

Managementresponse op de aanbevelingen van de accountant boardletter 2020

Gemeente Raalte

Algemeen:

Zoals de accountant in de aanbestedingsbrief van de boardletter aangeeft dienen zijn bevindingen en aanbevelingen te worden gelezen als constructieve aanwijzingen voor het college van burgemeester en wethouders, Dit helpt ons in het continue proces van het verbeteren van de beheersing van de bedrijfsvoering en de kwaliteit van de jaarrekening.

Wij zijn blij te lezen dat de accountant onderkent dat meerdere acties in gang zijn gezet om de interne beheersing verder te versterken wat ook door de accountant wordt gezien als positieve ontwikkeling.

Daarnaast doet de accountant een aantal aanbevelingen om het continue proces van leren en verbeteren verder uit te nutten. Hierover hebben we het gesprek met de accountant gevoerd tijdens de bespreking van de boardletter op 13 januari 2021. Wat hebben wij nog te doen om de (al eerder) door de accountant gedane aanbevelingen op het niveau te krijgen van 'bevinding opgelost/ beheersing voldoende'. Aandachtspunt hierbij is ook dat de te leveren inspanning in verhouding staat tot het risico dat gemitigeerd kan worden.

- **Aanbeveling 1:**

Verantwoordelijk directielid	Mark Duijtshoff
Eigenaar	Tamar Schror
Actiehouder	Gert-Jan Kikkert / Marjon Veldkamp

Funcitiescheiding sociale uitkeringen en verstrekkingen:

Zie Pagina 14:

Aanbevelingen

Wij adviseren het college om het proces van het verstrekken van sociale uitkeringen en verstrekkingen zo in te richten dat te allen tijde een tweede functionaris de aanvraag/beschikking moet autoriseren. Zodat bij toekomstige uitkeringen en verstrekkingen altijd sprake is van het "4 ogen principe". Voor de sociale uitkeringen in geld (Tozo-uitkeringen) en sociale verstrekkingen in natura aan personen (PGB, WMO en Jeugd) in 2020 vragen wij de gemeente om een Verbijzonderde Interne Controle (VIC) uit te voeren om vast te stellen of de lasten juist en rechtmatig zijn.

Management response:

Wij hebben intern een aantal afspraken gemaakt over de wijze waarop we het '4 ogen principe' toepassen: dit komt terug in casuïstiek overleg, collegiale afstemming, toetsing van tijdelijke medewerkers en een inwerktraject bij nieuwe medewerkers. Ook is er uiteraard een funcitiescheiding tussen de collega die een besluit neemt en de collega die dit besluit (administratief) verwerkt.

Wij begrijpen echter het punt dat het 4-ogen principe in veel gevallen niet zichtbaar wordt vastgelegd. Wij zullen deze aanbeveling dan ook verwerken in de inrichting van onze processen vanaf 2021.

Verder voert Deloitte een VIC uit binnen ons domein voor de PW en de IOAW over 2020. Wanneer u aanbeveelt dat wij aanvullende controles hierop uit moeten voeren, zullen we deze aanbeveling ook meenemen bij het bepalen van onze interne controles over 2021. Aanvullende controles betreffende TOZO en Sociale zaken t.b.v. 2020 worden uitgevoerd door Deloitte.

- **Aanbeveling 2:**

Verantwoordelijk directielid	Mark Duijtshoff
Eigenaar	Mieke Lammerts van Bueren
Actiehouder	Gerald van Rooij

Functiescheiding inkoopproces:

Zie Pagina 15:

Aanbeveling

Wij adviseren de budgetlimieten te verwerken in de digitale workflow, zodat bij een overschrijding deze facturen automatisch worden doorgestuurd naar een tweede medewerker voor akkoord. Ook adviseren wij de digitale workflow zo in te richten dat te allen tijde een tweede functionaris de factuur autoriseert. Voor de lasten in het boekjaar 2020 vragen wij het college een data-analyse op de lasten en de uitputting van de budgetten uit te voeren om vast te stellen of aan de budgethoudersregeling is voldaan en de inkopen rechtmatig zijn.

Management response:

Het risico wordt onderkend en op dit moment voeren we reeds aanvullende gegevensgerichte controles uit om dit risico te mitigeren. In DOWR-verband gaan we in 2021 nog nader onderzoeken of deze systeemcontrole realiseerbaar is.

Ten aanzien van de aanbeveling om te allen tijde een tweede functionaris een inkoopfactuur te laten autoriseren: dit kan een aanbeveling zijn indien de prestatieakkoordverklaarder ook fiatteert in de rol van budgethouder. Het is de vraag of de extra inspanning die hiervoor nodig is opweegt tegen het risico dat wordt genoemd. Vooreerst adviseren wij geen prioriteit aan dit onderdeel van de aanbeveling te geven en dit te betrekken bij de verdere doorontwikkeling van de VIC's in het kader van de verdere kwaliteitsverbetering/rechtmatigheidsverantwoording door het college.

Ten aanzien van het afdwingen van functiescheiding en limieten: In de praktijk wordt hier op gestuurd, maar systeemtechnisch niet afgedwongen. Er zijn inkoopadviseurs beschikbaar. Zij beoordelen ook de opzet, bestaan en werking. Daarom adviseren wij vooralsnog te steunen op de gevraagde data-analyse en in 2021 nader onderzoek te doen naar de systeemtechnische mogelijkheden voor afdwingen van functiescheiding en budgetlimieten

- **Aanbeveling 3:**

Verantwoordelijk directielid	Mark Duijtshoff
Eigenaar	Mieke Lammerts van Bueren
Actiehouder	Henk Ruigrok / Anne Denissen

Rechtmatigheid EU-aanbestedingen:

Zie Pagina 16:

Aanbeveling

Wij adviseren u verdere preventieve beheersmaatregelen te implementeren waardoor gewaarborgd wordt dat inkopen rechtmatig worden aanbesteed. Deze preventieve beheersmaatregelen kunnen bestaan uit:

- Afdwingen dat voor iedere inkoop een verplichting wordt aangemaakt. Dit kan worden gehandhaafd door geen facturen van leveranciers te accepteren waar geen verplichtingenummer op is weergegeven;

- Bestellingen boven een grensbedrag, die passend is binnen het aanbestedingsbeleid van de gemeente, automatisch via de inkoopadviseur in de workflow laten lopen zodat een aanbestedingsadvies ingewonnen wordt voor grote inkopen.

Management response:

In de 2e alinea van de observatie op pagina 16 van de boardletter wordt melding gemaakt van een aanbesteding in DOWR verband van een centraal contractenregister. Die opmerking wordt niet direct herkend, er loopt niet een dergelijke aanbesteding. Dit onderwerp zal als aandachtspunt meegenomen worden in een op termijn te starten aanbesteding van een nieuw financieel systeem. Zover is het echter nog niet.

Punt 1: het afdwingen van het vastleggen van een verplichting zien we niet direct als middel om de rechtmatigheid van een inkooptraject beter te waarborgen. Het vastleggen van een verplichting gebeurt immers ook pas na een inkooptraject is doorlopen, dus achteraf. Vanuit rechtmatigheid van EU-aanbestedingen zien we hierin niet direct toegevoegde waarde. Het gemeente breed afdwingen dat voor iedere inkoop een verplichting wordt aangemaakt brengt veel extra werkzaamheden met zich mee en zien wij op dit moment nog niet in verhouding staan tot het mogelijk risico dat hierbij kan worden gemitigeerd.

Punt 2: het automatisch via een workflow afdwingen dat een inkoopadviseur wordt betrokken bij grotere aanbestedingen is een herkenbaar advies vanuit voorgaande jaren. Het risico dat hiermee samenhangt wordt wel onderkend.

Er werden de afgelopen jaren geen onrechtmatigheden geconstateerd m.b.t. EU-aanbestedingen en daarmee lijken de huidige procedures te voldoen. Wij zien op dit moment dan ook geen aanleiding voor meer preventieve maatregelen zoals het automatisch (dus via een systeem) in een workflow opnemen van een advies van de inkoopadviseur. Wel gaan we in 2021 nader onderzoek doen naar mogelijkheden om preventieve maatregelen toe te passen in dit proces.

• Aanbeveling 4:

Verantwoordelijk directielid	Mark Duijthoff
Eigenaar	Mieke Lammerts van Bueren
Actiehouder	Gerald van Rooij

Memoriaal boekingen:

Zie Pagina 17:

Aanbeveling

Wij hebben reeds vastgesteld dat u stappen heeft gezet om bovenstaand risico te mitigeren. Echter dekken geen van de door u geïmplementeerde beheersmaatregelen het risico in zijn geheel af. Wij adviseren u om de periodieke analyse van de functiescheiding binnen de memoriaalboekingen verder te versterken om het risico achteraf volledig te mitigeren. Dit door alle memoriaalboekingen te betrekken in de analyse en de analyse uit te laten voeren door een onafhankelijke medewerker. Daarnaast adviseren wij u om te onderzoeken of het risico ook preventief aan de voorkant van het proces kan worden beheerst. Bijvoorbeeld door de functiescheiding in de financiële administratie te implementeren zodat een inhoudelijke controle voorafgaand aan het doorboeken van de memoriaalboeking afgedwongen wordt.

Management response:

Het risico van het doorvoeren van onjuiste memoriaalboekingen en daarmee het risico van niet consistente informatieverschaffing wordt onderkend. Het advies van analyse door een onafhankelijke medewerker en nader onderzoek voor preventieve maatregelen zal in 2021 verder worden opgepakt.

Voor de beeldvorming hieronder een weergave van het proces en gemaakte verbeter slagen:

Er is zeker sprake van een functiescheiding tussen het registreren en boeken van memoriaalboekingen in de financiële administratie. Vanuit de gemeente Raalte worden memorialen mét bijlagen geregistreerd in het financiële systeem. DOWR FA heeft de functionaliteit om de aangeleverde memoriaalboekingen (ná controle) te boeken in de financiële administratie. Deze functionaliteit is decentraal niet beschikbaar. Vanuit dit werkproces is in 2020 een verbeter slag doorgevoerd. De bijlagen bij een memoriaalboeking moeten de kern van de boeking

raken waardoor de juistheid van de boeking bewaakt kan worden door degene die de verwerking van de boeking voor zijn of haar rekening neemt.

In 2020 is bij één boeking geconstateerd dat het mogelijk was om decentraal een memoriaalboeking te boeken in de financiële administratie. Dit bleek mogelijk bij het simuleren van een boeking. Ná constatering is dit direct in het financieel systeem aangepast. Deze functionaliteit is niet meer beschikbaar.

- **Aanbeveling 5:**

Verantwoordelijk directielid	Mark Duijthoff
Eigenaar	Tamar Schror
Actiehouder	Gert-Jan Kikkert

Data-analyse sociaal domein:

Zie Pagina 19:

Aanbeveling

Wij adviseren het college de ontwikkelingen met betrekking tot data-analyses voort te zetten en verder te optimaliseren om zo de lasten in het sociaal domein te (blijven) beheersen. Data-analyse helpt om de juiste vragen te stellen die leiden tot meer inzicht in de ontwikkeling en uitvoering van de zorg. Bijvoorbeeld door het verkrijgen van inzichten in de ontwikkeling van de zwaarste, duurste en meest ingrijpende interventies.

Managementresponse:

Wij zijn het eens met uw standpunt om zo optimaal mogelijk gebruik te maken van de beschikbare data binnen ons domein om daar waar mogelijk te kunnen sturen op de risico's en lasten binnen het sociaal domein. Hoewel we het genoemde lokale dashboard en bijbehorende analyses nog aan het optimaliseren zijn, geeft de beschikbare data ons al wel inzicht in bepaalde trends en ontwikkelingen. Deze inzichten nemen we uiteraard ook nu al mee in onze sturing.

Tot slot zijn we in vergaand overleg met betrekking tot het duiden van onze regionale jeugdmonitor om zo ook op regionaal niveau inzicht in onze (lokale) cijfers te krijgen.

Het advies van de accountant om de ontwikkelingen met betrekking tot data-analyses voort te zetten en verder te optimaliseren volgen we dan ook graag op.

- **Aanbeveling 6:**

Verantwoordelijk directielid	Mark Duijthoff
Eigenaar	Mieke Lammerts van Bueren
Actiehouder	Hans Scholtheis

Algemene IT-beheersmaatregelen:

Zie Pagina 20:

Aanbeveling

Ondanks de positieve ontwikkeling in de afgelopen jaren concluderen wij dat de opzet en het bestaan van de General IT Controls op een aantal vlakken verbeterd kan worden. In het bijzonder vragen wij aandacht voor:

1. De interne beheersing van de beheertaken rondom SAP na uitbesteding naar Pink Roccade. De gemeente blijft verantwoordelijk voor een adequate beheersing van de systemen. Wij hebben begrepen dat met Pink Roccade een SLA is afgesloten. Echter naar aanleiding van ons gesprek tijdens de interim-controle is gebleken dat de afspraken nog niet in lijn zijn met de verwachtingen van de DOWR-gemeenten en de DOWR- I onderzoekt momenteel de mogelijkheden om nieuwe afspraken te maken. Daarnaast adviseren wij periodiek de naleving van de afspraken (inclusief verantwoording van Pink Roccade aan de gemeente) vast te stellen, de ISAE3402-rapportage is hiervoor het meest geëigende middel. Wij hebben begrepen dat deze aanbeveling inmiddels is opgepakt en van Pink Roccade een ISAE3402-rapportage zal worden ontvangen.

2. Verbeteren van de beheersing van het rechtenbeheer binnen de financiële applicaties. Wij hebben geconstateerd dat de gemeente diverse alternatieve beheersmaatregelen getroffen heeft om de risico's van het doorbreken van de controle technische functiescheiding rondom kritische processen (zoals betalingen) te mitigeren. Wij adviseren een risicoanalyse op te stellen waarin de risico's binnen de kritische processen worden beschreven en daarbij te bepalen of de huidige set van beheersmaatregelen afdoende is om deze risico's te mitigeren.

Management response:

- Punt 1: Wij herkennen de aanbeveling en daarom wil DOWR-i met de desbetreffende teams de bevinding m.b.t. contracten oplossen.
- Punt 2: Wij zijn ons bewust dat als gevolg van de beperkingen van het huidige financiële systeem wij niet alle risico's kunnen afdekken. Binnen de huidige mogelijkheden blijven wij continu alert op risico's en kansen voor het doorvoeren van verbeteringen. Onze focus ligt verder op het ervoor zorgen dat de huidige risico's en beperkingen worden meegenomen in een volgende aanbesteding van het financiële systeem welke in 2021 van start gaat en waarbij het nieuwe financieel systeem vanaf 1-1-2023 operationeel is.

Over het rechtenbeheer (met name het minimaliseren van het risico van accounts met hoge rechten in SAP) heeft DOWR-i eerder dit jaar op een constructieve manier gesproken met Deloitte.

Samen met technisch/functioneel beheer en Deloitte is een oplossing uitgewerkt die naar tevredenheid van alle partijen zou moeten zijn. De uitgewerkte oplossing was het RACI model.

In goed overleg is besloten dat dit niet de gewenste oplossing is.

In de huidige bevinding staat dat er interne maatregelen genomen moeten worden om de rechtenstructuur te borgen, en dat er aanvullende analyses uitgevoerd moeten worden.

Dit verrast ons omdat:

- DOWR-i reeds interne controles uitvoert op de rechten van users. De verantwoordelijkheden hierbij zijn ook benoemd.
- De aanbeveling om naar kritische processen te kijken en daarop analyses uit te voeren nieuw is. DOWR-i pakt deze bevindingen graag op.

Daarom willen we graag in samenspraak met DOWR-i, in gesprek gaan met Deloitte om hier invulling aan te geven.

Aanbeveling 7:

Verantwoordelijk directielid	Mark Duijtshoff
Eigenaar	Mieke Lammerts van Bueren
Actiehouder	Hans Scholtheis

Cybersecurity:

Zie Pagina 21:

Aanbeveling

Voor de doorontwikkeling van de beheersing van de cybersecurity risico's vragen wij nog aandacht voor:

1. In het informatiebeveiligingsbeleid van de gemeente zijn de doelstellingen beschreven die op basis van de BIO zijn opgesteld en vastgesteld door het college. Uw gemeente heeft in 2020 een aftrap gemaakt in het formuleren van kritieke prestatie-indicatoren (KPI) om de realisatie van de doelstellingen te toetsen. Het verdient de aanbeveling deze KPI's te formaliseren zodat periodiek de voortgang van het behalen van de doelstellingen door de gemeente getoetst kan worden.

2. Het voortzetten van het huidige plan in de doorontwikkeling van het Security Information & Event Management om de detectie en response op cybersecurity issues te versterken. Wij benadrukken het belang van de SIEM en de tijd en aandacht die benodigd is om tot een effectieve implementatie hiervan te komen.

Tenslotte geven wij nog het volgende mee: In 2020 is op basis van risicoclassificatie een analyse uitgevoerd op externe partijen die een belangrijke rol spelen in de IT-beheersing van de gemeente. Wij raden aan deze analyse uit te breiden naar het volledige spectrum van externe partijen die relevant zijn voor de IT-beheersing. Daarnaast raden wij aan om contractmanagement DOWR-I een vast onderdeel te maken van het beslissingsproces bij nieuwe contracten en dit te waarborgen in procedures.

Management response:

De benoemde risico's worden onderkend. De eerste twee bevindingen nemen we ter harte. De 3e bevinding wordt besproken met DOWR-i om te bepalen hoe inhoud geven kan worden aan dit advies.