebruik rolbeheer om documenten te verifiëren. • **Twee-Factor Authenticatie (2FA)**: 2FA voor belangrijke systemen ter beveiliging; **Evaluatie en aanpassing**: • **Feedback**: Medewerkers hebben de mogelijkheid om feedback te geven;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		belangrijke afwijkingen in digitale opbrengsten niet opmerken, waardoor potentiële problemen onopgemerkt blijven en de organisatie in een risicovolle situatie terechtkomt; 5. **Compliance Risico's**: Inadequate interne beheersingen kunnen leiden tot niet-naleving van wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) en andere financiële regelgeving. Dit kan resulteren in boetes en juridische complicaties; 6. **Reputatieschade**: Het vaststellen van tekortkomingen in de interne beheersingsmaatregelen kan leiden tot reputatieschade. Stakeholders, zoals gemeenten, kunnen hun vertrouwen in de organisatie verliezen, wat op lange termijn schadelijk kan zijn voor de bedrijfsvoering; 7. **Verlies van controle**: Bij onvoldoende interne controles kan de organisatie het overzicht verliezen over haar digitale opbrengsten, wat kan leiden tot onterecht uitgevoerde betalingen en een gebrek aan inzicht in de algehele financiële situatie.			• **Continu verbeteren**: Regelmatig evaluatie en verbetering van interne controles op basis van nieuwe risico's.		
Acties voor verbetering Om inadequate interne beheersingsmaatregelen voor digitale opbrengsten verder te minimaliseren, kunnen de volgende verbeteracties worden overwogen: 1. **Automatisering van controles**: Gebruik geautomatiseerde systemen om afwijkingen en fouten in digitale transacties sneller te detecteren; 2. **Verhoogde toezicht**: Voer meer frequente en gerichte audits uit om mogelijke zwakke punten vroegtijdig te identificeren; 3. **Strengere toegangscontroles**: Implementeer multi-factor authenticatie (zoals een wachtwoord én een code via een mobiele app) voor alle gevoelige systemen en processen; 4. **Continue training**: Geef regelmatig trainingen over nieuwe fraude- en cyberdreigingen;							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
5. **Realtime monitoring**: Zet realtime monitoring op van digitale transacties om verdachte activiteiten direct op te merken en in te grijpen.							
• Inadequaat systeem voor autorisatie en goedkeuring van transacties, met name binnen de inkoopprocessen; Dit betekent dat er mogelijk gebreken zijn in de controlemechanismen die ervoor zorgen dat aankopen en uitgaven de juiste goedkeuring ontvangen. Zonder een degelijk autorisatiesysteem kunnen ongeoorloofde of onjuiste transacties plaatsvinden, wat kan leiden tot financiële verliezen of inefficiënt gebruik van middelen. Het is essentieel om duidelijke goedkeuringsprocedures en verantwoordelijkheden vast te stellen om de integriteit van de financiële processen te waarborgen.	Ja	• **Fraude en ongeoorloofde betalingen**: Zonder adequaat goedkeuringssystemen kunnen frauduleuze of ongeoorloofde betalingen aan leveranciers plaatsvinden, wat leidt tot financiële verliezen; • **Betaling aan valse crediteuren**: Inadequate controle over inkoopfacturen kan resulteren in betalingen aan niet-bestaande of ongewenste crediteuren, wat leidt tot aanzienlijke financiële schade en reputatieverlies; • **Verlies van controle over budgetten**: Onvoldoende autorisatie kan resulteren in onterecht gemaakte uitgaven die niet zijn opgenomen in de goedgekeurde begroting, waardoor financiële planning en controle in gevaar komen; • **Vertraging in prestatielevering**: De levering van goederen en diensten vindt doorgaans plaats voordat de factuur wordt ontvangen. Bij ontvangst van de factuur is het essentieel om te verifiëren dat de geleverde prestatie daadwerkelijk heeft plaatsgevonden; • **Juridische en contractuele risico's**: Als betalingen worden gedaan zonder de juiste goedkeuring, kan GGDrU in een zwakkere positie komen te staan en zich mogelijk niet meer	M 	H 	**1. Fraude en ongeoorloofde betalingen** • **Implementatie van een robust goedkeuringsproces:** Duidelijk autorisatieprocedures, waarbij meerdere goedkeuringen vereist zijn voor betalingen; • **Tweefactorauthenticatie:** Tweefactorauthenticatie voor toegang tot financiële systemen en goedkeuringsprocessen. **2. Betaling aan valse crediteuren** • **Verificatie van crediteuren:** Grondige controles voordat nieuwe crediteuren worden toegevoegd, inclusief het verifiëren van hun identiteit en bedrijfsinformatie; • **Regelmatige audits van crediteurenlijst:** Periodieke audits om te controleren op ongebruikelijke of verdachte crediteuren; **3. Verlies van controle over budgetten** • **Budgettering en monitoring:** Strikte budgetteringsprocedures en monitor uitgaven regelmatig om afwijkingen te identificeren; • **Training van medewerkers:** Training voor management over budgetbeheer en de gevolgen van niet-naleving; **4. Vertraging in prestatielevering** • **Snelle factuurverwerking:** Zorg voor een efficiënt proces voor het goedkeuren van facturen zodat er geen vertragingen ontstaan;	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		beroepen op contractuele verplichtingen. Hier is een verbeterde formulering; • **Reputatieschade**: Het niet kunnen waarborgen van een adequaat autorisatiesysteem kan leiden tot reputatieschade bij stakeholders, waaronder medewerkers, leveranciers en inwoners, wat het vertrouwen in de organisatie ondermijnt; • **Compliance risico's**: Een gebrek aan goedkeuringsprocessen kan leiden tot niet-naleving van interne controlemaatregelen en wet- en regelgeving, wat kan resulteren in audits, sancties of andere juridische complicaties; • **Inaccurate rapportage**: Onvoldoende controle over goedkeuringen kan leiden tot fouten in financiële rapportages, wat de besluitvorming op strategisch niveau kan beïnvloeden en het vertrouwen van het management kan schaden.			• **Leverancierscommunicatie:** Houd regelmatig contact met leveranciers om de status van leveringen en bijbehorende facturen te volgen; **5. Juridische en contractuele risico's** • **Duidelijke contractuele afspraken:** Duidelijke en gedocumenteerde contracten met leveranciers om juridische geschillen te minimaliseren; • **Juridische controle:** Betalingen en contracten worden regelmatig gecontroleerd door de juridische afdeling; **6. Reputatieschade** • **Transparante communicatie:** Communicatie met stakeholders over de maatregelen die zijn genomen om risico's te beheersen; • **Cultuur van integriteit:** Stimuleren van een organisatiecultuur die ethisch gedrag en verantwoordelijkheidsbesef bevordert; **7. Compliance risico's** • **Regelmatige compliance audits:** Periodieke audits om te controleren of de organisatie voldoet aan interne controles en wet- en regelgeving; • **Documentatie en rapportage:** Goede documentatie van alle processen en procedures om de compliance te ondersteunen; **8. Inaccurate rapportage**		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					• **Automatisering van rapportageprocessen:** Gebruik van technologie om rapportages te automatiseren en te standaardiseren voor nauwkeurigheid; • **Training voor financiële medewerkers:** Trainingen over nauwkeurige rapportage en de juiste verwerking van financiële gegevens.		

Acties voor verbetering
Door deze aanvullende acties te implementeren, kan GGDrU niet alleen de kans op frauduleuze activiteiten en ongeoorloofde betalingen verkleinen, maar ook de impact van eventuele incidenten beperken en het vertrouwen van stakeholders vergroten:

- **Verbetering van goedkeuringsprocessen**
  - **Automatisering van goedkeuring:** Optimaliseer het digitale goedkeuringsproces binnen AFAS door workflows te standaardiseren, automatische meldingen in te voeren en real-time tracking mogelijk te maken. Dit bevordert transparantie, minimaliseert fouten en stelt GGDrU in staat om feedback te verzamelen voor voortdurende evaluatie en aanpassing van het proces aan de behoeften van de organisatie;
  - **Duidelijke goedkeuringshiërarchie:** Implementeer een heldere hiërarchie voor goedkeuringen, zodat verantwoordelijken op elk niveau weten wie goedkeuring moet geven voor welke uitgaven;
- **Regelmatig training en bewustwording**
  - **Opleidingsprogramma's:** Bied regelmatig trainingen aan om medewerkers bewust te maken van het belang van autorisatieprocessen en het herkennen van frauderisico's;
  - **Bewustwordingscampagnes:** Organiseer campagnes die medewerkers informeren over de gevolgen van frauduleuze activiteiten en benadruk hun rol in het voorkomen daarvan;
- **Versterking van interne controles:**
  - **Toegepaste controlemiddelen:** Implementeer een goedkeuringsproces dat gebaseerd is op rolgebaseerde autorisatie voor belangrijke documenten en transacties, inclusief prestatieleveringsdocumentatie. Zorg ervoor dat goedkeuringen in het systeem worden vastgelegd, zodat er altijd een audittrail beschikbaar is om de authenticiteit en integriteit van documenten te waarborgen;
- **Audits en beoordelingen**
  - **Regelmatige interne audits:** Voer periodieke interne audits uit om de effectiviteit van het autorisatiesysteem te evalueren en eventuele zwakke punten tijdig aan te pakken;
  - **Externe beoordelingen:** Overweeg het inschakelen van externe auditors voor een objectieve evaluatie van de financiële en operationele processen;
- **Invoeren van tweefactorauthenticatie**
  - **Implementatie van 2FA:** Zorg ervoor dat de toegang tot belangrijke systemen en goedkeuringsprocessen beveiligd is met tweefactorauthenticatie, waardoor de kans op ongeoorloofde toegang wordt geminimaliseerd;
- **Continu verbeteren van processen**
  - **Feedbacksystemen:** Creëer een feedbackmechanisme waarmee medewerkers problemen of onregelmatigheden in de processen kunnen melden;
  - **Evaluatie en aanpassing:** Evalueer regelmatig de effectiviteit van bestaande processen en pas deze aan waar nodig om nieuwe risico's te adresseren;
- **Versterken van de relatie met leveranciers**

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ **Regelmatige communicatie:** Onderhoud open communicatielijnen met leveranciers om vertrouwen te vergroten en hen te informeren over wijzigingen in procedures; ○ **Vaststellen van contractuele verplichtingen:** Zorg ervoor dat contracten duidelijke voorwaarden bevatten over goedkeuringsprocessen en betalingsverplichtingen; • **Compliance en Wetgeving** ○ **Monitoring van regelgeving:** Blijf op de hoogte van wijzigingen in wet- en regelgeving die van invloed kunnen zijn op de organisatie en pas de processen aan om aan deze vereisten te voldoen. ○ **Compliance-training:** Organiseer trainingen voor medewerkers om hen te onderrichten over naleving van regelgeving en interne beleidslijnen.							
• Onvoldoende gestructureerd betalingsproces door ongeoorloofde aanpassingen van de stamgegevens van crediteuren; Een onvoldoende gestructureerd betalingsproces door ongeoorloofde aanpassingen van de stamgegevens van crediteuren kan leiden tot frauduleuze betalingen aan niet-legitieme partijen, wat aanzienlijke financiële schade voor GGDrU kan veroorzaken. Daarnaast kan dit de relaties met betrouwbare crediteuren ondermijnen en operationele verstoringen veroorzaken, waardoor de continuïteit van zorgverlening in gevaar komt.	Ja	• **Fraude**: Onrechtmatige wijzigingen in crediteurengegevens kunnen leiden tot frauduleuze betalingen aan valse of ongewenste crediteuren, wat aanzienlijke financiële verliezen kan veroorzaken; • **Financieel verlies**: Foutieve of ongeoorloofde betalingen kunnen leiden tot onnodige kosten, wat de financiële gezondheid van GGDrU kan aantasten; • **Schade crediteurenrelatie:** Problemen met betalingen kunnen de relatie met legitieme crediteuren schaden, wat kan leiden tot een verminderd vertrouwen en zelfs de mogelijkheid dat zij hun diensten of producten intrekken; • **Operationele verstoring**: Onjuiste betalingen kunnen leiden tot verstoringen, zoals vertragingen in de levering van medische benodigdheden, wat de zorgverlening in gevaar kan brengen; • **Juridische gevolgen**: Indien betalingen zijn gedaan op basis van vervalste gegevens, kan GGDrU juridische aansprakelijk	M 	H 	**Logboek in AFAS** 1. **Registratie van wijzigingen** ○ **Automatische logregistratie**: Het AFAS-systeem registreert automatisch alle wijzigingen in bankrekeninggegevens, inclusief wie de wijziging heeft aangebracht, wanneer deze is aangebracht, en welke gegevens zijn gewijzigd; ○ **Documentatie van reden**: Dit verplicht medewerkers om een reden voor de wijziging in te voeren, zodat er een duidelijk overzicht is van de motieven achter elke aanpassing; 2. **Toegangscontrole** ○ **Beperk toegang tot wijzigingsfuncties**: Alleen bevoegde medewerkers hebben toegang tot de functies in AFAS die bankrekeninggegevens kunnen wijzigen. Dit beperkt de kans op ongeoorloofde aanpassingen;	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		zijn, wat kan resulteren in rechtszaken of boetes; • **Reputatieschade**: Het bekend worden van fraude of fouten in het betalingsproces kan leiden tot reputatieschade, wat het vertrouwen van stakeholders kan ondermijnen; • **Compliance Risico's**: Een inadequaat betalingsproces kan leiden tot niet-naleving van regelgeving en interne controlemaatregelen, wat kan resulteren in audits en sancties.			○ **Rolgebaseerde toegang**: Rolgebaseerde toegang waarbij verschillende gebruikersgroepen verschillende niveaus van toegang tot de logboekfuncties hebben; 3. **Audit trails** ○ **Ingebouwde audit trails**: Gebruik maken van de audit trail-functionaliteit van AFAS om een gedetailleerd overzicht te bieden van alle acties die zijn uitgevoerd binnen het systeem. Dit helpt bij het opsporen van verdachte activiteiten; ○ **Regelmatige audits**: Periodieke audits op het logboek om te controleren op ongebruikelijke patronen of verdachte wijzigingen in bankrekeninggegevens; 4. **Notificaties en Rapportages** ○ **Automatische meldingen**: Het systeem verstuurt automatisch meldingen naar relevante medewerkers wanneer wijzigingen in bankrekeninggegevens worden aangebracht. Dit bevordert transparantie en snelle reacties op mogelijke problemen;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					○ **Regelmatig rapportages**: Regelmatig rapportages van het logboek om een overzicht te hebben van recente wijzigingen en de betrokken medewerkers. Dit helpt bij het identificeren van trends en het aanpakken van potentiële risico's; 5. **Training en bewustwording** ○ **Opleiding over logboekgebruik**: Training van medewerkers in het gebruik van het logboek binnen AFAS en het belang van het registreren van wijzigingen. Dit verhoogt de bewustwording van de noodzaak voor nauwkeurigheid en transparantie; ○ **Cultuur van verantwoordelijkheid**: Stimuleren van een cultuur waarin medewerkers zich verantwoordelijk voelen voor het registreren van hun acties en het melden van verdachte activiteiten; **Functiescheiding Implementeren** 1. **Scheiding van verantwoordelijkheden**:		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					Verantwoordelijkheden voor het wijzigen van bankrekeninggegevens, het goedkeuren van betalingen en het uitvoeren van betalingen zijn gescheiden. Dit helpt te voorkomen dat één persoon ongecontroleerde wijzigingen kan doorvoeren; 2. **Verantwoordelijke rollen toewijzen**: ○ **Initiëren**: De medewerker die een wijziging in bankrekeninggegevens aanvraagt; ○ **Controleren**: Een tweede medewerker die de wijziging verifieert en goedkeurt; ○ **Uitvoeren**: Een derde medewerker die de betalingen daadwerkelijk uitvoert; **Verificatieprocessen** 1. **Persoonlijke verificatie**: Bij wijzigingen in bankrekeninggegevens, zoals een nieuwe rekening, moet de wijziging telefonisch of schriftelijk worden bevestigd met de betrokken crediteur. Dit vermindert de kans op frauduleuze wijzigingen; 2. **Documentatie van wijzigingen**: Alle wijzigingen in bankrekeninggegevens worden gedocumenteerd, inclusief de		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					redenen voor de wijziging en de goedkeuring van de betrokken partijen; **Gebruik van digitale handtekeningen** 1. **Authenticatieprocessen**: Digitale handtekeningen voor het goedkeuren van wijzigingen in bankrekeninggegevens. Dit zorgt voor een extra beveiligingslaag en maakt het moeilijker om onrechtmatige wijzigingen door te voeren; 2. **Workflow-integratie**: De digitale handtekeningen zijn naadloos geïntegreerd in de bestaande AFAS-workflow. Dit betekent dat wanneer een wijziging in bankrekeninggegevens wordt aangevraagd, de betrokken medewerkers automatisch een goedkeuringsverzoek ontvangen dat alleen kan worden goedgekeurd door het gebruik van hun digitale handtekening; 3. **Beveiliging en traceerbaarheid**: De digitale handtekeningen bieden een extra beveiligingslaag, waardoor onrechtmatige wijzigingen moeilijker door te voeren zijn. Bovendien zorgt deze methode voor traceerbaarheid, zodat het mogelijk is om te zien wie de wijziging heeft goedgekeurd en wanneer, wat helpt bij het verminderen van fraude-risico's en het waarborgen van accountability;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					4. **Training en implementatie**: Medewerkers worden goed opgeleid in het gebruik van digitale handtekeningen en de bijbehorende workflow in AFAS. Dit verhoogt de acceptatie en effectieve implementatie van deze maatregel; **Monitoring en Rapportage** 1. **Monitoring van wijzigingen**: Een systeem dat alle wijzigingen in bankrekeninggegevens in realtime monitort en rapporteert. Dit kan helpen bij het snel identificeren van verdachte activiteiten; 2. **Regelmatig rapportages**: Regelmatig rapportages over wijzigingen in bankrekeninggegevens en wie deze heeft goedgekeurd. Dit bevordert transparantie en kan helpen bij interne audits; **Training en Bewustwording** 1. **Opleidingen over functiescheiding**: Medewerkers zijn goed op de hoogte van het belang van functiescheiding en de specifieke procedures die zij moeten volgen bij het wijzigen van bankrekeninggegevens; 2. **Cultuur van waakzaamheid**: Stimuleren van een cultuur waarin medewerkers zich bewust zijn van frauderisico's en aangemoedigd worden om verdachte activiteiten te melden.		
Acties voor verbetering							

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Door deze aanvullende acties te implementeren, kan GGDrU niet alleen het restrisico verder minimaliseren, maar ook een sterke cultuur van integriteit en verantwoordelijkheid bevorderen, wat essentieel is voor het voorkomen van fraude en andere financiële risico's: **Regelmatige Training en Bewustwording** • **Opleidingsprogramma's**: Voer regelmatig trainingen uit voor medewerkers over het belang van interne controles, fraudepreventie en het gebruik van digitale handtekeningen. Dit vergroot het bewustzijn en de verantwoordelijkheid onder medewerkers; • **Simulaties van Frauderisico's**: Organiseer simulaties of workshops waarbij medewerkers worden geconfronteerd met mogelijke frauduleuze scenario's, zodat ze leren hoe ze deze kunnen herkennen en voorkomen; **2. Versterken van interne Controlemechanismen** • **Dynamische risicoanalyse**: Voer periodieke risicoanalyses uit om nieuwe of opkomende risico's te identificeren en te beoordelen, en pas de controles hierop aan; • **Beleid voor wijzigingen**: Stel strikte richtlijnen op voor het wijzigen van bankrekeninggegevens en andere belangrijke gegevens. Zorg ervoor dat deze wijzigingen alleen worden doorgevoerd na goedkeuring van meerdere bevoegde personen; **3. Audits en toezicht** • **Interne en externe Audits**: Voer regelmatig interne en externe audits uit om de effectiviteit van de beheersmaatregelen en controles te beoordelen en om zwaktes in processen te identificeren; • **Toezicht op logboeken**: Monitor logboeken regelmatig op verdachte activiteiten en volg afwijkingen of patronen op die kunnen wijzen op onregelmatigheden; **4. Technologische innovaties** • **Fraudedetectiesystemen**: Implementeer geavanceerde softwareoplossingen voor het detecteren van fraude en onregelmatigheden. Dit kan inhouden dat analyses worden uitgevoerd met behulp van kunstmatige intelligentie (AI), die afwijkingen in betalingspatronen kan identificeren; • **Tweefactorauthenticatie**: Implementeer tweefactorauthenticatie (2FA) voor toegang tot essentiële systemen en bij het goedkeuren van wijzigingen in financiële gegevens. 2FA is een beveiligingsmaatregel die vereist dat gebruikers twee verschillende vormen van identificatie verstrekken, zoals een wachtwoord en een eenmalige code, voordat ze toegang krijgen. Deze extra beveiligingslaag verkleint de kans op ongeoorloofde toegang en versterkt het vertrouwen van stakeholders in de gegevensbeveiliging van de organisatie; **5. Verbetering van communicatie met crediteuren** • **Proactieve communicatie**: Zorg voor open en regelmatige communicatie met crediteuren, vooral bij wijzigingen in bankgegevens. Dit kan helpen om ongewenste situaties te voorkomen; • **Verificatie van wijzigingen**: Voer altijd een verificatieproces uit met crediteuren bij wijzigingen in bankrekeninggegevens, zoals het bevestigen van wijzigingen via een telefoongesprek of een schriftelijke bevestiging; **6. Cultuur van transparantie** • **Rapportage van verdachte activiteiten**: Stimuleer een cultuur waarin medewerkers zich veilig voelen om verdachte activiteiten of afwijkingen te melden zonder angst voor repercussies; • **Beloningssysteem**: Introduceer een soort van beloningssysteem voor medewerkers die bijdragen aan het verbeteren van de integriteit van processen en het melden van potentiële risico's.							
• Onvoldoende fysieke beveiligingsmaatregelen voor contanten,	Ja	• **Diefstal of verduistering**: Onvoldoende beveiliging kan leiden tot diefstal van medische apparatuur, medicijnen of andere	M tot H	M tot H 😐	**2. Diefstal of Verduistering** • **Toegangscontrole**: Strikte toegangscontroles voor gebieden met waardevolle bedrijfsmiddelen,	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
beleggingen, voorraden of andere bedrijfsmiddelen; GGDrU heeft het gebruik van contanten, zoals muntgeld en bankbiljetten, geminimaliseerd, en werkt niet met effecten, zoals aandelen en obligaties. Onvoldoende beveiliging van contanten kan leiden tot diefstal of verlies, wat de financiële stabiliteit van GGDrU ondermijnt en het vertrouwen van cliënten en investeerders schaadt. Evenzo is het essentieel om beleggingen, zoals effecten en vastgoed, goed te beveiligen om ongeoorloofde toegang en manipulatie te voorkomen, aangezien dit kan resulteren in aanzienlijke financiële verliezen. Daarnaast is het waarborgen van de beveiliging van voorraden en andere bedrijfsmiddelen cruciaal voor de continuïteit van de zorgverlening, omdat verduistering of verlies van medische benodigdheden en apparatuur directe gevolgen heeft voor de kwaliteit van de zorg.		waardevolle bedrijfsmiddelen, wat niet alleen financieel verlies oplevert, maar ook de continuïteit van zorg kan bedreigen; • **Verlies van medische benodigdheden**: Onvoldoende controle over voorraden kan resulteren in het verlies van cruciale medische benodigdheden, wat directe gevolgen heeft voor de kwaliteit van de zorg en de veiligheid van gebruikers; • **Vervangingskosten**: Diefstal of schade aan bedrijfsmiddelen zoals gebouwen en apparatuur kan aanzienlijke vervangingskosten met zich meebrengen, wat een zware financiële last voor de organisatie kan zijn • **Operationele verstoring**: De onbeschikbaarheid van essentiële bedrijfsmiddelen door diefstal of schade kan leiden tot verstoringen in de dagelijkse operatie, waardoor de zorgverlening aan cliënten in gevaar komt; • **Verlies van vertrouwen**: Als stakeholders, waaronder inwoners en zorgverzekeraars, horen van beveiligingsproblemen en diefstal, kan dit hun vertrouwen in GGDrU schaden, wat kan leiden tot reputatieschade en een vermindering van de samenwerking en financiering**;** • **Juridische gevolgen**: Onvoldoende beveiliging kan ook leiden tot juridische complicaties,			inclusief elektronische toegangssystemen en identificatiekaarten; • **Beveiligingscamera's**: CCTV-camera's in en rond opslagruimten om toezicht te houden en diefstal te ontmoedigen; • **Medewerkerstraining**: Training aan personeel over beveiligingsprocedures en het melden van verdachte activiteiten; **2. Verlies van medische benodigdheden** • **Voorraadbeheer**: Effectief voorraadbeheersysteem met regelmatige controles om de beschikbaarheid van medische benodigdheden te waarborgen; • **Labeling en tracking**: Duidelijke labeling en tracking van voorraden, zodat elke afname gemakkelijk kan worden gevolgd; • **Veilige opslag**: Medische benodigdheden worden in beveiligde en goed gecontroleerde opslagruimtes gewaard; **3. Vervangingskosten** • **Preventief onderhoud**: Regelmatig onderhoud en inspecties op apparatuur en gebouwen om schade te voorkomen; • **Verzekeringen**: Adequate verzekeringen om financiële verliezen door schade of diefstal te dekken; **4. Operationele verstoring**		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		zoals aansprakelijkheidsclaims of boetes, als de organisatie niet in staat is om te voldoen aan wet- en regelgeving met betrekking tot de beveiliging van bedrijfsmiddelen.			• **Continuïteitsplanning**: Noodplan om operationele verstoringen snel te kunnen opvangen, inclusief alternatieve procedures en middelen; • **Regelmatige oefeningen**: Regelmatig oefeningen om personeel voor te bereiden op noodsituaties en operationele verstoringen; **5. Verlies van vertrouwen** • **Transparante communicatie**: Open communicatie met stakeholders over beveiligingsmaatregelen en incidenten om vertrouwen te behouden; • **Feedback mechanismen**: Mechanismen voor feedback van stakeholders om hun zorgen en suggesties serieus te nemen; **6. Juridische gevolgen** • **Compliance training**: Training van personeel over relevante wet- en regelgeving om juridische complicaties te voorkomen; • **Regelmatig audits**: Regelmatig interne audits om naleving van beveiligingsnormen en wetgeving te waarborgen. **Algemeen** • **Beveiligingsbeleid**: Een uitgebreid beveiligingsbeleid dat alle aspecten van fysieke beveiliging dekt; • **Risicoanalyse**: Regelmatig risicoanalyses om nieuwe		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					kwetsbaarheden te identificeren en aan te pakken.		

Acties voor verbetering
Door deze aanvullende acties te implementeren, kan de GGDrU het restrisico verder minimaliseren en een robuustere beveiligingsomgeving creëren.

1. Regelmatige beveiligingsaudits

- **Externe evaluatie**: Schakel externe experts in om de beveiligingsmaatregelen te evalueren en aanbevelingen te doen voor verbeteringen;
- **Interne controles**: Voer periodieke interne controles uit om de effectiviteit van bestaande maatregelen te beoordelen;

2. Technologische investeringen

- **Geavanceerde beveiligingssystemen**: Investeer in moderne beveiligingssystemen zoals biometrische toegang, alarmsystemen en geautomatiseerde voorraadbeheersystemen;
- **Data-analyse en AI (Engels: Artificial Intelligence)**: Maak gebruik van data-analyse en kunstmatige intelligentie om verdachte patronen of activiteiten vroegtijdig te identificeren;

3. Versterking van bedrijfscultuur

- **Cultuur van verantwoordelijkheid**: Stimuleer een cultuur waarin medewerkers verantwoordelijk worden gehouden voor de beveiliging van bedrijfsmiddelen;
- **Zichtbaarheid van beveiliging**: Maak beveiligingsmaatregelen zichtbaar en herkenbaar om medewerkers te herinneren aan de noodzaak van beveiliging;

4. Noodplannen en oefeningen

- **Regelmatige oefeningen**: Organiseer regelmatig oefensessies of simulaties om personeel voor te bereiden op noodsituaties en diefstalincidenten.
- **Noodcommunicatieplan**: Ontwikkel een communicatieplan om snel te kunnen reageren op beveiligingsincidenten.

5. Samenwerking met Lokale Autoriteiten

- **Contact met Politie en Veiligheidsdiensten**: Onderhoud goede relaties met lokale autoriteiten en beveiligingsdiensten om snel te kunnen reageren op incidenten en om advies te vragen over beveiligingsstrategieën.
- **Deelname aan Veiligheidsnetwerken**: Sluit je aan bij lokale veiligheidsnetwerken om best practices en ervaringen te delen met andere organisaties.

6. Personeelsbeleid

- **Achtergrondcontroles**: Voer grondige achtergrondcontroles uit bij nieuwe medewerkers, vooral voor posities met toegang tot waardevolle bedrijfsmiddelen.
- **Doorlopende Training**: Bied doorlopende training en bewustwordingsprogramma's aan voor personeel over beveiliging en fraudepreventie.

7. Feedback en Verbetering

- **Feedback Mechanismen**: Implementeer systemen voor medewerkers om beveiligingsproblemen of -zorgen te rapporteren zonder angst voor repercussies.
- **Continue Verbetering**: Evalueer regelmatig de effectiviteit van de maatregelen en pas deze aan op basis van feedback en nieuwe bedreigingen.

1. Het gebrek aan tijdige en adequate documentatie van transacties. Het gebrek aan tijdige en adequate documentatie van transacties verwijst naar de	Ja	• **Financiële Onzekerheid**: Onvolledige of vertraagde documentatie kan leiden tot onjuiste financiële rapportages, wat het management en externe belanghebbenden een vertekend beeld van de financiële	H 	H 	• **Standaardisatie van documentatieprocessen**: Gestandaardiseerde procedures voor het vastleggen van transacties, inclusief sjablonen en richtlijnen om de consistentie en volledigheid te waarborgen;	M to H  	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
situatie waarin financiële of operationele activiteiten binnen een organisatie niet op een juiste, volledige of tijdige manier worden vastgelegd;		gezondheid van de organisatie geeft; • **Compliance risico's**: Bij onvoldoende documentatie kan GGDrU in strijd komen met wettelijke en regelgevende vereisten, wat kan leiden tot juridische problemen, boetes en reputatieschade; • **Verhoogd risico op fraude**: Zonder adequate documentatie kunnen medewerkers zich gemakkelijker schuldig maken aan ongeoorloofd gedrag of fraude, omdat er minder controlemechanismen zijn om onregelmatigheden op te sporen; • **Moeilijkheden bij audits**: Slechte documentatie maakt het voor interne en externe auditors lastig om de juistheid en volledigheid van de financiële administratie te verifiëren, wat kan leiden tot onbetrouwbare auditresultaten; • **Verlies van informatie**: Tijdige documentatie is essentieel voor het behoud van belangrijke gegevens. Het ontbreken hiervan kan resulteren in het verlies van cruciale informatie die nodig is voor analyses, rapportages of strategische besluitvorming; • **Operationele inefficiëntie**: Onvoldoende documentatie kan leiden tot verwarring en vertragingen in operationele processen, wat de algehele			• **Tijdige verwerking**: • Deadlines voor de registratie van transacties om vertragingen te voorkomen en ervoor te zorgen dat documentatie altijd up-to-date is; • **Interne audits**: Regelmatig interne audits om de kwaliteit van de documentatie en de naleving van procedures te controleren. Dit helpt om eventuele tekortkomingen tijdig te signaleren en te corrigeren; • **Training en voorlichting**: Trainingen voor medewerkers over het belang van goede documentatie, de juiste procedures en de mogelijke gevolgen van onvoldoende documentatie. Dit verhoogt de bewustwording en verantwoordelijkheid; • **Toezicht en controle**: Toegewezen specifieke verantwoordelijkheden voor de documentatie van transacties en toezicht door een verantwoordelijke manager of teamleider; • **Gebruik van technologie**: Software en systemen die automatische meldingen geven bij uitstaande documentatie of transacties die niet tijdig zijn geregistreerd, en die de toegang tot transactiedata beheren; • **Feedback mechanismen**: Systeem waar medewerkers feedback kunnen geven over de		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		efficiëntie en effectiviteit van de organisatie schaadt; • **Slechte besluitvorming**: Gebrek aan accurate en tijdige gegevens kan het management verhinderen om goed geïnformeerde beslissingen te nemen, wat kan leiden tot suboptimale strategische keuzes; • **Cultuur van onverantwoordelijkheid**: Het negeren van documentatievereisten kan een cultuur creëren waarin medewerkers zich minder verantwoordelijk voelen voor hun acties, wat de integriteit en ethiek binnen de organisatie kan ondermijnen.			documentatieprocessen en waar eventuele problemen of knelpunten kunnen worden gemeld; • **Periodieke evaluatie**: Regelmatig evalueren van de documentatieprocessen en -procedures om ervoor te zorgen dat ze effectief zijn en blijven voldoen aan de behoeften van de organisatie.		

Acties voor verbetering

Door deze acties te implementeren kan GGDrU de kans op documentatieproblemen verder verminderen en de algehele betrouwbaarheid van hun transactiedocumentatie verbeteren:

- **Versterking van de cultuur van verantwoording**:
  Moedig een cultuur aan waarin medewerkers zich verantwoordelijk voelen voor nauwkeurige documentatie en waar fouten of tekortkomingen openlijk worden besproken en gecorrigeerd
- **Periodieke training en opfriscursussen**:
- Organiseer regelmatige trainingen voor medewerkers over documentatieprocedures en het belang ervan, inclusief updates over nieuwe systemen of processen;
- **Technologische innovaties**:
- Overweeg de implementatie van geavanceerde documentbeheer- en automatiseringssystemen die real-time gegevensinvoer mogelijk maken en automatische rapportages genereren over ontbrekende of vertraagde documentatie;
- **Feedback en evaluatie**:
- Implementeer een structureel feedbackmechanisme waarbij medewerkers suggesties kunnen doen voor verbeteringen in documentatieprocessen, en evalueer regelmatig de effectiviteit van de huidige maatregelen;
- **Continue monitoring**:
- Voer een systeem van continue monitoring en evaluatie in dat gebruikmaakt van dashboards en rapportages om trends en afwijkingen in documentatieprocessen tijdig te signaleren;
- **Crisismanagementplannen**:
- Ontwikkel plannen voor onverwachte situaties (bijvoorbeeld een toename van werkzaamheden) zodat de organisatie voorbereid is om documentatieprocessen te waarborgen, zelfs onder druk.

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
• Het ontbreken van verplichte vakantiedagen voor medewerkers in sleutelposities binnen de interne beheersing vormt een risico, omdat dit onafhankelijk toezicht op hun werkzaamheden uitsluit. Dit kan ongeoorloofd gedrag verdoezelen en een cultuur van fraude bevorderen. Het is cruciaal om verplichte vakanties in te voeren voor meer transparantie en integriteit binnen de organisatie; Het ontbreken van verplichte vakantiedagen voor personeel in sleutelposities vergroot het risico op fraude en diefstal, omdat deze medewerkers geen onafhankelijke controle op hun activiteiten hebben. Dit kan leiden tot een gebrek aan transparantie en verantwoordelijkheidsgevoel, waardoor ongeoorloofd gedrag gemakkelijker wordt verborgen. Bovendien kan het gebrek aan verplichte rustperiodes een ongezonde werkcultuur bevorderen en de organisatie kwetsbaar maken voor operationele verstoringen.	Ja	• **Fraude en misbruik**: Medewerkers kunnen ongeoorloofd gedrag of fraude plegen zonder dat dit wordt opgemerkt, aangezien ze constant toegang hebben tot hun verantwoordelijkheden en systemen; • **Gebrek aan onafhankelijkheid**: Het ontbreken van een verplichte vakantie kan leiden tot een gebrek aan onafhankelijk toezicht. Collega's of management hebben mogelijk geen inzicht in ongebruikelijke handelingen of fouten; • **Cultuur van onethisch edrag**: Het niet verplicht stellen van vakanties kan een cultuur van onverschilligheid of zelfs omkoping bevorderen, waarin medewerkers zich niet verantwoordelijk voelen voor hun handelen; • **Verhoogde fouten**: Medewerkers die continu werken zonder pauzes zijn vatbaarder voor vermoeidheid en fouten, wat kan leiden tot onjuiste beslissingen of administratieve tekortkomingen; • **Risico op burn-out**: Het ontbreken van verplichte vakanties kan ook leiden tot burn-out onder medewerkers, wat hun effectiviteit en de algehele prestaties van de organisatie kan beïnvloeden.	H ☹	H ☹	• **Invoering van verplichte vakantiedagen**: Beleid dat ook medewerkers in sleutelposities verplicht om jaarlijks een vastgesteld aantal vakantiedagen op te nemen. Dit bevordert niet alleen welzijn, maar verhoogt ook de transparantie; • **Regelmatige toezicht en controle**: Verantwoordelijkheden en activiteiten van medewerkers in sleutelposities worden regelmatig worden beoordeeld door een onafhankelijke derde partij of door andere teamleden. Dit kan helpen om ongebruikelijk gedrag tijdig te signaleren; • **Opleiding en bewustwording**: Trainingen over het belang van verplichte vakantiedagen en de risico's van fraude en ongeoorloofd gedrag. Cultuur waarin medewerkers zich verantwoordelijk voelen voor hun acties en begrijpen waarom deze maatregelen noodzakelijk zijn; • **Monitoring van werkzaamheden**: Systeem voor het registreren en monitoren van de werkzaamheden van medewerkers in sleutelposities. Dit helpt om eventuele onregelmatigheden of afwijkingen snel te identificeren; • **Rotatie van functies**: Functie-rotatiesysteem voor medewerkers in sleutelposities. Dit kan de continuïteit van de werkzaamheden waarborgen en	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					zorgen voor een frisse blik op de processen; • **Feedbackmechanismen**: Anonieme kanalen waar medewerkers hun zorgen over ongeoorloofd gedrag of de cultuur binnen de organisatie kunnen uiten, zonder angst voor repercussies; • **Audit en evaluatie**: Regelmatige audits van de interne beheersingssystemen en evalueer de effectiviteit van de maatregelen. Dit helpt om de naleving te waarborgen en de integriteit van de organisatie te versterken.		
• Onvoldoende kennis van informatietechnologie bij het management, waardoor IT-personeel de mogelijkheid heeft om bedrijfsmiddelen onrechtmatig toe te eigenen;	Ja	• **Fraude en misbruik**: IT-personeel kan kwetsbaarheden in systemen uitbuiten om bedrijfsmiddelen of gegevens onrechtmatig toe te eigenen, wat kan leiden tot financiële verliezen; • **Gegevenslekken**: Onvoldoende toezicht kan resulteren in het onterecht delen of stelen van gevoelige informatie, met schadelijke gevolgen voor de privacy en reputatie van de organisatie; • **Slechte besluitvorming**: Gebrek aan inzicht in technologische aspecten kan leiden tot slechte strategische beslissingen, wat de operationele efficiëntie en	H ☹	H ☹	• **Opleiding en training**: Gerichte trainingen voor het management om hun kennis van informatietechnologie en relevante systemen te verbeteren; • **Inzet van IT-experts**: Betrekken van IT-experts bij het managementteam om ervoor te zorgen dat technologische beslissingen goed onderbouwd zijn en aansluiten bij de organisatiebehoeften; • **Regelmatige evaluatie**: Periodieke beoordelingen van de IT-infrastructuur en processen om eventuele kennishiaten te identificeren en aan te pakken; • **Implementatie van technologieën**: Investeringen in gebruiksvriendelijke technologieën	M tot H 😐 ☹	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		effectiviteit van de organisatie beïnvloedt; • **Compliance risico's**: Het niet voldoen aan regelgeving en normen voor gegevensbeveiliging kan juridische en financiële repercussies met zich meebrengen; • **Verlies van vertrouwen**: Klanten en stakeholders kunnen het vertrouwen in GGDrU verliezen als gevolg van onprofessionele omgang met IT-beheer en beveiliging; • **Verhoogde operationele kosten**: Problemen die voortkomen uit een gebrek aan kennis kunnen leiden tot hogere kosten voor het herstel van beveiligingsincidenten of systeemfouten; • **Verlies van concurrentievermogen**: Ineffectief gebruik van technologie kan GGDrU achterlaten bij concurrenten die beter gebruikmaken van informatietechnologie.			die het management ondersteunen in hun dagelijkse werkzaamheden en die eenvoudig te begrijpen zijn; • **Communicatie en rapportage**: Duidelijke communicatielijnen tussen IT-personeel en management om technische informatie toegankelijk en begrijpelijk te maken; • **Feedback mechanismen**: Systeem voor feedback van het management over IT-ondersteuning, zodat IT-personeel kan inspelen op hun behoeften en zorgen; • **Externe adviseurs**: Inschakelen van externe IT-adviseurs voor strategisch advies en om het management te helpen bij het maken van geïnformeerde beslissingen.		

Acties voor verbetering

Door deze acties te implementeren, kan GGDrU het restrisico verder verlagen en een veiligere en effectievere werkomgeving creëren:

1. **Continue opleiding en training**:
    - Organiseer regelmatig trainingen en workshops voor het management en relevante medewerkers over informatietechnologie, cybersecurity en gegevensbeheer. Dit helpt bij het up-to-date houden van kennis en vaardigheden;
2. **Invoering van IT-audits**:
    - Voer periodieke interne en externe audits uit van de IT-systemen en -processen om eventuele tekortkomingen in de beheersmaatregelen te identificeren en aan te pakken;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
3. **Versterking van beleid en procedures**: ○ Ontwikkel en implementeer duidelijke richtlijnen en procedures voor het gebruik van IT-systemen en bedrijfsmiddelen. Zorg ervoor dat deze toegankelijk zijn voor alle medewerkers; 4. **Betrekken van IT-experts**: ○ Schakel externe IT-experts in om het management te adviseren over belangrijke technologiegerelateerde beslissingen en om best practices te delen; 5. **Regelmatige evaluatie van beheersmaatregelen**: ○ Voer regelmatig evaluaties uit van de bestaande beheersmaatregelen en -procedures om te waarborgen dat deze effectief blijven in het voorkomen van ongeoorloofd gedrag; 6. **Implementatie van toegangscontroles**: ○ Zorg ervoor dat toegang tot gevoelige gegevens en systemen beperkt is tot alleen die medewerkers die deze informatie nodig hebben voor hun werk; 7. **Cultuur van transparantie en verantwoording**: ○ Moedig een cultuur aan waarin medewerkers zich vrij voelen om onregelmatigheden te melden en waar integriteit wordt gewaardeerd; 8. **Oprichten van een IT-commissiegroep**: ○ Stel een groep samen van IT-specialisten en managementleden die regelmatig overlegt om de IT-strategie te evalueren en te verbeteren; 9. **Gebruik van technologie voor monitoring**: ○ Implementeer technologieën die ongebruikelijke activiteiten of toegangspatronen automatisch kunnen detecteren en rapporteren, zodat tijdig kan worden ingegrepen; 10. **Feedback mechanismen**: ○ Creëer anonieme kanalen voor medewerkers om eventuele zorgen of problemen met betrekking tot IT-beveiliging en gebruik te rapporteren zonder angst voor repercussies.							
• Inadequate beoordeling van de frauderisico's met betrekking tot cybersecurity en cloud computing	Ja	• **Gegevensinbreuken:** Onvoldoende bescherming kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens, wat kan resulteren in datalekken en schending van privacy; • **Financiële verliezen:** Cyberaanvallen kunnen directe financiële schade veroorzaken door diefstal van fondsen of kosten verbonden aan het herstel van systemen en gegevens; • **Reputatieschade:** Een datalek of cyberaanval kan het vertrouwen van cliënten en partners in GGDrU schaden, wat leidt tot reputatieverlies en mogelijke	H 	H 	• **Risicoanalyse:** Regelmatige en uitgebreide risicoanalyses uit om potentiële cyberdreigingen te identificeren en te evalueren; • **Beveiligingsbeleid:** Ontwikkeling en implementatie gedegen beveiligingsbeleid dat richtlijnen geeft voor databeveiliging, toegang tot systemen en gebruik van cloud-diensten; • **Toegangscontrole:** Implementatie strenge toegangscontroles en autorisatieprocedures om ervoor te zorgen dat alleen geautoriseerde medewerkers toegang hebben tot gevoelige gegevens en systemen; • **Training en bewustwording:** Bieden van regelmatig training aan medewerkers over cybersecurity-	M tot H 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		gevolgen voor toekomstige samenwerkingen; • **Compliance-risico's:** Niet voldoen aan wettelijke vereisten voor gegevensbeveiliging kan resulteren in juridische gevolgen en boetes; • **Operationele onderbrekingen:** Cyberaanvallen kunnen leiden tot stilstand van systemen, waardoor de operationele processen van GGDrU worden verstoord; • **Verlies van intellectueel eigendom:** Onbeveiligde cloudomgevingen kunnen leiden tot diefstal van waardevolle intellectuele eigendommen of bedrijfsgevoelige informatie; • **Verhoogde kwetsbaarheid voor toekomstige aanvallen:** Een eerdere cyberaanval kan de organisatie kwetsbaarder maken voor toekomstige aanvallen, vooral als beveiligingsmaatregelen niet adequaat worden aangepast.			bewustzijn en hoe te reageren op potentiële bedreigingen zoals phishing; • **Monitoring en detectie:** Gebruik van geavanceerde monitoringtools voor het detecteren van ongebruikelijke activiteiten of inbreuken op de beveiliging; • **Incident response plan:** Gedetailleerd incident response plan om snel en effectief te reageren op beveiligingsincidenten; • **Updates en patches:** Regelmatige updates en patches van software en systemen om kwetsbaarheden te verhelpen; • **Externe audits:** Regelmatig externe audits om de effectiviteit van de beveiligingsmaatregelen te beoordelen en aan te passen waar nodig; • **Back-up en herstel:** Implementatie robuuste back-up- en herstelprocedures om gegevensverlies te voorkomen in het geval van een cyberaanval; • **Compliance checks:** Naleving van relevante wet- en regelgeving met betrekking tot databeveiliging en privacy.		

Acties voor verbetering

Hier zijn enkele verbeteracties voor GGDrU met betrekking tot de onjuiste inschatting van frauderisico's van cybersecurity en cloud computing:

1. **Regelmatige risicoanalyses:** Voer periodieke beoordelingen uit van de cybersecurityrisico's, met een focus op cloud computing, om nieuwe bedreigingen tijdig te identificeren;
2. **Training en bewustwording:** Organiseer trainingen voor medewerkers over cybersecurity en de risico's van cloud computing, inclusief het herkennen van verdachte activiteiten;
3. **Implementatie van beveiligingsprotocollen:** Ontwikkel en implementeer duidelijke beveiligingsrichtlijnen en -protocollen voor het gebruik van cloudservices;

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
4. **Monitoring en incidentrespons:** Zet een continu monitoringsysteem op voor verdachte activiteiten en zorg voor een duidelijk incidentresponsplan; 5. **Samenwerking met experts:** Overweeg samenwerking met externe cybersecurity-experts om de beveiligingsmaatregelen te verbeteren en up-to-date te blijven met de nieuwste dreigingen; 6. **Gebruik van Technologie:** Investeer in geavanceerde beveiligingstechnologieën zoals multi-factor authenticatie en encryptie voor gevoelige data.							
• Onvoldoende beveiligingsmaatregelen voor de toegang tot geautomatiseerde bestanden, inclusief een gebrek aan interne controles met betrekking tot de logbestanden van computersystemen en de evaluatie daarvan;	Ja	• **Onbevoegde Toegang:** Gebrek aan adequate beveiliging kan leiden tot onbevoegde toegang tot vertrouwelijke gegevens, wat de integriteit en vertrouwelijkheid van informatie in gevaar brengt; • **Gegevensdiefstal:** Onvoldoende beveiliging kan cybercriminelen in staat stellen om gevoelige gegevens te stelen, wat kan leiden tot financiële verliezen en reputatieschade; • **Fraude:** Medewerkers kunnen misbruik maken van hun toegang tot systemen om frauduleuze activiteiten uit te voeren, zoals het manipuleren van gegevens of het uitvoeren van ongeoorloofde transacties; • **Verlies van gegevensintegriteit:** Als logbestanden niet goed worden beheerd en gecontroleerd, kan dit leiden tot onjuiste of vervalste gegevens, wat de besluitvorming en rapportage kan beïnvloeden; • **Compliance risico's:** Onvoldoende toegangsbeveiliging kan	H ☹	H ☹	1. **Sterke wachtwoordenbeleid:** Beleid dat sterke wachtwoorden vereist en regelmatige wijzigingen van wachtwoorden afdwingt; 2. **Toegangscontrole:** Toegang tot gevoelige bestanden en systemen tot alleen geautoriseerde medewerkers. Gebruik van rolgebaseerde toegangscontrole; 3. **Authenticatie:** Meervoudige authenticatie (MFA) voor extra beveiliging bij toegang tot kritieke systemen; 4. **Monitoring en Logging:** Gedetailleerde logboeken bij van toegang tot systemen en bestanden. Voer regelmatig controles uit op deze logbestanden om verdachte activiteiten op te sporen; 5. **Regelmatige audits:** Periodieke interne audits om de effectiviteit van de toegangsbeveiligingsmaatregelen te controleren en te beoordelen; 6. **Opleiding en bewustwording:** Training voor medewerkers over beveiligingsbewustzijn, waaronder het belang van toegangsbeveiliging en hoe ze verdachte activiteiten kunnen melden; 7. **Incidentenresponsplan:**	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		leiden tot schendingen van regelgeving en wetgeving, wat kan resulteren in juridische gevolgen en boetes; • **Impact op bedrijfscontinuïteit:** Bij een beveiligingsinbreuk kunnen operationele processen verstoord raken, wat leidt tot vertragingen en verhoogde kosten; • **Slechte bedrijfscultuur:** Als medewerkers zich niet verantwoordelijk voelen voor gegevensbeveiliging, kan dit leiden tot een cultuur van onverschilligheid ten opzichte van belangrijke beveiligingsmaatregelen.			Implementatie plan voor het reageren op beveiligingsincidenten, inclusief procedures voor het melden en onderzoeken van datalekken; 8. **Regelmatige evaluatie van beveiligingsmaatregelen:** Regelmatig evaluatie en update van de beveiligingsmaatregelen en -procedures om ervoor te zorgen dat ze effectief blijven tegen nieuwe dreigingen; 9. **Beveiligingssoftware:** Geavanceerde beveiligingssoftware, zoals firewalls en antivirusprogramma's, om systemen te beschermen tegen ongeoorloofde toegang en malware; 10. **Data-encryptie:** Versleuteling gevoelige gegevens, zowel in rust als tijdens verzending, om de impact van eventuele datalekken te minimaliseren.		
Acties voor verbetering Door deze acties te implementeren, kan GGDrU het restrisico effectief verminderen: 1. **Cybersecurity training:** Voer regelmatige trainingen uit voor medewerkers om hen bewust te maken van beveiligingsrisico's en best practices; 2. **Updates van beveiligingssoftware:** Zorg voor tijdige updates en patchbeheer van software en systemen om kwetsbaarheden te minimaliseren; 3. **Geavanceerde beveiligingstechnologie:** Implementeer meerlaagse beveiligingsmaatregelen zoals firewalls, intrusion detection systems (IDS) en encryptie; 4. **Regelmatige beoordelingen:** Voer periodieke audits en assessments uit om de effectiviteit van beveiligingsmaatregelen te evalueren; 5. **Incident response plan:** Ontwikkel en oefen een effectief incident response plan om snel te reageren op beveiligingsinbreuken; 6. **Toegangsbeheer:** Implementeer strikte toegangscontroles en autorisatieprocedures om ongeautoriseerde toegang te voorkomen; 7. **Feedback en verbetering:** Creëer een systeem voor het melden van beveiligingsincidenten en -zwaktes om continue verbetering te waarborgen.							
• Onvoldoende screening van sollicitanten bij indiensttreding, inclusief het ontbreken van een Verklaring Omtrent Gedrag	Ja	• **Fraude en misbruik:** Het aannemen van medewerkers met een geschiedenis van ongepast gedrag kan leiden tot fraude of misbruik van middelen;	M 😐	H ☹️	1. **Strikte Screening Procedures:** Duidelijke richtlijnen voor de screening van sollicitanten, inclusief het vereisen van	M 😐	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
en achtergrondonderzoeken;		• **Reputatieschade:** Negatieve publiciteit kan ontstaan als blijkt dat ongeschikte medewerkers zijn aangenomen, wat het imago van de organisatie schaadt; • **Veiligheidsrisico's:** Medewerkers zonder de juiste achtergrond kunnen een risico vormen voor de veiligheid van collega's en cliënten; • **Onvoldoende kwaliteit:** Het ontbreken van een degelijke screening kan resulteren in een lagere kwaliteit van dienstverlening, omdat ongeschikte kandidaten worden aangenomen; • **Juridische gevolgen:** Er kunnen juridische problemen ontstaan als de organisatie niet voldoet aan de verplichtingen rondom screenings en veiligheidseisen.			Verklaring Omtrent Gedrag (VOG) en achtergrondonderzoeken; 2. **Opleiding van HR-Medewerkers:** Training voor HR-medewerkers over effectieve screeningtechnieken en de juridische aspecten van het aanstellingsproces; 3. **Gebruik van Gestandaardiseerde vragenlijsten:** Gestandaardiseerde vragenlijsten en beoordelingscriteria om de objectiviteit en consistentie van de screening te waarborgen; 4. **Referentiecontroles:** Grondige referentiecontroles bij voormalige werkgevers om inzicht te krijgen in het gedrag en de prestaties van de kandidaat; 5. **Interviewtechnieken:** Training interviewers in effectieve interviewtechnieken om relevante informatie over de geschiktheid van de kandidaten te verzamelen; 6. **Periodieke evaluatie van procedures:** Implementatie en actualisatie screeningprocedures om ervoor te zorgen dat ze voldoen aan de laatste normen en best practices. 7. **Documentatie en archivering:** Goede documentatie en archivering van alle screeningresultaten om transparantie en traceerbaarheid te waarborgen;		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
					8. **Feedback mechanismen:** Systeem voor feedback van medewerkers en leidinggevenden over de effectiviteit van het screeningproces.		
Acties voor verbetering Om het restrisico verder te verlagen, kunnen de volgende verbeteracties worden overwogen: • **Versterken van de VOG-eisen:** Regelmatig herzien van de eisen voor de Verklaring Omtrent Gedrag om ervoor te zorgen dat deze aansluiten bij de actuele risico's binnen de organisatie. • **Gebruik van externe screening diensten:** Overweeg het inschakelen van externe bureaus voor uitgebreide achtergrondcontroles, vooral voor functies met hoge risico's. Dit kan helpen om de screening te versterken en het risico op inadequate aanstellingen verder te verlagen. • **Broker inschakelen:** GGDrU overweegt het inschakelen van een broker om het screeningproces te optimaliseren en om de juiste kandidaten voor specifieke functies te vinden, waardoor de kans op mismatches vermindert. • **Integratie van technologie:** Implementeer geavanceerde software voor het verzamelen en analyseren van achtergrondinformatie, zodat de screening efficiënter en grondiger kan worden uitgevoerd. • **Cultuur van integriteit:** Bevorder een cultuur van integriteit binnen de organisatie waarin medewerkers gestimuleerd worden om mogelijke onregelmatigheden te melden; • **Training en bewustwording:** Organiseer trainingen voor medewerkers over het belang van integriteit en de impact van onjuiste aanstellingen op de organisatie; • **Regelmatige audits van het screeningproces:** Voer periodieke audits uit van het screeningproces om te beoordelen of de procedures effectief zijn en voldoen aan de geldende normen; • **Feedback van medewerkers:** Stimuleer medewerkers om feedback te geven over het screeningproces en eventuele zorgen of ervaringen die zij hebben met nieuwe collega's.							
• Inadequate vastlegging en goedkeuring van nevenactiviteiten;	Ja	• **Conflicten van belang:** Medewerkers kunnen besluiten nemen die niet in het beste belang van GGDrU zijn, wat leidt tot onethisch gedrag of belangenverstrengeling; • **Fraude en misbruik:** Onvoldoende toezicht op nevenfuncties kan medewerkers in staat stellen om ongeoorloofde of frauduleuze activiteiten te	H 	H 	• **Duidelijke Richtlijnen:** Duidelijke richtlijnen voor het registreren en autoriseren van nevenfuncties, inclusief criteria voor acceptatie en rapportageverplichtingen; • **Registratiesysteem:** Centraal systeem voor het registreren van nevenfuncties, waarbij medewerkers verplicht zijn om hun nevenfuncties aan te geven en bij te werken; • **Autorisatieprocessen:** Formeel autorisatieproces waarbij	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		verrichten zonder ontdekking; • **Slechte reputatie:** Onvoldoende registratie kan leiden tot negatieve publiciteit en een beschadigd imago van GGDrU als bekend wordt dat medewerkers nevenfuncties hebben die in strijd zijn met de organisatiebeleid; • **Juridische gevolgen:** Het negeren van het registratieproces kan resulteren in schendingen van wet- en regelgeving, wat juridische repercussies en boetes met zich mee kan brengen; • **Verlies van vertrouwen:** Gebrek aan transparantie in nevenfuncties kan leiden tot een verlies van vertrouwen onder medewerkers en stakeholders, waardoor de organisatiecultuur negatief wordt beïnvloed; • **Onvoldoende toezicht:** Zonder adequate registratie is het moeilijk om het gedrag en de prestaties van medewerkers te monitoren, wat kan resulteren in een afname van de algehele effectiviteit van de organisatie.			nevenfuncties door een leidinggevende of HR-afdeling goedgekeurd moeten worden voordat ze worden aanvaard; • **Regelmatige herzieningen:** Periodieke herzieningen van geregistreerde nevenfuncties om te controleren op naleving en om ervoor te zorgen dat alle functies actueel zijn; • **Training en voorlichting:** Trainingen aan medewerkers over het belang van het registreren van nevenfuncties en de mogelijke gevolgen van onjuiste registratie; • **Toezicht en monitoring:** Toezicht \op de naleving van de richtlijnen, inclusief regelmatige audits van geregistreerde nevenfuncties om onregelmatigheden te identificeren; • **Rapportagemogelijkheden:** Anonieme kanalen waar medewerkers zorgen over niet-geregistreerde nevenfuncties kunnen melden zonder angst voor repercussies; • **Consequenties bij overtredingen:** Duidelijke consequenties voor medewerkers die hun nevenfuncties niet correct registreren of autoriseren, om naleving te bevorderen.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Acties voor verbetering Door deze acties te implementeren, kan GGDrU de registratie en autorisatie van nevenfuncties verbeteren, wat zal bijdragen aan een betere compliance en het verminderen van risico's: 1. **Implementatie van Duidelijke Richtlijnen:** ○ Ontwikkel en communiceer heldere richtlijnen voor de registratie en autorisatie van nevenfuncties, inclusief specifieke verantwoordelijkheden voor medewerkers; 2. **Training en voorlichting:** ○ Bied regelmatige training aan voor medewerkers over het belang van correcte registratie van nevenfuncties en de mogelijke gevolgen van niet-naleving; 3. **Versterking van registratieprocessen:** ○ Introduceer een gebruiksvriendelijk systeem voor het registreren van nevenfuncties, inclusief verplichting tot goedkeuring door een leidinggevende; 4. **Regelmatige audits:** ○ Voer periodieke interne audits uit om de naleving van de registratieprocedures te controleren en eventuele onregelmatigheden tijdig op te sporen. 5. **Monitoring en Rapportage:** ○ Implementeer een monitoringmechanisme dat afwijkingen in de registratie van nevenfuncties in real-time kan signaleren; 6. **Feedback mechanismen:** ○ Creëer anonieme meldpunten waar medewerkers mogelijke onregelmatigheden of twijfels over de registratie kunnen rapporteren; 7. **Vierogenprincipe:** ○ Pas het principe van vierogenprincipe toe bij de autorisatie van nevenfuncties om het risico op ongepaste goedkeuringen te minimaliseren; 8. **Cultuur van transparantie:** ○ Bevorder een organisatiecultuur die open communicatie over nevenfuncties en ethisch gedrag stimuleert; 9. **Continue evaluatie van procedures:** ○ Voer regelmatig evaluaties uit van de bestaande procedures en richtlijnen om ervoor te zorgen dat ze effectief blijven en voldoen aan de behoeften van de organisatie; 10. **Versterking van Toegangscontrole:** • Beperk de toegang tot systemen waar nevenfuncties geregistreerd worden tot alleen geautoriseerde medewerkers.							
• Onvoldoende toezicht op interne beheersingsmaatregelen die bedoeld zijn om de integriteit van de door onderzoeksmedewerkers verzamelde en gebruikte data te waarborgen;	Ja	• **Verlies van datakwaliteit**: Onjuiste of onvolledige gegevens kunnen leiden tot onbetrouwbare onderzoeksresultaten; • **Fraude of manipulatie van data**: Gebrek aan monitoring kan ruimte geven voor ongeoorloofd gedrag, zoals het manipuleren van data; • **Reputatieschade**: Problemen met de integriteit van data kunnen het vertrouwen in de organisatie schaden;	M 	H 	• **Regelmatige evaluaties**: Periodieke beoordelingen van interne beheersingsmaatregelen om hun effectiviteit te waarborgen; • **Training en opleiding**: Trainingen voor medewerkers over het belang van gegevensintegriteit en de rol van interne controles; • **Toegangscontrole**: Beperkte toegang tot onderzoeksdata door geautoriseerde medewerkers en goedkeuringsprocedures; • **Monitoring en rapportage**: Real-time monitoring van onderzoeksdata en gebruik	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		• **Compliance-risico's**: Niet voldoen aan interne en externe regelgeving kan leiden tot juridische en financiële gevolgen.			rapportagetools om afwijkingen snel te signaleren; • **Audits**: Regelmatig interne audits om naleving van beheersingsmaatregelen te controleren en mogelijke tekortkomingen te identificeren; • **Feedback mechanismen**: Anonieme kanalen voor medewerkers om onregelmatigheden of zorgen te rapporteren zonder angst voor repercussies; • **Documentatie en procedures**: Duidelijke richtlijnen en gedetailleerde documentatie van alle processen met betrekking tot gegevensverzameling en -gebruik.		

Door deze acties te implementeren kan GGDrU de effectiviteit van hun interne controles verbeteren en de integriteit van hun onderzoeksdata waarborgen:

1. **Verbeterde opleiding en training**:
   - Regelmatige trainingen voor medewerkers over de procedures voor dataverzameling en -gebruik, inclusief de ethische en wettelijke implicaties van onjuiste gegevensverwerking;
2. **Invoering van geavanceerde monitoringtools**:
   - Implementatie van softwareoplossingen die real-time monitoring van gegevensverzameling en -verwerking mogelijk maken, met meldingen voor afwijkingen;
3. **Versterken van documentatie en rapportage**:
   - Creëren van gedetailleerde richtlijnen en protocollen voor documentatie en rapportage van onderzoeksdata om transparantie en traceerbaarheid te verbeteren;
4. **Regelmatige risicoanalyse**:
   - Voeren van periodieke risicoanalyses om nieuwe of veranderende risico's met betrekking tot gegevensintegriteit tijdig te identificeren en aan te pakken;
5. **Feedbackmechanismen versterken**:
   - Anonieme kanalen voor medewerkers creëren om zorgen of onregelmatigheden te rapporteren, waardoor een cultuur van openheid en verantwoordelijkheid wordt bevorderd;
6. **Audits en evaluaties**:
   - Invoeren van meer frequente interne audits om de naleving van procedures te controleren en om de effectiviteit van bestaande beheersmaatregelen te evalueren;
7. **Toegang en autorisatie**:
   - Het implementeren van strengere toegangscontroles tot gegevens en systemen, zodat alleen geautoriseerde medewerkers toegang hebben tot gevoelige onderzoeksdata;
8. **Cultuur van integriteit bevorderen**:
   - Het bevorderen van een organisatiecultuur waarin ethisch gedrag en dataconsistentie worden gewaardeerd en gestimuleerd;
9. **Communicatie verbeteren**:

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
○ Regelmatig communiceren met medewerkers over de belang van gegevensintegriteit en de gevolgen van non-compliance; 10. **Beleid en Procedures Updaten**: ○ Het regelmatig herzien en actualiseren van beleidsdocumenten en procedures om te zorgen dat deze in lijn zijn met best practices en actuele regelgeving.							
2.2 Rationalisatie		Rationalisatie met betrekking tot de toe-eigening van bedrijfsmiddelen bij GGDrU verwijst naar de rechtvaardigingen die medewerkers gebruiken om ongeoorloofd gebruik van middelen te verantwoorden. Dit kan voortkomen uit persoonlijke rechtvaardiging, groepsdruk, of de perceptie van een lage kans op ontdekking. Medewerkers kunnen denken dat hun gedrag acceptabel is, vooral in een cultuur waar dergelijke praktijken genormaliseerd worden. Dit kan leiden tot financiële verliezen, reputatieschade en een afname van de moraal onder medewerkers. Het is essentieel voor GGDrU om sterke controles en een cultuur van verantwoordelijkheid te bevorderen om deze rationalisaties te voorkomen.					
2.3.1 Het nalaten om risico's rondom het oneigenlijk toe-eigenen van bedrijfsmiddelen te monitoren en beperken, door:		Er is onvoldoende aandacht voor de risico's van ongeoorloofd gebruik van middelen en bedrijfsmiddelen, zoals financiële verliezen, fraude en reputatieschade. Zonder actieve monitoring kunnen medewerkers zich onbestraft gedragen, wat kan leiden tot onverschilligheid of corruptie, en administratieve fouten door onduidelijke procedures. Het is cruciaal voor GGDrU om een proactieve aanpak te hanteren met duidelijke richtlijnen en controles, zodat deze risico's tijdig worden					

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		geïdentificeerd en aangepakt, wat bijdraagt aan een cultuur van integriteit en de effectiviteit van de organisatie waarborgt.					
• Het negeren van interne controles met betrekking tot het ongeoorloofd toe-eigenen van bedrijfsmiddelen door bestaande beheersingsmaatregelen te omzeilen of door geen passende corrigerende acties te ondernemen voor bekende tekortkomingen in deze controles.	Ja	• **Financiële verliezen**: Door onvoldoende controle kan diefstal of misbruik van bedrijfsmiddelen onopgemerkt blijven, wat kan leiden tot aanzienlijke financiële schade; • **Fraude en corruptie**: Zonder effectieve controlemechanismen is er een verhoogd risico op fraude, waarbij medewerkers of derden misbruik kunnen maken van de situatie; • **Reputatieschade**: Het gebrek aan toezicht kan leiden tot incidenten die het vertrouwen van klanten, partners of stakeholders in de organisatie ondermijnen; • **Juridische en compliance risico's**: Het niet naleven van interne beheersingsmaatregelen kan resulteren in juridische problemen of boetes als gevolg van schendingen van wet- en regelgeving; • **Verlies van efficiëntie**: Onvoldoende controle kan leiden tot misbruik van middelen, waardoor de organisatie minder efficiënt werkt en haar doelstellingen niet behaalt.	H 	M 	• **Versterking van interne controles**: Interne controles op gevoelige processen, zoals het beheer van bedrijfsmiddelen, met duidelijke verantwoordelijkheden en bevoegdheden; • **Regelmatige audits**: Periodieke audits om de naleving van interne controles te controleren en afwijkingen vroegtijdig op te sporen; • **Training en Voorlichting**: Trainingen aan medewerkers over het belang van interne controles en de gevolgen van het omzeilen van deze maatregelen; • **Incidentenrapportage**: Transparant rapportagesysteem waar medewerkers zonder repercussies interne tekortkomingen of overtredingen kunnen melden; • **Monitoring en Evaluatie**: Continu monitoringsysteem om de effectiviteit van controles te volgen en regelmatige evaluaties uit te voeren voor verdere verbetering; • **Duidelijke consequenties voor overtredingen**: Consequenties voor het overtreden of negeren van interne controles om een cultuur van naleving te bevorderen.	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Acties voor verbetering Door deze verbeteringen door te voeren, kan GGDrU het restrisico verder terugdringen: 1. **Versterking van de interne audits**: Voer vaker onaangekondigde en grondige interne audits uit om naleving van beheersmaatregelen te controleren; 2. **Verbeterde technologie-implementatie**: Gebruik geavanceerde monitoringsoftware die real-time rapportage en meldingen geeft van verdachte activiteiten met betrekking tot bedrijfsmiddelen; 3. **Continu bewustzijn**: Organiseer regelmatig bewustwordingscampagnes en training voor medewerkers om hen te blijven informeren over het belang van interne controles en de gevolgen van niet-naleving; 4. **Verbeterde follow-up op incidenten**: Zorg voor een snellere en effectievere afhandeling van bekende tekortkomingen en geïdentificeerde incidenten; 5. **Verhoogde transparantie en communicatie**: Maak rapportages over risico's en interne controles transparant voor medewerkers, zodat ze meer betrokken worden bij het naleven van de richtlijnen.							
• Gedragingen die wijzen op onvrede of ontevredenheid over de organisatie en de manier waarop medewerkers handelen	Ja	• **Verlies van werknemers**: Ontevreden medewerkers zijn eerder geneigd de organisatie te verlaten, wat kan leiden tot hoge personeelsverloop en kosten voor werving en training van nieuw personeel; • **Verminderde productiviteit**: Onvrede kan leiden tot demotivatie en lagere productiviteit, wat de algehele prestaties van de organisatie schaadt; • **Slechte teamdynamiek**: Ongelukkige medewerkers kunnen een negatieve invloed hebben op teamgeest en samenwerking, wat kan leiden tot conflicten en een minder effectieve werkomgeving; • **Reputatieschade**: Negatieve ervaringen van medewerkers kunnen zich verspreiden, zowel intern als extern, wat het imago van de organisatie kan schaden en het moeilijker maakt om talent aan te trekken; • **Meer klachten**: Medewerkers die ontevreden zijn, kunnen eerder	H 	M 	• **Regelmatig medewerkers-enquêtes**: Regelmatig enquêtes om de tevredenheid en betrokkenheid van medewerkers te meten en feedback te verzamelen; • **Open communicatiekanalen**: Platforms waar medewerkers vrijuit hun zorgen en ideeën kunnen delen zonder angst voor repercussies**;** • **Feedbacksessies**: Periodieke feedbacksessies om medewerkers de gelegenheid te geven om hun mening te geven over beleid en procedures; • **Opleiding en Ontwikkeling**: Trainingen gericht op persoonlijke ontwikkeling en loopbaanplanning om de betrokkenheid te vergroten; • **Erkenning en beloning**: Programma's voor het erkennen en belonen van medewerkers voor hun bijdragen en prestaties; • **Teambuildingactiviteiten**: Activiteiten die de teamgeest bevorderen en de samenwerking tussen medewerkers verbeteren; • **Intranet en nieuwsbrieven**:	M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		klachten indienen, wat kan leiden tot een grotere administratieve last en mogelijk juridische problemen; • **Risico op ongeoorloofd gedrag**: Onvrede kan leiden tot een cultuur waarin medewerkers zich minder verantwoordelijk voelen voor de bedrijfsmiddelen van de organisatie, wat het risico op ongeoorloofd gedrag of fraude vergroot; • **Schade aan klantrelaties**: Ontevreden medewerkers kunnen een negatieve impact hebben op de service en interactie met cliënten, wat kan leiden tot ontevreden klanten en verlies van zakelijke kansen; • **Slechte innovatie**: Een ontevreden personeelsbestand kan minder geneigd zijn om nieuwe ideeën en verbeteringen voor te stellen, wat innovatie en groei in de organisatie kan belemmeren.			Gebruik van intranet en nieuwsbrieven om medewerkers op de hoogte te houden van organisatie-ontwikkelingen en successen; • **Mentorschapsprogramma's**: Mentorschap om nieuwe medewerkers te begeleiden en hun integratie te vergemakkelijken; • **Monitoring van werkdruk**: Zorgen voor evenwichtige werkverdeling om burn-out te voorkomen; • **Cultuur van vertrouwen**: Cultuur van vertrouwen en respect waarin medewerkers zich veilig voelen om hun zorgen te uiten.		
Acties voor verbetering Door deze acties te implementeren, kan GGDrU de onvrede onder medewerkers aanpakken en een positievere werkomgeving creëren. • **Medewerkerstevredenheidsonderzoeken**: Voer regelmatig enquêtes uit om de tevredenheid van medewerkers te meten en inzicht te krijgen in hun zorgen en verwachtingen; • **Open communicatiekanalen**: Creëer platforms waar medewerkers openlijk hun feedback en suggesties kunnen delen, zodat ze zich gehoord voelen; • **Feedback en verbeteracties**: Neem de resultaten van de tevredenheidsonderzoeken serieus en ontwikkel actieplannen om de aangeduide problemen aan te pakken; • **Leiderschapstraining**: Train leidinggevenden in effectieve communicatie en empathisch leiderschap, zodat zij beter kunnen inspelen op de behoeften van hun teamleden; • **Erkenning en beloning**: Implementeer een erkenningsprogramma om medewerkers te belonen voor hun inzet en positieve bijdragen, wat kan helpen om de moraal te verhogen; • **Loopbaanontwikkeling**: Bied mogelijkheden voor professionele ontwikkeling en loopbaanplanning om medewerkers te helpen groeien binnen de organisatie. • **Conflictbeheersing**: Zorg voor training in conflictbeheersing en mediatie om eventuele geschillen op de werkvloer snel en effectief op te lossen; • **Persoonlijke gesprekken**: Stimuleer managers om regelmatig persoonlijke gesprekken te voeren met teamleden om hun welzijn en tevredenheid te monitoren.							
• Het tolereren van kruimeldiefstal	Ja	**Escalatie naar grotere fraude:** • Wanneer kleine diefstallen worden getolereerd, kunnen	H 	H 	• **Bewustwordingscampagnes:** Campagnes om medewerkers bewust te maken van de impact van diefstal en	L tot M 	Ja

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Het tolereren van kruimeldiefstal verwijst naar een situatie waarin kleine, ogenschijnlijk onbenullige diefstallen of ongeoorloofd gebruik van middelen binnen een organisatie worden genegeerd of niet serieus worden genomen. Dit kan zich uiten in bijvoorbeeld het stelen van kantoorbenodigdheden, kleine geldbedragen, of het onterecht gebruiken van bedrijfseigendommen.		medewerkers zich aangemoedigd voelen om ernstigere diefstal of frauduleuze activiteiten uit te voeren, wat leidt tot grotere verliezen voor de organisatie; **2. Verlies financiële middelen:** • De cumulatieve kosten van kruimeldiefstal kunnen na verloop van tijd aanzienlijk oplopen, wat kan resulteren in financiële verliezen die de begroting en middelen van GGDrU onder druk zetten; **3. Slechte bedrijfscultuur:** • Het tolereren van ongeoorloofd gedrag kan leiden tot een cultuur van onverschilligheid en wantrouwen, waar medewerkers zich niet verantwoordelijk voelen voor de bedrijfsmiddelen van de organisatie en niet het gevoel hebben dat ze bijdragen aan de organisatie; **4. Negatieve impact op houding:** • Medewerkers die hard werken en zich aan de regels houden, kunnen gefrustreerd raken door het feit dat anderen profiteren van onethisch gedrag zonder consequenties, wat kan leiden tot een daling van de motivatie en betrokkenheid; **5. Reputatieschade:** • Het publieke imago van GGDrU kan worden geschaad			de ethische normen die binnen de organisatie gelden; • **Strikte handhaving van beleid:** Duidelijke richtlijnen en procedures met betrekking tot diefstal en ongeoorloofd gedrag, inclusief sancties voor overtreders; • **Monitoring en toezicht:** Regelmatig controles op bedrijfsmiddelen om verdachte activiteiten tijdig op te sporen en aan te pakken. • **Rapportage mechanismen:** Anonieme meldpunten waar medewerkers ongeoorloofd gedrag kunnen rapporteren zonder angst voor repercussies; • **Training en Opleiding:** Trainingen aan medewerkers over de gevolgen van kruimeldiefstal en het belang van ethisch gedrag binnen de organisatie; • **Vierogenprincipe**: Vierogenprincipe bij belangrijke transacties en goedkeuringen om de kans op ongeoorloofd gedrag te verkleinen; • **Regelmatig audits:** Periodieke interne audits uit om de naleving van de richtlijnen te controleren en eventuele onregelmatigheden tijdig op te sporen; • **Cultuur van integriteit:** Cultuur waarin medewerkers zich verantwoordelijk voelen voor de bedrijfsmiddelen van de organisatie en worden aangemoedigd om elkaar aan te spreken op onethisch gedrag; • **Versterking van Toegangscontrole:**	😐	

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
		als bekend wordt dat er ongeoorloofd gedrag plaatsvindt en niet wordt aangepakt, wat het vertrouwen van cliënten en stakeholders kan ondermijnen; **6. Toegenomen administratieve lasten:** • Het niet aanpakken van kruimeldiefstal kan leiden tot een grotere administratieve last, aangezien de organisatie meer tijd en middelen moet besteden aan het toezicht houden op bedrijfsmiddelen en het oplossen van gerelateerde problemen; **7. Compliance risico's:** • Afhankelijk van de aard van de bedrijfsmiddelen die worden gestolen, kan het tolereren van kruimeldiefstal ook leiden tot schendingen van regelgeving of compliance-vereisten, wat kan resulteren in juridische repercussies of boetes; **8. Afname van efficiëntie:** • De focus op het omgaan met de gevolgen van ongeoorloofd gedrag kan afleiden van de dagelijkse operaties, waardoor de algehele efficiëntie en effectiviteit van de organisatie in gevaar komen.			Toegang tot waardevolle bedrijfsmiddelen en middelen tot alleen die medewerkers die dit echt nodig hebben voor hun werk; • **Continue Evaluatie van Procedures:** Regematig evaluatie van bestaande procedures en maatregelen om ervoor te zorgen dat deze effectief blijven in het voorkomen van kruimeldiefstal en andere vormen van ongeoorloofd gedrag.		

Risicofactoren	Zijn er potentiële fraude-risico's te identificeren? Ja/Nee	Omschrijving potentiële fraude-risico's	Kans (H, M, L)	Impact (H, M, L)	Welke interne beheersmaatregelen zijn getroffen?	Rest-risico (H, M, L)	Actie vereist?
Acties voor verbetering Door deze acties te implementeren, kan GGDrU de risico's van kruimeldiefstal verder beperken en een sterke cultuur van verantwoordelijkheid en transparantie binnen de organisatie bevorderen: 1. **Versterking van interne communicatie**: ○ Regelmatige updates over de impact van kruimeldiefstal en de status van beleidshandhaving; 2. **Verbeterde technologie**: ○ Investeren in geavanceerde bewakingssystemen en software om verdachte activiteiten sneller te detecteren; 3. **Betrekken van leidinggevenden**: ○ Leidinggevenden verantwoordelijk maken voor het monitoren van teamgedrag en het bevorderen van een cultuur van integriteit; 4. **Exit-interviews**: ○ Voer exit-interviews uit om te begrijpen waarom medewerkers de organisatie verlaten en of er zorgen zijn over diefstal of andere ongeoorloofde praktijken; 5. **Versterking van procedures voor ongeoorloofd gedrag**: ○ Zorg voor duidelijk gedefinieerde en breed gecommuniceerde gevolgen voor kruimeldiefstal en andere vormen van fraude; 6. **Regelmatig cultuurevaluatie**: ○ Voer periodieke evaluaties uit van de organisatiecultuur om ervoor te zorgen dat integriteit en ethisch gedrag worden bevorderd.							

GGD regio Utrecht
Postbus 51
3700 AB Zeist

T 030 608 608 6
E info@ggdru.nl
I www.ggdru.nl

Uitgave
© GGD regio Utrecht
November 2027

GGD
regio Utrecht