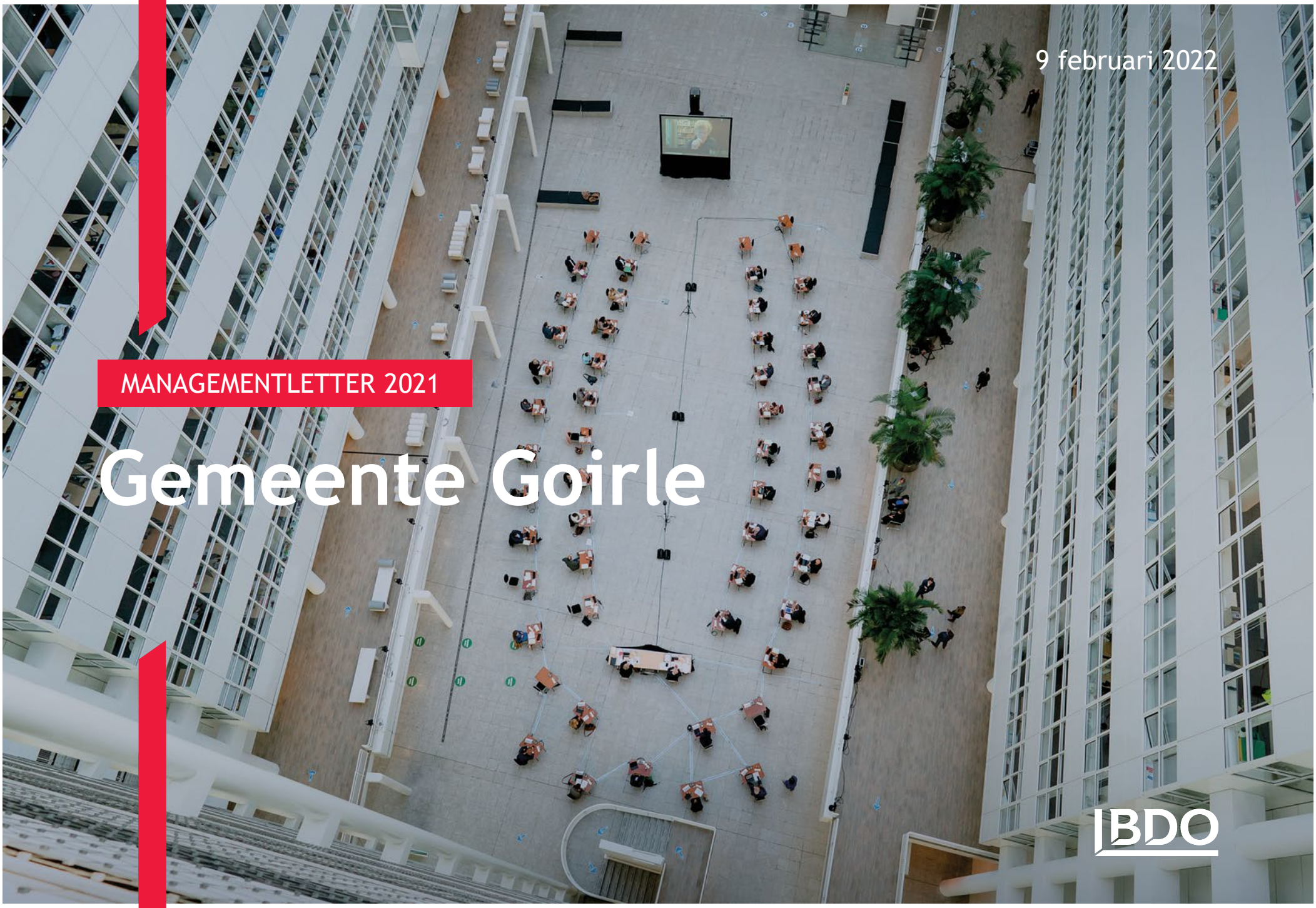


9 februari 2022

MANAGEMENTLETTER 2021

Gemeente Goirle

BDO

Aanbiedingsbrief

Aan het college van burgemeester en wethouders
van de gemeente Goirle
Postbus 17
5050 AA GOIRLE

Tilburg, 9 februari 2022

Kenmerk: NBo/DMe/MvdB/1036018/2205054

Geacht college,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2021 van de gemeente Goirle brengen wij u met deze managementletter verslag uit over onze bevindingen naar aanleiding van onze interim-controle.

Voor een nadere omschrijving van onze opdracht, de reikwijdte en aanpak van onze controle en overige afspraken verwijzen wij naar onze opdrachtbevestiging d.d. 7 september 2021.

In deze rapportage richten wij ons met name op mogelijke verbeterpunten in de bedrijfsvoering en de processen die wij hebben onderzocht in het kader van de controle van de jaarrekening. Onze managementletter is daarom van nature kritisch van aard. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelf controlerend vermogen van uw organisatie.

Als gevolg van de aanhoudende coronacrisis zijn wij helaas beperkt in staat geweest om bij u op locatie te komen waardoor wij veel digitaal hebben moeten afstemmen. Ondanks de minder persoonlijke en directe contacten is de interim-controle en samenwerking goed verlopen.

Wij willen de organisatie bedanken voor de prettige samenwerking en vertrouwen erop u met deze managementletter naar aanleiding van onze interim-controle 2021 van dienst te zijn geweest. Wij zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,

BDO Audit & Assurance B.V.
namens deze,

drs. D.O. Meeuwissen RA

VORIGE PAGINA
VOLGENDE PAGINA
INHOUDSOPGAVE
DASHBOARD

Inhoudsopgave

1. DASHBOARD

2. ONTWIKKELINGEN & ACTUALITEITEN

3. INTERNE BEHEERSING

4. BEVINDINGEN SIGNIFICANTE PROCESSEN

5. IT-BEHEERSING

6. VOORUITBLIK JAARREKENING 2021

1. Dashboard

1.1 Dashboard interim-controle

1.1 Dashboard interim-controle

ACTUALITEITEN - WET- EN REGELGEVING

- Boekjaar 2022 is het eerste jaar van de rechtmatigheidsverantwoording. Na een intensief jaar met corona is er nu ruimte ontstaan om de invoering van de rechtmatigheidsverantwoording (met ingang van 2022) goed voor te bereiden. Wij denken graag met u mee.
- Met de publicatie van de kadernota 2022 (augustus 2021) kan de organisatie verdere invulling geven aan de rechtmatigheids-verantwoording. Hierin worden diverse aspecten van de rechtmatigheidsverantwoording aan de orde gesteld middels aanbevelingen maar ook stellige uitspraken. Wij adviseren het college en de raad met elkaar in gesprek te blijven over de invoering van de rechtmatigheidsverantwoording.
- De komende jaren zal vanuit de accountantscontrole nog nadrukkelijker aandacht worden gegeven aan fraudepreventie, waarbij ook de rol van bestuurders en toezichthoudende organen, zoals de gemeenteraad, bij het voorkomen en detecteren van fraude aan de orde komt. Dit vraagt om actief toezicht op risico's en beheersmaatregelen ter voorkoming van fraude en aandacht voor onder andere de verantwoordelijkheden en termijnen voor de opvolging van aanbevelingen.

ACTUALITEITEN - CORONA & SOCIAAL DOMEIN

- Vorig jaar hebben wij samen met u veel aandacht besteed aan de gevolgen van de coronacrisis. De impact bleek voor de meeste gemeenten mee te vallen. Desondanks is het zaak alert te blijven op de ontwikkelingen en de financiële afwikkeling van de coronacrisis.
- Binnen Wmo begeleiding is (net als bij huishouding) het in strijd met het rechtszekerheidsbeginsel indien in de beschikking de hoeveelheden c.q. tijdseenheden ontbreken. Wij hebben vastgesteld dat uw gemeente resultaatgerichte indicaties voor begeleiding afgeeft en adviseren u passende maatregelen te nemen voor wat betreft toekomstige indiceringen.
- Per 1 januari 2022 wijzigt het woonplaatsbeginsel in de Jeugdwet naar de woonplaats waar de jeugdige staat ingeschreven op het moment van de zorgvraag. Wij adviseren u de effecten van deze wetswijziging in kaart te brengen en uw organisatie op de veranderende werkwijze voor te bereiden.
- Voor de invoering van de nieuwe Wet inburgering zijn twee handreikingen verschenen. Wij adviseren kennis te nemen van beide handreikingen en waar nodig actie te ondernemen.

INTERNE BEHEERSING

- Wij komen tot de conclusie dat uw administratieve organisatie en interne beheersing (AO/IB) binnen de belangrijkste processen, voor zover relevant voor de controle van de jaarrekening, ten aanzien van de controletechnische functiescheiding voldoet.
- Binnen deze processen is sprake van interne beheersmaatregelen. Deze maatregelen worden echter niet altijd toereikend genoeg vastgelegd, waardoor achteraf niet toetsbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd.
- Omdat de AO/IB niet altijd goed is opgezet, bestaat of goed werkt, kunnen wij voor wat betreft de insteek van onze controle niet volledig op de processen steunen en bestaat onze controleaanpak overwegend uit gegevensgerichte werkzaamheden. Deze situatie is ongewijzigd ten opzichte van voorgaand controlejaar.
- Zie hieronder voor onze detailbevindingen met betrekking tot de significante processen.

BEVINDINGEN SIGNIFICANTE PROCESSEN

- Gemeentelijke belastingen en heffingen:
  - Gezien de problematiek rondom TOG en als gevolg hiervan de beëindiging van de dienstverleningsovereenkomst vragen wij uw aandacht voor een zorgvuldige en tijdige (financiële) afwikkeling voor het boekjaar 2021.
  - Hiertoe verzoeken wij u een goede analyse (position paper/conversierapport) op te stellen ter onderbouwing van de verantwoording van de gemeentelijke belastingen en heffingen in de jaarrekening 2021.
- Zorgvuldige en tijdige afwikkeling IB-signalen is vanuit ons accountantsverslag 2020 een blijvend aandachtspunt.
- Verder vragen wij uw aandacht voor het aantoonbaar maken van de interne beheersing rondom het planning & control-proces, het schattingsproces grondexploitaties, proces uitkeringen in geld (Participatiewet), uitkeringen in natura (Wmo en Jeugdzorg), gemeentelijke belastingen en verbonden partijen.
- Het controleprotocol en normenkader 2021 dient u nog te laten vaststellen voorafgaand aan de jaarrekeningcontrole.

IT-BEHEERSING

- Vanaf boekjaar 2020 heeft u het nieuw financieel systeem Key2Financiën geïmplementeerd. Na deze implementatie hebben wij in het kader van onze controle 2020 de IT-beheersmaatregelen van het nieuw financieel pakket beoordeeld en in ons accountantsverslag 2020 in detail gerapporteerd over onze bevindingen en aanbevelingen.
- Uit navraag ten tijde van de interim-controle hebben wij vernomen dat uw organisatie in 2021 opvolging heeft gegeven aan onze bevindingen uit het accountantsverslag 2020. Medio november jl. hebben wij van uw organisatie opdracht gekregen een IT-audit te verrichten om vast te kunnen stellen of de IT-beheersmaatregelen (aantoonbaar) voldoende aanwezig zijn.
- Op het moment dat de algemene IT-beheersmaatregelen aantoonbaar voldoende aanwezig zijn, biedt dit nieuwe mogelijkheden voor zowel de verbijzonderde interne controle als de externe controle (meer systeemgerichte en minder gegevensgerichte controles). Daarmee wordt de IT-beheersing rondom het nieuw financieel pakket optimaal benut.
- Cybersecurity en netwerk inbraak zijn landelijk momenteel hottopics en vergt ook voor de gemeente Goirle aandacht.

VOORUITBLIK JAARREKENING 2021

Naast de zichtbare follow-up van de bevindingen en aanbevelingen uit deze managementletter vragen wij uw aandacht voor de volgende onderwerpen in de voorbereiding op het jaarrekeningtraject 2021.

- Actualisatie van de grondexploitatieopzet de Boschkens per 31-12-2021 inclusief financiële doorrekeningen;
- Aanlevering van spendanalyse over gehele vierjaarsperiode 2018-2021 met een interne toetsing op naleving van Europese aanbestedingsregels rekening houdend met de aandachtspunten uit SDO-notitie 'Uitvoering van controle op aanbestedingsrechtmatigheid bij jaarrekeningcontrole van decentrale overheden';
- Aansluiting tussen de saldi in de onderhoudsvoorzieningen per 31-12-2021 en de beheerplannen inclusief een verschillenanalyse;
- De verantwoordingsinformatie inzake de gemeentelijke belastingen/heffingen vanuit TOG;
- Voor overige aandachtspunten verwijzen wij naar hoofdstuk 6.1 in deze managementletter.

2. Ontwikkelingen & Actualiteiten

2.1 Gevolgen coronacrisis voor jaarrekening
2.2 Rechtmatigheidsverantwoording
2.3 Frauderisicobeheersing
2.4 Ontwikkelingen in het sociaal domein

2.1 Gevolgen coronacrisis voor jaarrekening 2021

Gevolgen COVID-19 strak blijven monitoren

Interne controle voortvarend oppakken

Bijzondere aandacht voor vaststellen subsidies

Gevolgen coronacrisis voor 2021 en verder

Vorig jaar hebben wij samen met u veel aandacht besteed aan de gevolgen van de coronacrisis, voor de korte en (middel)lange termijn. Aan de hand van een impact-analyse en de corona-checklist zijn wij nagegaan wat de effecten waren voor de informatievoorziening aan de raad, de interne beheersing alsmede de financiële implicaties op de korte en (middel)lange termijn. Met name door de onduidelijkheden in het begin van de crisis omtrent de financiële gevolgen en de compensatie door het rijk waren het onzekere tijden. In de loop van de tijd bleek de impact voor de meeste gemeenten mee te vallen. Niettemin is het zaak alert te blijven op de ontwikkelingen en de afwikkeling van de ontvangen rijksgelden. Ook de waardering van mogelijke verhoudingen met verbonden partijen verdienen hierbij extra aandacht. Wij adviseren u dit strak te blijven monitoren en de raad te blijven informeren over eventuele bijstellingen van de (meerjaren)begroting.

Tozo en TONK

Alle coronasteunmaatregelen zijn per 1 oktober 2021 beëindigd, waardoor het rijk afspraken heeft gemaakt over de afronding van de Tozo en de TONK. Vanaf het einde van de Tozo per 1 oktober 2021 tot het einde van het jaar geldt een tijdelijk aangepast Besluit bijstandverlening zelfstandigen (Bbz). Ook de TONK is onderdeel van het coronasteunpakket dat per 1 oktober 2021 wordt afgerond. Vanaf dan is het aan de gemeenten om huishoudens in financiële nood te ondersteunen vanuit het gebruikelijke instrumentarium, zoals de bijzondere bijstand. Uiteraard dienen beide regelingen in de jaarrekening/SiSa-bijlage te worden verantwoord. Van afgelopen voorjaar weten wij inmiddels dat deze controle intensief kan zijn. Wij vragen dan ook uw aandacht voor een tijdige (interne) controle op de verstrekte uitkeringen, zodat de verantwoording goed kan verlopen.

Vaststelling verstrekte subsidies

Veelal worden de in 2020 verstrekte subsidies in het voorjaar van 2021 vastgesteld. Aan de hand van de in de subsidieverordening en -beschikking opgenomen voorwaarden wordt nagegaan of een organisatie heeft voldaan aan de vereisten. Voor het jaar 2020 zal dat wellicht niet evident zijn; denk hierbij aan te leveren prestaties. Sommige gemeenten hebben (met de raad) afspraken gemaakt over de toe te passen handelswijze c.q. verantwoordingswijze. Indien dat bij de gemeente Goirle niet het geval is, adviseren wij u dat waar nodig alsnog te doen om zodoende de rechtmatigheid van de subsidievaststelling te kunnen waarborgen.

Voorwaardencriterium - subsidies

In samenhang met bovenstaande vragen wij met betrekking tot het voorwaardencriterium uw aandacht voor een tijdige (interne) controle op de subsidievaststellingen, zodat de verantwoording goed kan verlopen. Belangrijke aandachtspunten om de rechtmatigheid van subsidievaststellingen aantoonbaar vast te stellen betreffen:

- Is sprake van het opschorten van subsidieverplichtingen waaraan de aanvrager niet hoeft te voldoen?
- Indien gebruik is gemaakt van de hardheidsclausule is hier dan terecht gebruik van gemaakt en is de reden voor toepassen voldoende gemotiveerd (collegebesluit op subsidie niveau)?
- Indien artikelen uit de subsidieverordening buitenwerking zijn gesteld is dit dan door middel van een raadsbesluit bekrachtigd? (raadsbesluit op generiek niveau a.g.v. COVID-19)?

2.2 Rechtmatigheidsverantwoording (1/2)

Invoering rechtmatigheids-verantwoording 2022

Nieuwe notities:
- Kadernota 2022
- Addendum Kadernota 2021
- Notitie bedrijfsvoering

Stand van zaken en kaders rechtmatigheidsverantwoording met ingang van 2022

Eind juni werd bekend dat de invoering van de rechtmatigheidsverantwoording een jaar is uitgesteld, met ingang van het begrotingsjaar 2022. Op dat moment stond ook de wetswijziging voor december 2021 op de agenda van de Tweede Kamer waarna de wetswijziging zou worden ingevoerd met ingang van het begrotingsjaar 2022. Daarmee is er ruimte ontstaan om, na een intensief jaar met corona, de invoering goed voor te bereiden. Eind augustus 2021 heeft de commissie BBV (na consultatie) een nieuwe Kadernota Rechtmatigheid 2022 uitgebracht. Tegelijk met deze kadernota is eveneens een notitie over de paragraaf bedrijfsvoering en een addendum op de Kadernota Rechtmatigheid 2021 gepubliceerd. Recent hebben wij vernomen dat de in december 2021 geplande wetswijziging op de agenda van de Tweede Kamer is verschoven naar januari 2022. Desondanks gaan wij er vooralsnog vanuit dat de invoering van de wetswijziging doorgang vindt met ingang van begrotingsjaar 2022.

De verwachting is dat de commissie SDO van de NBA nog een notitie voor de accountants uitbrengt over de gevolgen van de invoering van de rechtmatigheidsverantwoording en de commissie BADO over de wijze van verantwoorden vanuit de optiek van gemeenten. Daarmee worden zowel accountants als gemeenten geïnformeerd en gefaciliteerd om de rechtmatigheidsverantwoording goed te kunnen invoeren. Wij adviseren u om hier kennis van te nemen.

Hoofdlijnen Kadernota Rechtmatigheid 2022

In de Kadernota Rechtmatigheid 2022 wordt uitgebreid ingegaan op het bestuurlijk belang van de rechtmatigheid voor de raad. Daarnaast worden de reikwijdte, de normen, de verantwoordelijkheden van het college en de criteria van de rechtmatigheid beschreven. Ook wordt in de kadernota ingegaan op de toepassing van de tolerantiegrenzen, de afwijkingen en de weging hiervan en is hierin een verplicht verantwoordingsmodel opgenomen. In de kadernota is een aantal stellige uitspraken gedaan die moeten worden gevolgd, waarbij de eerste uitspraak nadrukkelijk de rol van de gemeenteraad benoemd. Bij onduidelijkheden over de interpretatie van de rechtmatigheid moet de gemeenteraad aangeven welke uitleg moet worden gegeven aan de regelgeving en dit vastleggen in een besluit.

Het voert te ver om in deze managementletter uitgebreid in te gaan op de inhoud van deze kadernota, de stellige uitspraken en de aanbevelingen. Een aantal punten willen wij er wel uit lichten:
- De kadernota 2022 introduceert het begrip ‘onduidelijkheden’. Dit begrip geeft aan dat er situaties zijn waarin het ook voor het college niet duidelijk is of er rechtmatig is gehandeld. Deze situaties moeten worden toegelicht en worden gewogen door de gemeenteraad.
- De commissie BBV adviseert ook fraude door eigen medewerkers toe te lichten in de paragraaf bedrijfsvoering.
- Middels een verplicht model moet het college zich verantwoorden over de rechtmatigheid, afwijkingen en onduidelijkheden.
- In de paragraaf bedrijfsvoering moet vervolgens een toelichting worden gegeven op de afwijkingen en de maatregelen die het college neemt om de afwijkingen in de toekomst te voorkomen.
- De grens voor afwijkingen (zowel fouten als onduidelijkheden) wordt door de gemeenteraad bepaald en is maximaal 3% van de lasten (inclusief de mutatie in de reserves). Fouten en onduidelijkheden worden niet bij elkaar opgeteld.
- De invoering betekent eveneens dat de verordeningen ex artikel 212 en 213 van de Gemeentewet en het normenkader moeten worden geactualiseerd. Tevens moeten afspraken worden gemaakt met de accountant.
- Bij aan derden uitbestede werkzaamheden is het belangrijk als gemeente zelf zekerheid te krijgen omtrent de rechtmatigheid. De wijze waarop dat kan, is in de Kadernota uitgewerkt.

2.2 Rechtmatigheidsverantwoording (2/2)

Paragraaf bedrijfsvoering, de plek om afwijkingen te rapporteren

Beperkte wijzigingen in de rechtmatigheids-controle voor (het laatste jaar) 2021

Onze visie op de rechtmatigheids-verantwoording

Wij denken graag met u mee over invoering van rechtmatigheids-verantwoording

Status invoering rechtmatigheids-verantwoording

Hoofdlijnen Notitie bedrijfsvoering

De belangrijkste boodschap van deze nieuwe notitie is dat het college in de paragraaf bedrijfsvoering aanvullende informatie opneemt over individueel geconstateerde afwijkingen in de rechtmatigheidsverantwoording. Daarbij moet het college beschrijven welke actie wordt ondernomen om deze in de toekomst te voorkomen. De notitie werkt een aantal aanbevelingen en voorbeelden omtrent de paragraaf bedrijfsvoering verder uit.

Hoofdlijnen Addendum Kadernota Rechtmatigheid 2021

Het uitgangspunt van de commissie BBV is dat in principe weinig verandert in de rechtmatigheidscontrole over 2021, het laatste jaar dat de accountant een oordeel afgeeft met betrekking tot de rechtmatigheid. De wijzigingen in het addendum op de Kadernota Rechtmatigheid 2021 zijn dan ook beperkt. Er wordt meer aandacht gevraagd voor fraude en M&O-beleid en niet-financiële onrechtmatigheden in het kader van de Wet Fido moeten worden toegelicht in de paragraaf bedrijfsvoering.

Onze visie op de rechtmatigheidsverantwoording

BDO ziet, evenals de commissie BBV, de invoering van de rechtmatigheidsverantwoording als een kans om de controlerende rol van de gemeenteraad te versterken en te investeren in een verdere ontwikkeling van de bedrijfsvoering. Begin 2020 hebben wij hierover een visiepaper ‘Rechtmatigheidsverantwoording, een kans op meer control’ uitgebracht met daarin verschillende varianten en een invoeringsplan.

Het gaat bij de invoering van de rechtmatigheidsverantwoording om fundamentele vragen als:

- Op welke onderwerpen en met welke diepgang wilt u als gemeenteraad kaders stellen en controleren?
- In hoeverre werkt het college rechtmatig en/of bent u in control?
- In hoeverre is uw bedrijfsvoering, interne controle en IT-beheer op orde en wat is ervoor nodig om daar te komen?
- En misschien wel de moeilijkste vraag van allemaal: wat zijn de ambities en is de organisatie in staat om aan die doelen en verwachtingen te voldoen?

De wijziging in de verantwoordelijkheden ten aanzien van de rechtmatigheid betekent niet dat er minder rechtmatigheidscontroles moeten worden uitgevoerd, maar dat het college deze zelfstandig/intern moet inrichten, uitvoeren, controleren en rapporteren. Als accountant zullen wij die werkzaamheden vervolgens toetsen, teneinde te kunnen controleren en verklaren dat de rechtmatigheidsverklaring van het college een getrouw beeld geeft.

Status rechtmatigheidsverantwoording gemeente Goirle

Doordat onder andere de behandeling van de wet in de Tweede Kamer en de kadernota Rechtmatigheid lang op zich lieten wachten, was er lange tijd onduidelijkheid over de precieze invulling van de rechtmatigheidsverantwoording. De status van de invoering van de rechtmatigheidsverantwoording is met name om deze reden ongewijzigd ten opzichte van vorig jaar. In ons accountantsverslag 2020 hebben wij gerapporteerd over de stappen die de gemeente Goirle dient te ondernemen ter voorbereiding op de invoering van de rechtmatigheidsverantwoording. Ten tijde van de interim-controle 2021 hebben wij niet kunnen vaststellen dat uw gemeente deze stappen heeft gezet. Wij adviseren het college en de raad tijdig met elkaar in gesprek te gaan c.q. in gesprek te blijven over de invoering van de rechtmatigheidsverantwoording en zorg te dragen voor een duidelijk plan van aanpak inclusief overkoepelend interne controleplan wat aansluit op de invoering van de rechtmatigheidsverantwoording. Vanzelfsprekend denken wij graag met u mee.

2.3 Frauderisicobeheersing (1/2)

Controleverklaring gaat ook meer aandacht besteden aan frauderisicobeheersing en continuïteit

Diverse voorbeelden van maatregelen om frauderisico's te beheersen

Frauderisico indelen naar druk, gelegenheid en rechtvaardiging

Ontwikkelingen met betrekking tot fraude en de controle van de jaarrekening

Zoals aangegeven in ons accountantsverslag bij de jaarrekening 2020 zal de komende jaren vanuit de accountantscontrole nog nadrukkelijker aandacht worden gegeven aan fraudepreventie.

In februari 2021 heeft onze beroepsorganisatie de NBA hiervoor een notitie "Best practice maatregelen frauderisicobeheersing voor bestuurders en toezichthouders" ter consultatie uitgebracht. In deze notitie komt nadrukkelijk de rol van de bestuurders en toezichthoudende organen, zoals de gemeenteraad, bij het voorkomen en detecteren van fraude aan de orde. Door de nadruk te leggen op het voorkomen van fraude kunnen de gelegenheden tot fraude afnemen. Dit vraagt om actief toezicht op risico's en beheersmaatregelen ter voorkoming van fraude.

Begin september 2021 is tevens een nieuwe opzet van de controleverklaring ter consultatie uitgebracht. In de nieuwe controleverklaring, die zal ingaan vanaf boekjaar 2022, wordt van de accountants verwacht dat zij expliciete passages opnemen aangaande frauderisico-beheersing en continuïteit.

Zoals opgenomen in het consultatiedocument, kunnen bestuurders en toezichthouders diverse maatregelen nemen om de frauderisico's te beheersen. De belangrijkste voorbeelden uit het consultatiedocument zijn:

- Zorgdragen voor een goede 'tone at the top', cultuur en gedrag;
- Opstellen van diverse anti-corruptiemaatregelen (relaties met afnemers/leveranciers, gedragscodes t.a.v. nevenactiviteiten/ geschenken/etc.);
- Een goede interne beheersing (AO/IB), waaronder een periodieke frauderisicoanalyse;
- Het organiseren van tegenspraak, controle/compliance functies en diversiteit;
- Aandacht voor werknemers en bestuursleden (bijv. persoonlijke omstandigheden die kunnen leiden tot een druk om fraude te plegen);
- Periodieke medewerkers tevredenheidsonderzoeken;
- Fraudemeldpunt en klokkenluidersregeling;
- Contact en medewerking met uw accountant;
- Training en opleiding omtrent het fraudebewustzijn;
- Een adequate administratie met aandacht voor (fraude)risicovolle schattingsposten;
- Een transparant en integer beloningsbeleid;
- Een duidelijk plan om te reageren op (een vermoeden van) fraude.

Frauderisico's worden in de theorie en praktijk altijd ingedeeld naar drie omstandigheden (de zogenaamde fraudedriehoek), bestaande uit gelegenheid, druk en rationalisatie zoals hiernaast weergegeven. Wij verzoeken u bij de actualisatie van uw frauderisicoanalyse de drie omstandigheden hierin te verwerken.

2.3 Frauderisicobeheersing (2/2)

Onze rol in relatie tot frauderisicobeheersing

Onze rol als accountant inzake fraude

Zoals weergegeven in de controlestandaarden en onze opdrachtbevestiging, ligt de primaire verantwoordelijkheid voor het voorkomen en ontdekken van fraude bij zowel het management, het college als de gemeenteraad. Als accountant zijn wij niet verantwoordelijk en aansprakelijk voor de preventie van fraude. Onze controleopdracht heeft tot doel om vast te stellen dat de jaarrekening geen afwijkingen van materieel belang bevat die het gevolg zijn van fraude of fouten. Het onderkennen van risico's op een materiële fraude (frauderisico's), het uitvoeren van daarop gerichte controlewerkzaamheden en het actie ondernemen in het geval van een vermoeden van fraude, is dus een onlosmakelijk onderdeel van de accountantscontrole. Daarentegen is het voor de accountant lastig om een daadwerkelijke fraude te identificeren. Dit komt onder andere doordat de organisatie dagelijks aanwezig is en de accountant niet, fraude gepaard gaat met opgezette plannen om de fraude te verhullen, zoals valsheid in geschrifte, het opzettelijk nalaten om transacties vast te leggen of het opzettelijk aan de accountant verkeerd voorstellen van zaken. Samenspanning binnen organisaties of met derde partijen maakt dit vraagstuk nog lastiger. Door de kenmerken van fraude is het dus mogelijk dat een controle, ook al is die opgezet en uitgevoerd in overeenstemming met algemeen aanvaarde controlestandaarden, een fraude van materieel belang niet ontdekt.

Voor de organisatie maken wij onze werkzaamheden zichtbaar door het verstrekken van onze fraude- en compliance checklist en het bespreken van en rapporteren over (een vermoeden van) fraude. Vanaf 2022 zullen wij hierover communiceren met het maatschappelijk verkeer via onze controleverklaring.

Onze aanbevelingen in relatie tot frauderisicobeheersing

Onze waarnemingen en aanbevelingen inzake uw frauderisicobeheersing

Naast onze controlerende rol hebben wij in het kader van de interim-controle, onze kennis van de organisatie en de processen en deze ontwikkeling een aantal bevindingen en aanbevelingen inzake uw frauderisicobeheersing:

- U heeft geen overkoepelend M&O-beleid. In de diverse verordeningen zijn wel afzonderlijke bepalingen ter voorkoming en bestrijding van misbruik en oneigenlijk gebruik opgenomen.
- U heeft uw frauderisicoanalyse niet recent geactualiseerd. De laatste actualisatie heeft bij de interim-controle 2019 plaatsgevonden.
- De gemeente beschikt over een klokkenluidersregeling en gedragscode inzake integriteit ten aanzien van raadsleden, B&W en ambtsdragers.
- Het controleplan en de werkzaamheden van de verbijzonderde interne controle besteden geen specifieke aandacht aan fraude.
- Fraude(preventie) staat niet periodiek op de agenda van de gemeenteraad en/of auditcomité.
- Middelen omtrent het organisatie breed stimuleren van fraudebewustzijn, zoals training en opleiding, ontbreken.
- Een duidelijk (stappen)plan om te reageren op (een vermoeden van) fraude is niet beschikbaar.
- Onze fraude- en compliance checklist is bij uw organisatie nog onderhanden. Of hieruit risico's volgen die onze en uw aandacht verdienen is daarmee nog niet bekend. In dit kader verzoeken wij u er voor zorg te dragen dat wij de ingevulde fraude- en compliance checklist en de geactualiseerde frauderisicoanalyse voorafgaand aan onze jaarrekeningcontrole (februari 2022) ontvangen.

Ons advies

Wij adviseren u acties c.q. stappen te ondernemen met betrekking tot het vergroten van de actieve rol van de gemeenteraad / auditcomité ten aanzien van zowel fraudebewustzijn als frauderisicobeheersing en de periodieke monitoring hiervan expliciet op de agenda te zetten. Graag blijven wij op de hoogte van de acties c.q. stappen die u in dit kader onderneemt.

2.4 Ontwikkelingen in het sociaal domein

Ontwikkelingen met betrekking tot het sociaal domein en de controle van de jaarrekening

Vanuit onze natuurlijke adviesrol willen wij u attenderen op een aantal ontwikkelingen op het gebied van het sociaal domein. Wij schetsen deze ontwikkelingen op hoofdlijnen met als doel u hierop te attenderen. Dit betekent dat wij geen uitgebreid onderzoek hebben uitgevoerd naar deze onderwerpen of deze onderwerpen specifiek hebben gemaakt voor uw organisatie.

Resultaatgericht indiceren niet meer toegestaan

Uitspraak resultaatgericht indiceren

Onlangs is er een uitspraak geweest door de Centrale Raad van Beroep (CRvB) inzake een casus met betrekking tot het resultaatgericht indiceren. In deze casus is de indicatie van een cliënt voor begeleiding in natura niet langer toegekend in uren, maar in een te behalen resultaat. Uit het ondersteuningsplan blijkt wel welk resultaat moet worden behaald, binnen welke periode, met welke activiteiten en met welke frequentie, maar een tijdsindicatie in aantal zorguren ontbreekt. De CRvB oordeelt dat een manier van verstrekken, die maakt dat een cliënt en een zorgaanbieder niet weten hoeveel, naar tijdseenheden bepaalde, maatschappelijke ondersteuning het college heeft verstrekt, in strijd is met het rechtszekerheidsbeginsel. Dit is voor begeleiding niet anders dan voor huishoudelijke ondersteuning. Wij hebben vastgesteld dat u resultaatgerichte indicaties afgeeft en adviseren u waar nodig passende maatregelen te nemen, voor wat betreft toekomstige af te geven indicaties, rekening houdend met de recente uitspraak door de CRvB.

Vanaf 2022 nieuw woonplaatsbeginsel

Woonplaatsbeginsel Jeugdwet

Het woonplaatsbeginsel in de Jeugdwet regelt welke gemeente (financieel) verantwoordelijk is. Het huidige woonplaatsbeginsel is gebaseerd op de woonplaats van de gezagsdrager van een jeugdige. Het nieuwe woonplaatsbeginsel, dat vanaf 1 januari 2022 van toepassing wordt, gaat uit van de woonplaats waar de jeugdige staat ingeschreven op het moment van de zorgvraag. Het doel van deze wetswijziging is het verminderen van administratieve lasten, het sneller kunnen leveren van zorg en ondersteuning aan jeugdigen en het versterken van preventie. Voor gemeenten en zorgaanbieders betekent de implementatie van het nieuwe woonplaatsbeginsel een behoorlijke (administratieve) verandering. Daarom hebben gemeenten en zorgaanbieders uitgesproken dat ze behoefte hebben aan duidelijke afspraken over de implementatie van het woonplaatsbeginsel om onduidelijkheden en discussie te voorkomen. Om die reden zijn aanvullende afspraken gemaakt die zijn vastgelegd in een convenant. Het convenant is vastgesteld door de VNG-commissie Zorg, Jeugd en Onderwijs. Wij adviseren u de effecten van deze wijziging in kaart te brengen en uw organisatie voor te bereiden op de veranderende werkwijze.

Nieuwe Wet inburgering

Handreikingen Wet inburgering

Om gemeenten handvatten te geven op het gebied van informatievoorziening bij de invoering van de nieuwe Wet inburgering zijn onlangs twee handreikingen verschenen: de handreiking ‘Gegevensuitwisseling gemeenten en ketenpartners nieuwe Wet inburgering’ en de handreiking ‘Leveranciers’. Beide handreikingen helpen gemeenten op weg met de uitwisseling van gegevens tussen landelijke ketenpartners en de afspraken die zij moeten maken met hun softwareleveranciers. Wij adviseren u kennis te nemen van beide handreikingen en waar nodig actie te ondernemen.

3. Interne beheersing

3.1 Onze controle nog transparanter
3.2. Effectiviteit processen

3.1 Onze controle nog transparanter (1/2)

Belangrijkste aandachtspunten:
- Management override of controls
- Ongeautoriseerde handelingen in K2F
- Schattingen grondexploitatie
- EU-aanbestedingen

Inleiding

Wij vinden het van groot belang dat wij inzicht geven in de normen en verwachtingen ten aanzien van onze controle en de vertaling hiervan specifiek voor de gemeente Goirle. Alleen dan gaat de discussie niet alleen over de kwaliteit van de accountantscontrole, maar vooral ook over de wijze waarop de gemeente hiervan kan profiteren. In deze managementletter hebben wij daarom meer in detail uitgelegd op welke wijze wij de controle hebben ingericht en welke afwegingen wij daarbij maken. Wij doen dat door in deze paragraaf onze risico-inschatting, de belangrijkste processen, onze controleaanpak en de afwegingen te beschrijven.

Onze inschatting van de belangrijkste aandachtspunten

In het kader van de controle van een jaarrekening en onze controleaanpak maken wij een inschatting van de belangrijke aandachtspunten. Voor de controle van de jaarrekening 2021 van uw gemeente zien wij de volgende aandachtspunten:

- *Management override of controls*
  In onze controlestandaarden wordt expliciet ‘management override of controls’ als belangrijk aandachtspunt benoemd. Management override of controls houdt in dat het management of andere sleutelfunctionarissen zich in de unieke positie bevinden dat zij, gezien hun positie binnen de organisatie, vastgestelde procedures of autorisaties kunnen omzeilen of doorbreken. Als accountant dienen wij in onze werkzaamheden specifiek aandacht hieraan te besteden. Wij zijn van mening dat de mogelijkheden om buiten de getroffen interne beheersmaatregelen invloed uit te uitoefenen op de in de jaarrekening gepresenteerde cijfers beperkt zijn binnen uw gemeente. Het verrichten van een onjuiste/fictieve memoriaalboeking in de laatste maand van een tussentijdse rapportageperiode of het boekjaar dan wel bij het opstellen van de tussentijdse rapportage of de jaarrekening zien wij als enige mogelijkheid. Derhalve controleren wij deze memoriaalboekingen in detail.

- *Ongeautoriseerde handelingen in Key2Financiën*
  De logische toegangsbeveiliging van Key2Financiën dient goed te zijn ingericht ter voorkoming dat functionarissen meer bevoegdheden hebben dan noodzakelijk vanuit hun functie. Te ruime bevoegdheden kunnen ertoe leiden dat functionarissen handelingen verrichten die zij gezien hun functie niet mogen verrichten met eventuele omvangrijke gevolgen. Tijdens onze controle beoordelen wij de opzet en het bestaan van de logische toegangsbeveiliging van Key2Financiën en controleren wij of handelingen door de juiste functionarissen zijn verricht. Onze focus ligt hierbij op de juiste autorisatie van de inkoopfacturen en IBAN-wijzigingen. Wij zien dit als de voornaamste handelingen die uw functionarissen ongeautoriseerd zouden willen verrichten.

- *Schattingen grondexploitatie de Boschkens*
  In de jaarrekening 2020 is de grondexploitatie Heisteeg afgesloten. De grondexploitatie de Boschkens is na het afsluiten van de grondexploitatie Heisteeg de laatste lopende grondexploitatie binnen uw gemeente. Bij de jaarrekeningcontrole hebben wij specifiek aandacht voor de schattingselementen in de exploitatieopzet van de grondexploitatie de Boschkens, met name gezien de materiële omvang van de nog te maken kosten en nog te realiseren opbrengsten (schattingsrisico).

- *Naleving Europese aanbestedingsregels*
  Middels een inkoopanalyse controleren wij de aanbesteding van de lasten in 2021 waarbij wij middels een steekproef vaststellen of de Europese aanbestedingsregels zijn nageleefd.

3.1 Onze controle nog transparanter (2/2)

Belangrijkste processen

Onze inschatting van de belangrijkste processen

In het kader van onze controle hebben wij de volgende processen onderkend:

- het Planning & Control-proces (inclusief memoriaal proces);
- het proces aanbestedingen;
- het inkoop- en betalingsproces;
- het proces grondexploitatie(opzetten);
- het personeelsproces;
- het proces omtrent sociaal domein:
  - het proces uitkeringen in geld (Participatiewet);
  - het proces uitkeringen in natura (Wmo en Jeugdzorg);
- het gemeentelijke belastingenproces;
- het subsidieverstrekkingenproces;
- het proces omgevingsvergunningen;
- het proces huren en pachten;
- het proces omtrent verbonden partijen;
- het proces omtrent IT/automatisering.

Natuurlijk zijn er meer processen met financiële gevolgen te onderkennen, maar deze processen zien wij als de belangrijkste processen.

Per proces toetsen wij:

- Controletechnische functiescheiding
- Interne beheers-maatregelen
- IT-beheers-maatregelen
- Verbijzonderde interne controle

Onze controleaanpak

In onze controleaanpak is de insteek, daar waar mogelijk, te steunen op de interne beheersing in uw belangrijkste processen. Dit noemen wij een systeemgerichte aanpak, waarbij wij kunnen steunen op toereikende beheersmaatregelen in uw processen en IT-systemen. Voor elk proces beoordelen wij de volgende onderdelen:

- **Controle technische functiescheiding (CTFS):** Is er binnen de belangrijkste processen sprake van voldoende functiescheiding?
- **AO/IB:** Is er sprake van een toereikende administratieve organisatie met toereikende interne beheersmaatregelen?
- **IT-maatregelen: I**s er sprake van toereikende IT-beheersmaatregelen om een betrouwbare gegevensverwerking te waarborgen?
- **VIC:** Heeft de verbijzonderde interne controle (VIC) de interne beheersmaatregelen getoetst?

Indien al deze vragen positief kunnen worden beantwoord, is de organisatie optimaal in control en kunnen ook wij gebruik maken van uw interne beheersing. De vaak tijdrovende en gedetailleerde gegevensgerichte werkzaamheden (die ook nog eens achteraf plaatsvinden), kunnen dan beperkt blijven tot een minimum. Voor de uitkomsten van onze beoordeling van de interne beheersing in uw belangrijkste processen verwijzen wij naar het overzicht en de toelichtingen in paragraaf 3.2 ‘Effectiviteit processen’.

Indien wij deze vragen niet geheel positief kunnen beantwoorden en niet op uw interne beheersing kunnen steunen, betekent niet dat uw organisatie niet in control is, maar wel dat de interne beheersmaatregelen niet altijd aantoonbaar in de processen en IT-systemen zijn verankerd conform de daaraan te stellen eisen vanuit onze accountantscontrole. Het gevolg hiervan is dat wij in onze controleaanpak een overwegend gegevensgerichte, in plaats van een systeemgerichte, aanpak zullen hanteren.

3.2 Effectiviteit processen (1/2)

Samenvatting effectiviteit processen

In hoofdstuk 4 rapporteren we over onze detailbevindingen

Geen wijzigingen in de belangrijkste processen

Voor wat betreft onze aanpak kunnen wij nog niet altijd steunen op de interne beheersing; onze aanpak is daarmee hoofdzakelijk gegevens-gericht

Samenvatting effectiviteit van de processen

In het overzicht op de volgende pagina geven wij weer hoe de belangrijkste processen scoren op eerdergenoemde onderdelen (zie ook hoofdstuk 5 ten aanzien van IT-beheersing).

Daarnaast rapporteren wij in deze managementletter (hoofdstuk 4) over onze detailbevindingen met betrekking tot de significante processen.

Wij concluderen dat de door ons beoordeelde processen in grote lijnen niet zijn gewijzigd ten opzichte van vorig jaar. Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat in de interne beheersorganisatie van uw gemeente (voor zover relevant voor de jaarrekeningcontrole) binnen de belangrijkste processen over het algemeen sprake is van minimaal noodzakelijke primaire functiescheiding. Tevens is binnen de processen sprake van interne beheersmaatregelen. Deze maatregelen worden echter niet altijd toereikend genoeg vastgelegd, waardoor achteraf niet toetsbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd.

Omdat de AO/IB niet altijd goed is opgezet, bestaat of goed werkt, kunnen wij voor wat betreft de insteek van onze controle niet volledig op de processen steunen en bestaat onze controleaanpak overwegend uit gegevensgerichte werkzaamheden. Er zijn in onze aanpak daarom aanvullende gegevensgerichte werkzaamheden noodzakelijk.

3.2 Effectiviteit processen (2/2)

PROCES	CTFS	AO/IB	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Planning & Control			N.v.t.	Een procesbeschrijving die ingaat op de totstandkoming van de begroting en rapportages ontbreekt. Wij adviseren u deze alsnog op te stellen om inzichtelijk te maken welke interne beheersmaatregelen uw organisatie heeft getroffen om te waarborgen dat sprake is van een adequaat functionerende planning & control cyclus. In lijn met voorgaand jaar verwachten wij van de verbijzonderde interne controle bij aanvang van de jaarrekeningcontrole een integrale analyse en steekproefcontrole op de memoriaalboekingen. Aandachtspunt is het tijdig vaststellen van het controleprotocol en normenkader 2021 (zie ook hoofdstuk 4.1 Detailbevindingen processen' in deze managementletter).
Subsidies				Proces subsidies is onveranderd. Aandachtspunt is de zichtbare periodieke aansluiting subsidievolgsysteem met financiële administratie. Zie verder ook hoofdstuk '2.1 Gevolgen coronacrisis voor jaarrekening 2021' in deze managementletter.
Inkopen & betalingsproces				De maatregelen ten aanzien van de prestatieverklaring en de verplichtingenadministratie inclusief monitoring van kredietoverschrijdingen worden niet altijd toereikend genoeg vastgelegd, waardoor achteraf niet toetsbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd. Daarnaast is vanuit de IT-audit 2020 sprake van ontoereikende IT-beheersmaatregelen (logische toegangsbeveiliging: superusers) om een betrouwbare gegevensverwerking te waarborgen. Inmiddels hebben we vernomen dat ook hier opvolging aan is gegeven. Dit zal nog moeten blijken uit de geplande IT-audit 2021. Zie ook hoofdstuk '5.1 IT-beheersing in deze managementletter'.
Aanbestedingen			N.v.t.	Voor de aandachtspunten rondom aanbestedingsrechtmatigheid verwijzen wij naar onze managementletter 2020. De interne beheersing rondom de naleving van de aanbestedingsrechtmatigheid is een blijvend aandachtspunt. De budgethouder/inkoper monitort (potentiële) opdrachten nog onvoldoende zichtbaar op naleving van Europese aanbestedingsregels om tijdig te kunnen bijsturen. Wat nog aandacht verdient is met name de schriftelijke raming van de opdracht voorafgaand aan de keuze van de aanbestedingsvorm en tussentijdse monitoring van eventuele wezenlijke wijzigingen van de opdracht in relatie tot naleving van de Europese aanbestedingsregels. De inkoopanalyse met betrekking tot de aanbestedingsrechtmatigheid vindt conform planning begin 2022 plaats voorafgaand aan de jaarrekeningcontrole.
Personeel				Proces personeelskosten is adequaat. Een aanvullende interne beheersmaatregel is aan te bevelen om te waarborgen dat interne procedures rondom declaratie van dienstreizen en reiskosten woon-werk strikt worden nageleefd en eventuele afwijkingen tijdig worden gesignaleerd en afgewikkeld.
Sociaal Domein				Zie hoofdstuk '4.1 Detailbevindingen processen' in deze managementletter.
Belastingen			N.v.t.	Zie hoofdstuk '4.1 Detailbevindingen processen' in deze managementletter.
Grondexploitatie			N.v.t.	Zie hoofdstuk '4.1 Detailbevindingen processen' in deze managementletter.
Verbonden partijen		N.v.t.	N.v.t.	Zie hoofdstuk '4.1 Detailbevindingen processen' in deze managementletter.
Verhuur			N.v.t.	Proces verhuuropbrengsten is adequaat en volledigheid is gewaarborgd. We zien nog een aandachtspunt ten aanzien van de zichtbare vastlegging van de beheersmaatregelen.
Omgevingsvergunningen				Proces omgevingsvergunningen is ten opzichte van voorgaand jaar onveranderd en blijvend adequaat.
ICT/automatisering			N.v.t.	Zie hoofdstuk '5 IT-beheersing in deze managementletter'.

Proces is ontoereikend, meerdere bevindingen en aanbevelingen. Risico x impact is hoog.

Proces is toereikend, één of enkele aanbevelingen resteren. Risico x impact is middel.

Proces is adequaat, enkel aanbevelingen ter verdere optimalisatie. Risico x impact is laag.

4. Bevindingen significante processen

4.1 Detailbevindingen processen

4.1 Detailbevindingen processen (1/6)

Uitvoeringstaken gemeentelijke belastingen en heffingen tot en met 2021 uitbesteed aan TOG, vanaf 2022 in eigen beheer

Verscherpt toezicht vanuit de gemeente brengt tekortkomingen aan het licht

TOG formeel in gebreke gesteld

Impact problematiek TOG voor de jaarrekeningcontrole 2021

Gemeentelijke belastingen en heffingen

De gemeente Goirle heeft de uitvoering van de gemeentelijke belastingen en heffingen sinds een aantal jaren uitbesteed aan TOG Nederland B.V. (hierna: TOG). Ten tijde van onze interim-controle hebben wij gesproken met uw senior medewerker belastingen en teamleider belastingen. Aanleiding van dit gesprek was de kwaliteit van de dienstverlening door TOG en de opgelopen vertraging in de belastingheffingen. Hierover heeft uw gemeente het afgelopen jaar diverse gesprekken gevoerd met TOG en afspraken gemaakt. Desondanks constateert uw gemeente geen of onvoldoende verbetering. Dit heeft ertoe geleid dat de overeenkomst met TOG na 31 december 2021 niet wordt voortgezet en dat de uitvoering van de gemeentelijke belastingen en heffingen in eigen beheer wordt uitgevoerd.

Naar aanleiding van bovenstaande signalen is uw gemeente nadrukkelijker toezicht gaan houden op de dienstverlening vanuit TOG. Steekproefsgewijs heeft uw medewerker belastingen controles verricht op proefkohieren. De geconstateerde fouten bestonden onder andere uit:

- Objecten zonder WOZ-waardebepaling;
- Onjuiste WOZ-waarde;
- Onjuiste eigenaar;
- Onjuiste gebruiker en het missen van aanslagregels.

Vanwege het continue niet ‘tijdig’ nakomen van de afspraken is TOG formeel in gebreke gesteld door de gemeente. TOG is nadrukkelijk geïnformeerd over het feit dat zij niets mogen versturen zonder dat vooraf door medewerker belastingen een akkoord is gegeven.

De problematiek die hiervoor is geschetst heeft ook een directe impact op onze controlewerkzaamheden in het kader van de jaarrekeningcontrole 2021. Dat betekent dat wij gezien de geconstateerde onjuistheden van uiteenlopende aard aanvullende controlewerkzaamheden zullen moeten verrichten, gericht op het vaststellen dat de jaarrekening 2021 vrij is van materiële afwijkingen als gevolg van fouten en/of fraude. Denk hierbij ook aan mogelijke fouten uit voorgaande jaren. Wij zullen zoveel als mogelijk aansluiting zoeken op de diverse checks en herstelwerkzaamheden die vanuit uw organisatie zijn opgezet. In goed overleg met uw organisatie streven wij naar een duidelijk plan van aanpak en planning richting de jaarrekeningcontrole. Het contact hierover loopt via uw senior medewerker belastingen en teamleider belastingen.

4.1 Detailbevindingen processen (2/6)

Uitbreiding personele capaciteit

De gemeenten Goirle, Hilvarenbeek en Oisterwijk (GHO) hebben in samenwerking een team gevormd om de kwaliteitsbeheersing rondom de gemeentelijke belastingen en heffingen weer op het gewenste niveau te krijgen. Het gevormde team bestaat uit:

- Een stuurgroep GHO (per gemeente vertegenwoordigd door een MT-lid).
- Team belastingen GHO:
  - Teamleider belastingen.
  - Drie senior medewerkers belastingen.
- Externe inhuur voor:
  - Controles op data in VRiS (drie externe medewerkers).
  - Controles op gebruiksoppervlakte en herwaarderingen (twee medewerkers).
  - Juridische en inhoudelijke ondersteuning (twee externe medewerkers).
  - Adviseur en projectleider (één externe medewerker).

Herstelwerkzaamheden nog onderhanden

De herstelwerkzaamheden die dit team verricht zijn met name gericht op:

- Integrale controle kohieren: Elke belastingregel op een kohier kijkt de medewerker belastingen na. Op elk kohier krijgt TOG een terugkoppeling over de regels waarvoor zij wel en waarvoor zij niet een WOZ-beschikking/aanslagbiljet mogen versturen. Ook verricht de medewerker belastingen controles op onder andere overzichten die TOG levert aan de Waarderingskamer, het versturen van verminderingen en de dwanginvordering.
- 0-meting belastingapplicatie: GHO heeft door een extern bureau een 0-meting laten uitvoeren. Deze 0-meting laat zien dat er onlogische mutaties in de belastingapplicatie zitten. Twee medewerkers zijn ingehuurd om de resultaten van de 0-meting te controleren en correct te muteren. Dit kan resulteren in het opleggen van ‘missende’ belastingaanslagen over 2021. Tevens wordt hiermee een kwaliteitsslag gemaakt voor de belastingaanslagen 2022.
- Kadastermutaties: Het verwerken van de kadastermutaties door TOG blijkt foutgevoelig te zijn. Dit vanwege onvoldoende kennis binnen hun vaste medewerkers. Het verwerken van de kadastermutaties voert team belastingen nu zelf uit en ook deze taak ligt bij de twee medewerkers die zijn ingehuurd. Zij voeren tevens controles uit op eerder ontstane ‘uitval’ en controles op reeds verwerkte mutaties die TOG, eerder dit kalenderjaar, heeft uitgevoerd en die van belang zijn voor de WOZ-beschikkingen/aanslagen 2022.
- Geblokkeerde objecten: De WOZ-beschikkingen/aanslagen gemeentelijke belastingen 2021 van objecten die geblokkeerd stonden zijn in november 2021 opgelegd. Dit geldt tevens voor een gering aantal blokkeringen over 2020 en 2019. Hierbij opgemerkt dat ook de Waarderingskamer constateerde dat er achterstanden zijn. Medio december wenst de Waarderingskamer een update hierover.
- Afronding werkzaamheden TOG: Met TOG is de afspraak gemaakt welke werkzaamheden zij voor 31 december 2021 moeten afronden. Hieronder valt ook de accountantscontrole die TOG zelf jaarlijks laat uitvoeren.
- Controles op gebruikersoppervlakte en herwaardering: Waarderen naar gebruikersoppervlakten is verplicht met ingang van 1 januari 2022.
- Nieuwe applicatie: De ervaringen van afgelopen jaar zijn aanleiding geweest om de outsourcingsovereenkomst met TOG niet te verlengen. Het college van burgemeester en wethouders heeft ingestemd met de aanschaf van een nieuwe applicatie “Level” waarmee uw gemeente alle WOZ/belastingwerkzaamheden zelf in eigen beheer gaat uitvoeren. In december 2021 staat de conversie gepland en in november 2021 de proefconversie. Denk hierbij aan het opstellen van een conversierapportage.
- Verzuimtraject: De stuurgroep heeft ingestemd om het verzuimtraject in te gaan en hierbij wordt uw gemeente ondersteund door extern ingehuurde juristen.

4.1 Detailbevindingen processen (3/6)

Onze observatie en aanbeveling

Onze observatie is dat uw organisatie tijdig heeft ingegrepen en belangrijke stappen heeft ondernomen om de kwaliteitsbeheersing omtrent de volledigheid, juistheid en rechtmatigheid van de gemeentelijke belastingen en heffingen weer op orde te krijgen. Gezien de problematiek rondom TOG en de uiteenlopende gevolgen met impact voor uw gemeente is dat geen eenvoudige opgave en vergt de nodige inspanning van uw organisatie. In het kader van de voorbereidingen op de jaarrekening 2021 is het belangrijk als gemeente zelf zekerheid te krijgen omtrent de verantwoording van de gemeentelijke belastingen en heffingen rechtmatigheid.

Wij verzoeken de gemeente Goirle een goede analyse (position paper) op te stellen ter onderbouwing van de volledige, juiste en rechtmatige verantwoording van de gemeentelijke belastingen en heffingen in de jaarrekening. In deze analyse vragen wij u op een gestructureerde wijze verifieerbaar in kaart te brengen welke werkzaamheden uw organisatie heeft verricht om zelf zekerheid te verkrijgen omtrent de verantwoording van de gemeentelijke belastingen en heffingen in de jaarrekening. De wijze waarop dat kan is een controledossier waarin de position paper als leidraad dient voor ondersteunende documentatie die als onderbouwing is inbegrepen. De vastleggingen in dit controledossier dienen zodanig te worden gedocumenteerd dat het in het kader van de jaarrekening 2021 verifieerbaar is.

Controleprotocol en normenkader 2021 nog vast te stellen

Controleprotocol en normenkader 2021

Als accountant van uw gemeente onderzoeken wij of de jaarrekening het door de wet vereiste inzicht geeft. De uitslag van ons onderzoek geven wij weer in een controleverklaring over de getrouwheid van de jaarrekening en de rechtmatigheid van de totstandkoming van de in de jaarrekening opgenomen baten, lasten en balansmutaties. De controle op de rechtmatigheid richt zich alleen op de financiële beheershandelingen als gevolg van de wet- en regelgeving zoals opgenomen in het door het college vastgestelde normenkader. Wij constateren dat het controleprotocol en normenkader 2021 bij uw gemeente nog onderhanden is. Graag vragen wij uw aandacht voor het tijdig vaststellen hiervan voorafgaand aan onze jaarrekeningcontrole.

Zorgvuldige en tijdige afwikkeling IB-signalen is een blijvend aandachtspunt

M&O beleid en afwikkeling IB-signalen (Tozo)

In ons accountantsverslag 2020 hebben wij gerapporteerd over onze constatering dat bij uw gemeente geen specifiek M&O-beleid en controleplan IB-signalen, zoals verwoord in hoofdstuk 9.13 van de ‘nota verwachtingen accountantscontrole 2020’ d.d. 8 april 2021, aanwezig is. Ten tijde van de interim-controle 2021 hebben wij vastgesteld dat deze constatering nog actueel is. Wij adviseren uw organisatie het opstellen van het M&O-beleid en controleplan IB-signalen op korte termijn op te pakken en vragen uw aandacht voor het tijdig monitoren van de uitvoering.

Volledigheidshalve melden we dat we hebben vernomen dat uw gemeente de afwikkeling IB-signalen in samenwerking met de gemeente Tilburg oppakt. Des temeer is het belangrijk om in het controleplan IB-signalen de rollen en verantwoordelijkheden duidelijk vast te leggen en de naleving hiervan actief te blijven monitoren. Tevens dient voldoende aandacht uit te gaan naar de wijze van uitvoering afwikkeling IB-signalen en rapportering over de uitkomsten, bevindingen en conclusies. De informatieverstrekking (zichtbare vastlegging uitgevoerde werkzaamheden ondersteund met verificatiedocumenten) is daarin een belangrijke om de afwikkeling van de IB-signalen aantoonbaar en controleerbaar te maken.
Vóórafgaand aan de jaarrekeningcontrole (begin januari 2022) zullen wij de follow-up bekijken van de afwikkeling van de IB-signalen en de eventuele impact op de jaarrekening en onze controlewerkzaamheden bepalen.

4.1 Detailbevindingen processen (4/6)

Voortgang actualisatie opzet en bestaan AO/IB

Processen welke uw organisatie nog onderhanden heeft

Aandacht voor een tijdige follow-up

▶ Schattingsproces grondexploitaties

▶ Proces uitkeringen (Participatiewet)

Zichtbare actualisatie van uw interne beheersing (opzet en bestaan AO/IB)
Na afronding van onze jaarrekeningcontrole 2020 hebben wij samen met uw organisatie vooruitgeblikt naar de interim-controle 2021. Tijdens deze vooruitblik hebben wij onze verwachtingen op elkaar afgestemd om tijdig voorbereidingen te treffen op onze interim-controle. Hierbij hebben wij aangegeven de focus te leggen op de actualisatie van de opzetbeschrijving van de administratieve organisatie en interne beheersing (AO/IB) van uw belangrijkste processen (zie hoofdstuk 3.1) en het aantoonbaar maken van het bestaan hiervan middels ondersteunende documentatie. Ten tijde van de interim-controle hebben wij samen met uw organisatie de voortgang geïnventariseerd en geconstateerd dat onderstaande processen nog onderhanden zijn:

- het Planning & Control-proces;
- het (schattings)proces grondexploitatie;
- het gemeentelijke belastingenproces;
- het proces uitkeringen in geld (Participatiewet);
- het proces uitkeringen in natura (Wmo en Jeugdzorg);
- het proces omtrent verbonden partijen/ service organisaties.

Wij vragen uw aandacht voor een tijdige en zorgvuldige afwikkeling. Voorafgaand aan de jaarrekeningcontrole (januari 2022) zullen wij de follow-up beoordelen en de eventuele impact op onze jaarrekeningcontrole bepalen. Specifiek ten aanzien van het schattingsproces grondexploitatie, het proces uitkeringen in geld (Participatiewet) en het proces omtrent verbonden partijen volgt hierna nog een nadere toelichting.

Schattingsproces grondexploitatie
De jaarrekeningpost ten aanzien van de grondexploitaties is inherent onderhevig aan subjectieve schattingselementen door de invloed van parameters (zoals kostenstijgingen, fasering, druk op verkoopprijzen, rente-effecten). Deze parameters zijn bepalend voor de in de toekomst te realiseren opbrengsten en kosten en daarmee ook op de jaarlijks te bepalen tussentijdse winstneming op basis van de POC-methode. Bij uw gemeente is het een stuk minder complex aangezien nog maar sprake is van één lopende grondexploitatie (de Boschkens).

Desalniettemin dient uw gemeente (de betrouwbaarheid en redelijkheid van) de belangrijkste schattingselementen jaarlijks te evalueren en de uitgangspunten die hieraan ten grondslag liggen te actualiseren. Voorafgaand aan de interim-controle (juli 2021) hebben wij u om inzicht gevraagd in de interne beheersing specifiek rondom dit schattingsproces aan de hand van de zogenaamde vijf w-vragen (wie doet wat, wanneer, waarmee en met welk doel). Het betreft hier de beschrijving van de aanwezige beheersmaatregelen in het proces (opzet) en het aantoonbaar maken van het bestaan hiervan middels ondersteunende documentatie (lijncontrole 2021). Ten tijde van de interim-controle hebben wij dit inzicht nog niet verkregen.

Participatiewet
Ten tijde van de interim-controle hebben wij van uw organisatie inzicht verkregen in de opzet van de interne beheersing rondom het proces uitkeringen in geld (Participatiewet). In de beschrijving van deze opzet is in beeld gebracht welke beheersmaatregelen (waaronder functiescheiding en 4-ogen principe) in het proces zijn verankerd om de juistheid en rechtmatigheid van de uitkeringen blijvend te waarborgen. Het bestaan van deze beheersmaatregelen middels ondersteunende documentatie (lijncontrole 2021) heeft u organisatie nog niet kunnen aantonen.

▶ Beheersing verbonden partijen/ service organisaties

Deelwaarnemingen periode januari tot en met augustus 2021

Werkzaamheden voorafgaand aan de jaarrekeningcontrole (januari)

Resterende werkzaamheden

Verbonden partijen/ service organisaties

Doordat gemeenten steeds meer opereren in een samenwerkingsverband, al dan niet via een gemeenschappelijke regeling, dient er steeds meer bewustzijn te komen over de werking hiervan. De gemeente Goirle heeft een aantal verbonden partijen die voor de gemeente taken uitvoeren of waarmee de gemeente samenwerkt. De verantwoording door deze verbonden partijen vindt plaats binnen uw reguliere P&C cyclus van de begroting en jaarrekening (paragraaf verbonden partijen). Hoewel naar aanleiding van de gerezen situatie rondom TOG in dit specifieke geval de monitoring is aangescherpt heeft het risicomanagement rondom de serviceorganisaties nog (te) weinig de expliciete aandacht.

Wij constateren dat uw gemeente momenteel niet beschikt over een actueel nota/beleid verbonden partijen. Uw huidige nota verbonden partijen is van 2006. Het risico bestaat dat de risico's (beleidsmatig, juridisch, financieel) die de gemeente loopt uit hoofde van samenwerkingsrelaties onvoldoende worden beheerst. Zinvol lijkt de invulling van het risicomanagement per samenwerkingsrelatie concreet vorm en inhoud te geven met, per samenwerkingsrelatie uit te werken, toezicht-arrangementen. De monitoring (control) op de naleving van de arrangementen zou dan vervolgens intern nader kunnen worden belegd als onderdeel van de bestaande P&C-cyclus. Wij adviseren u in dit kader een kaderstellend document (nota/beleid verbonden partijen) op te stellen waarin uitgangspunten worden opgenomen alsmede werkafspraken om risicomanagement rondom samenwerkingsrelaties vorm te geven.

Gegevensgerichte controlewerkzaamheden 2021

Tijdens de interim-controle hebben wij naast het vaststellen van de opzet en het bestaan van de AO/IB binnen de processen ook diverse deelwaarnemingen geselecteerd over het eerste half jaar 2021 (januari – juni) met betrekking tot onderstaande posten.

- Inkomensoverdrachten (uitkeringen EU, Rijk, provincie en gemeenten);
- Uitkeringen in natura (Wmo);
- Uitkeringen in geld (Participatiewet);
- Subsidieverstrekkingen;
- Inkomensoverdrachten (exploitatiebijdragen aan derden);
- Salarissen en sociale lasten;
- Aankopen goederen en diensten.

In goed overleg en met behulp van uw medewerker AO IC zijn deze steekproeven in de organisatie uitgezet en is de benodigde controle-informatie verzameld. Ten tijde van de interim-controle hebben wij hier onze controlewerkzaamheden op verricht en komen tot de conclusie dat hier geen bijzonderheden uit naar voren zijn gekomen die in het kader van onze jaarrekeningcontrole van materieel belang zijn. Wel constateren wij dat onze controlevragen die wij ten tijde van de interim-controle hebben uitgezet in uw organisatie met betrekking tot de uitkeringen in natura (Wmo) en aankopen goederen en diensten nog onderhanden zijn. Deze vragen zien toe op ontbrekende bewijsstukken die benodigd zijn om een oordeel te kunnen vormen over de getrouwheid en rechtmatigheid van de geselecteerde deelwaarnemingen. Wij vragen uw aandacht voor een tijdige follow-up voorafgaand aan de jaarrekeningcontrole.

Bij de voorbereiding richting de jaarrekeningcontrole maken wij, evenals voorgaande jaren, afspraken over de resterende deelwaarnemingen en de hiervoor benodigde controle-informatie over de periode juli tot en met december 2021.

4.1 Detailbevindingen processen (6/6)

Aandacht voor een tijdige follow-up managementletter en accountantsverslag 2020

Follow-up rapportages 2020

Voorafgaand aan de interim-controle 2021 hebben wij uw organisatie om een schriftelijke follow-up gevraagd op onze bevindingen en aanbevelingen uit de managementletter en accountantsverslag 2020. Ten tijde van de interim-controle 2021 hebben wij moeten constateren dat deze schriftelijke follow-up nog ontbreekt. Vanwege tijdgebrek en andere prioriteiten is dit in uw organisatie nog onderhanden. Wij vragen uw aandacht voor een tijdige schriftelijke follow-up voorafgaand aan de jaarrekeningcontrole. Dit komt ten goede aan de efficiëntie van het jaarrekeningproces en de jaarrekeningcontrole.

5. IT-beheersing

5.1 IT-beheersing

5.2 Nieuw belastingsysteem met ingang van 2022

5.3 Bevindingen IT-beheersing | Overall beeld

5.4 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol

5.5 IT-audit | Benchmark Overheid

5.1 IT-beheersing (1/2)

Wij beoordelen betrouwbaarheid en continuïteit IT voor zover relevant voor jaarrekeningcontrole

IT-werkzaamheden en onze controlerende rol

Ingevolge artikel 2:393 lid 4 BW dient de accountant in zijn verslag aandacht te besteden aan de bevindingen die naar voren zijn gekomen uit de beoordeling van de automatiseringsomgeving wat betreft de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Wij benadrukken dat onze jaarrekeningcontrole gericht is op het geven van een oordeel omtrent de jaarrekening zelf en zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan. De IT-auditwerkzaamheden zijn geïntegreerd in de controleaanpak van de jaarrekening.

Het inzicht in de betrouwbare werking van de IT-systemen en -applicaties en het gebruik ervan door de organisatie vormen een onderdeel van de kwaliteit van de interne beheersing en de administratieve organisatie. Algemene IT-beheersmaatregelen rond uw kritieke systemen leveren daarnaast een belangrijke bijdrage aan het mitigeren van de risico's op ongeautoriseerde handelingen, onbeheerste wijzigingen en het optreden van verstoringen met impact op de gegevensverwerking.

Beoordeeld systeem (voorgaand jaar):
- Key2Financiën

Per 1 januari 2020 heeft uw gemeente samen met de gemeenten Hilvarenbeek en Oisterwijk het nieuw financieel systeem Key2Financiën geïmplementeerd. Na deze implementatie hebben wij in het kader van onze jaarrekeningcontrole 2020 de IT-beheersmaatregelen van het nieuw financieel pakket beoordeeld op de volgende onderdelen:
- Logische toegangsbeveiliging; om het risico van ongeautoriseerde handelingen te adresseren.
- Wijzigingsbeheer; om het risico van onbeheerste wijzigingen te adresseren.
- Continuïteit; om het risico van verstoringen te adresseren.

Detailbevindingen IT-beheersing en opvolging in 2021

In ons accountantsverslag 2020 hebben wij in detail gerapporteerd over onze bevindingen en aanbevelingen. Verbeterpunten lagen op het gebied van logische toegangsbeveiliging (autorisatiebeheer en superuserrechten). Inmiddels hebben wij vernomen dat uw gemeente samen met de gemeenten Hilvarenbeek en Oisterwijk opvolging heeft gegeven aan onze aanbevelingen. In dit hoofdstuk geven wij allereerst een samenvatting van onze bevindingen voor de genoemde applicaties. Daarna gaan wij, vanuit onze natuurlijke adviesfunctie, in op een aantal actuele ontwikkelingen ten aanzien van de belastingapplicatie, de baseline informatiebeveiliging overheid en de ITGC benchmark overheid.

Quick wins indien IT-beheersmaatregelen aantoonbaar voldoende aanwezig zijn

Op het moment dat de intern getroffen algemene IT-beheersmaatregelen aantoonbaar voldoende aanwezig zijn, biedt dit nieuwe mogelijkheden voor het realiseren van quick wins om processen aan de voorkant meer systeemgericht te controleren in plaats van achteraf gegevensgericht. Daarmee wordt de IT-beheersing rondom het nieuw financieel pakket optimaal benut in de dagelijkse bedrijfsvoering. In relatie tot de invoering van de rechtmatigheidsverantwoording levert dit ook voordelen op voor de verbijzonderde interne controle (minder gegevensgerichte controles achteraf) en is uw gemeente beter in staat om aan de voorkant aantoonbaar in control te zijn.

5.1 IT-beheersing (2/2)

Zorg en inspanningsplicht bij bescherming persoonsgegevens

Data-incidenten en melding datalekken

Aandacht gevraagd voor cybersecurity en impact op uw gemeente

Dataprivacy

De Algemene verordening gegevensbescherming (AVG) ziet toe op de bescherming van persoonsgegevens. De gemeente Goirle heeft als verwerkingsverantwoordelijke van bijzondere persoonsgegevens een zorg en inspanningsplicht om gegevens op een adequate manier in te richten. Hiertoe moet uw gemeente compliance met AVG kunnen aantonen waaronder inbreuken op persoonlijke gegevens kunnen vaststellen en in voorkomend geval de desbetreffende bevoegde instanties en personen op de hoogte brengen. In onze controle hebben wij de maatregelen rond het meldproces van datalekken, zoals vereist vanuit de Wet meldplicht datalekken, geïnventariseerd. Wij hebben vastgesteld dat u een proces heeft ingericht voor het registreren van de beveiligingsincidenten waaruit datalekken naar voren kunnen komen en de afwikkeling hiervan tot en met een (eventuele) melding bij de Autoriteit Persoonsgegevens en het informeren van de betrokkenen. Wij hebben van uw coördinator gegevensbescherming vernomen dat er in de periode van januari - oktober 2021 5 data-incidenten hebben plaatsgevonden waarvan geen melding is gedaan bij de Autoriteit Persoonsgegevens. Volledigheidshalve melden we dat melding aan de AP niet noodzakelijk is gebleken.

Cybersecurity

Cybersecurity is anno 2021 een hottopic. In de huidige tijd is het veelal niet meer de vraag of een organisatie slachtoffer kan worden van een netwerkinbraak of cyberaanval, maar wanneer deze zal plaatsvinden en wat de impact hiervan is. In het uiterste en meest zorgwekkende geval zal de informatievoorziening opnieuw opgebouwd dienen te worden. Het ligt dan ook voor uw gemeente voor de hand om het risico inzake cybersecurity te onderkennen. Wij adviseren u alert te blijven op cyber gerelateerde risico's en initiatieven te nemen om het belang van cybersecurity onder de aandacht te brengen van werknemers. In dit kader geven wij u ter overweging mee om een nulmeting uit te voeren om eventuele cyber aandachtsgebieden te identificeren.
Uit ervaring is gebleken dat een aantal zaken belangrijk zijn om vooraf te organiseren. Hieronder geven wij een aantal tips welke mogelijk ook voor uw gemeente van belang zijn:

- De inrichting van de crisisorganisatie.
- Het opstellen van een up-to-date continuïteitsplan.
- Het opstellen van een draaiboek waarin de verschillende fasen van herstel zijn opgenomen (eerste uren, dagen, weken en nazorg):
  - Prioriteiten bepalen ten aanzien van de continuïteit van de bedrijfsvoering;
  - Het maken van een melding bij de Autoriteit Persoonsgegevens ingeval van persoonsgegevens en het doen van aangifte;
  - Een communicatieplan (stakeholders);
  - Externe ondersteuning (specialist).
- Het bewaren van offline back-ups naast netwerk back-ups en het regelmatig testen van deze offline back-ups;
- Het invoeren van netwerk segmentatie en software tijdig updaten;
- Het toepassen van multifactor authenticatie;
- 24/7 veiligheidsmonitoring op dataverkeer;
- Het overzetten van websites naar https://
- Zorgdragen dat wachtwoorden en toegangsrechten up-to-date zijn.

Uiteraard merken wij hierbij op dat de keuze voor maatregelen te allen tijde een afweging blijft tussen veiligheid, betaalbaarheid en werkbaarheid binnen de organisatie. De set aan maatregelen zal hiermee tussen organisaties verschillen, afgestemd op de specifieke behoeften.

5.2 Nieuw belastingsysteem met ingang van 2022

Aandachtspunten bij inrichting en overgang nieuw belastingsysteem

Aandachtpunten bij inrichting van nieuw belastingsysteem

De gemeente Goirle heeft de uitvoering van de gemeentelijke belastingen en heffingen sinds een aantal jaren uitbesteed aan TOG. De uitvoeringsovereenkomst met TOG loopt eind 2021 af. Wij hebben vernomen dat met ingang van 2022 afscheid wordt genomen van TOG en dat de gemeentelijke belastingen en heffingen door de gemeente zelf worden uitgevoerd. Als gevolg hiervan wordt uw huidig belastingsysteem “VRiS Belastingen” (leverancier TOG) met ingang van 2022 vervangen door een nieuwe applicatie “Level”.

Wij benadrukken dat belangrijke beheersmaatregelen zoals functiescheiding (4-ogenprincipe), het muteren en autoriseren van stamgegevens, controles gericht op de volledigheid van de gemeentelijke belastingen en heffingen en loggingsfunctionaliteiten mooie kansen biedt om verder in-control te komen. Vanuit controleperspectief geven wij graag een aantal belangrijke aandachtspunten mee die hier verder aan bij kunnen dragen:

- Bepalen van functiescheiding in de gebruikers rollen/autorisaties, waarbij geaccordeerde normposities worden opgesteld alsmede na inrichting en aanvullend (minimaal) jaarlijks wordt gecontroleerd of alle aanwezige accounts en autorisaties nog valide zijn;
- Inrichting van adequate wachtwoordeisen (betreft: Multi-Factor Authenticatie, Single-Sign-On, geen accounts vrijgesteld van verplicht wachtwoord wijzigen);
- Inrichten van audit-trails op mutaties aan de gebruikers gedurende het boekjaar;
- Een procedure voor wijzigingsbeheer beschrijven en hanteren. In deze procedure zijn een aantal (OTAP) fases van belang, namelijk: aanvragen wijziging, risico/impact analyse, goedkeuring van wijzigingsverzoek, testen in testomgeving (aanpak en resultaten), goedkeuring voor in-productie name van wijziging en migratie naar productie;
- Het aantal beheeraccounts en generiek genaamde accounts zoveel mogelijk in te perken. Tevens een duidelijke functiescheiding aanbrengen tussen het gebruik en het beheer van de applicatie. Dit bijvoorbeeld door de kritische applicatiebeheer processen (zoals o.a. het aanmaken, verwijderen, wijzigen van gebruikers en rechten, het wijzigen van systeeminstellingen zoals wachtwoordinstellingen, loginstellingen, het installeren van updates) te centraliseren bij de ICT-afdeling.

Bij een overgang van “VRiS Belastingen” naar “Level” dienen uiteraard ook werkzaamheden en vastleggingen gedaan te worden om te borgen dat de overzetting van (historische) data volledig en juist is. In het kader van de jaarrekeningcontrole 2022 is dit tevens van belang om te voorkomen dat het achteraf tot problemen ten aanzien van de betrouwbaarheid leidt. Hieronder hebben wij een aantal belangrijke aandachtspunten opgenomen om grip te krijgen op de conversie van data.

- Het in kaart brengen van de belangrijkste registraties (scope van registraties zoals: kohieren, stamgegevens, overlopende posten etc.)
- Het opstellen van een conversieplan voor het overzetten (type overzetting zoals bijv. opschonen en verrijken van data);
- Het bepalen van een controle-aanpak om betrouwbaarheid (volledigheid en juistheid) van conversiedata vast te stellen;
- Het laten uitvoeren van een onafhankelijke review onderzoek op het conversiedossier om daarmee de betrouwbaarheid van de conversie vast te stellen.

Graag denken wij tijdig met u mee over de impact van deze aandachtspunten, zodat geborgd kan worden dat uitkomsten van het nieuwe systeem dienstbaar zijn aan de interne (en externe) controle. Volledigheidshalve melden we dat we in het kader van onze jaarrekeningcontrole 2022 aanvullende werkzaamheden dienen te verrichten in de vorm van een IT-audit op het nieuwe belastingsysteem “Level”. Graag maken wij hier tijdig aanvullende afspraken over met uw organisatie.

5.3 Bevindingen IT-beheersing | Overall beeld

Logische toegangs-beveiliging (criteria 1) nog ontoereikend bij K2F.

Logische toegangs-beveiliging (criteria 1, 2 en 5) nog ontoereikend bij S4SD.

Change management nog ontoereikend bij S4SD.

Continuïteit is toereikend.

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar de bijlage

PROCES	K2F 2021	S4SD 2021
1. Procedure autorisatiebeheer		
2. Periodieke controle op juistheid ingerichte autorisaties		
3. Identificatie van gebruikers voor toegang tot systemen en data		
4. Wachtwoordbeleid (authenticatie)		
5. Administrators en superusers		
6. Wijzigingenbeheer updates en gescheiden omgevingen (ontwikkel-test-productie)		
7. Continuïteit (fysieke toegang, back-up, monitoring en restoretest). *1	Via Equalit	

KORTE OMSCHRIJVING RESULTATEN	
1	**K2F - toekennen rollen/rechten:** Uit voorgaande audit is gebleken dat er een normpositie bestaat voor K2F. Echter op basis van 1 indiensttreding vastgesteld dat de toekenning van rollen geschiedt op basis van inzicht van de leidinggevende en/of naar eigen inzicht van de applicatiebeheerder en niet op basis van de normpositie. **K2F& S4SD - intrekken rollen/rechten:** Voor één willekeurige uitdiensttreding per applicatie vastgesteld dat de rechten tijdig zijn ingetrokken.
2	**K2F:** Er worden een (aantoonbare) periodieke review uitgevoerd op juistheid van ingerichte autorisaties en/of de actualiteit van gebruikersaccounts. **S4SD:** Er worden geen (aantoonbare) periodieke review uitgevoerd op juistheid van ingerichte autorisaties en/of de actualiteit van gebruikersaccounts.
3	Generieke accounts binnen applicatie K2F zijn verklaarbaar bevonden.
4	De wachtwoordvereisten voor K2F en S4SD voldoen aan de BDO minimum best practice. *2
5	**K2F:** Superusers zijn beperkt tot de beheerorganisatie. **S4SD:** In S4SD Hilvarenbeek zijn 2 medewerkers uit de lijnorganisatie met superuserrechten. In S4SD Oisterwijk zijn 4 voormalig applicatiebeheerders met superuserrechten. Hiermee zijn superusers niet beperkt tot het strikt noodzakelijke.
6	**K2F:** Testwerkzaamheden worden gedocumenteerd en uitgevoerd door eindgebruikers. Daarnaast wordt inzichtelijk akkoord gegeven voor inproductiename van de wijziging. **S4SD:** Testwerkzaamheden worden niet structureel gedocumenteerd en uitgevoerd door eindgebruikers. Er wordt wel een aantoonbaar akkoord gegeven voor inproductiename van de wijziging.
7	Continuïteitsmaatregelen zijn getroffen door de serviceorganisatie en de gemeente Oisterwijk ontvangt hier assurance over. *1 *2

onvoldoende verbeterpunten voldoende

*1 = *Dit punt behoeft nuancering gezien het bestaan en de werking van maatregelen in februari 2022 pas beoordeeld kan worden. Er is geen aanleiding om te stellen dat de maatregelen ineffectief zijn voor boekjaar 2021.*

*2 = *Hoewel dit punt toereikend is, zijn in de bijlage zijn aanbevelingen opgenomen.*

5.4 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol (1/2)

IT en onze natuurlijke adviesrol

De organisatie heeft een verdere verbetering van de IT-beheersing voor ogen

IT-werkzaamheden en onze natuurlijke adviesrol

Vanuit onze natuurlijke adviesrol willen wij u attenderen op een aantal ontwikkelingen op het gebied van IT. Deze ontwikkelingen zijn niet altijd direct gerelateerd aan onze controle van de jaarrekening, maar wel van belang voor uw bedrijfsvoering. Wij schetsen in deze managementletter de ontwikkelingen op hoofdlijnen met als doel u te attenderen op deze ontwikkelingen. Dat betekent ook dat wij geen uitgebreid onderzoek hebben uitgevoerd naar deze onderwerpen. Waar relevant, zijn ze specifiek gemaakt voor uw organisatie.

Professionalisering van IT-beheersing

Ten aanzien van IT-beheersing zien wij dat gemeente Goirle, Hilvarenbeek en Oisterwijk (hierna: GHO) de nodige tijd en middelen investeert om verder in control te komen binnen deze geautomatiseerde gegevensverwerking. De maatregelen die wij hebben getoetst omtrent de IT General Controls (logische toegangsbeveiliging, wijzigingsbeheer en continuïteit) laten zien dat u de afgelopen jaren stappen hebt gezet en bezig bent om verscheidene verbeteringen te implementeren.

5.4 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol (2/2)

Informatiebeveiliging bij GHO

Ontwikkelingen bij GHO

Aandachtspunten bij implementeren Baseline Informatiebeveiliging

Ontwikkelingen rondom Informatiebeveiliging

Vanuit onze natuurlijke adviesrol willen wij u attenderen op een aantal ontwikkelingen op het gebied van IT. Deze ontwikkelingen zijn niet altijd direct gerelateerd aan onze controle van de jaarrekening, maar wel van belang voor uw bedrijfsvoering. In deze informatie gedreven samenleving verwerken organisaties (steeds meer) grote hoeveelheden informatie, veelal digitaal maar ook nog analoog. Hoewel organisaties in veel gevallen afhankelijk zijn van deze informatie en deze veel voordelen biedt, kan het voor uw organisatie of voor anderen ook de nodige risico's opleveren. Deze risico's kunnen leiden tot vervelende en impactvolle incidenten; door digitalisering worden de gevolgen van incidenten ook steeds omvangrijker, met mogelijk een serieuze impact op de organisatiedoelen. Zicht en grip op de risico's rondom informatie vereisen zicht en grip op de informatie zelf en de toegang daartoe.

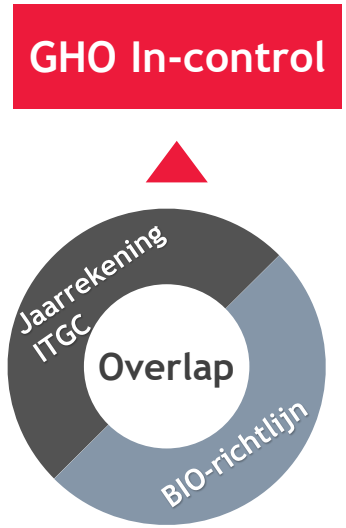
In de (lokale) overheidsbranche valt de Baseline Informatiebeveiliging Overheid (hierna: BIO) en IT-beheersing in het kader van de jaarrekeningcontrole niet meer los van elkaar te zien. Onze verwachting is dat er in de toekomst een geïntegreerde 'Single Information Single Audit'-aanpak voor dergelijke audits zal komen. De basis voor een geïntegreerde aanpak is een Information Security Management Systeem (ISMS). Waarmee u in kaart kunt brengen welke audits gekoppeld zijn aan welke BIO-normen. Zoals bijvoorbeeld de IT General Controls uit deze IT audit.

De ITGC-maatregelen die wij hebben getoetst omtrent logische toegangsbeveiliging, wijzigingsbeheer en continuïteit laten zien dat er vervolgacties nodig zijn om tot een beheersbaar niveau te komen op dit onderdeel. In de bijlage hebben wij vanuit onze IT General Controls een referentie naar de vergelijkbare BIO-norm toegevoegd*.

Daarnaast willen bij het implementeren baseline, u attenderen op een aantal belangrijke stappen bij het implementeren van een BIO-baseline:

- Het uitvoeren van een nulmeting (gap-analyse) waarin zowel de implementatie van de huidige baseline als de te ondernemen stappen voor de BIO in kaart worden gebracht;
- Het trainen van het lijnmanagement door middel van bijvoorbeeld workshops, om een risico gestuurde aanpak (omtrent informatiebeveiliging) te integreren in de bedrijfsvoering en bewustwording omtrent verantwoordelijkheden van informatiebeveiliging te creëren;
- Het uitvoeren van een security scan voor het bepalen van de vereiste maatregelen per proces;
- Het implementeren van de beheersingsmaatregelen die op basis van deze security scan zijn bepaald;
- Het uitvoeren van een BIO-audit om te bepalen in hoeverre uw organisatie voldoet aan de BIO-vereisten.

Graag denken wij tijdig met u mee over de gevolgen van de BIO voor de interne beheersing van de processen.

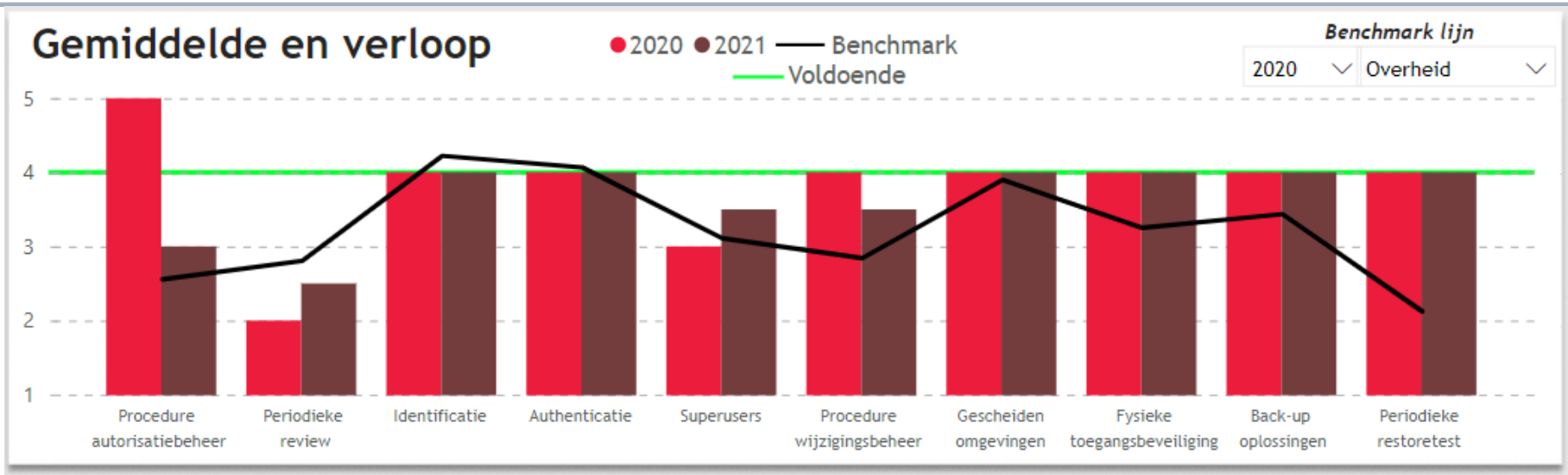


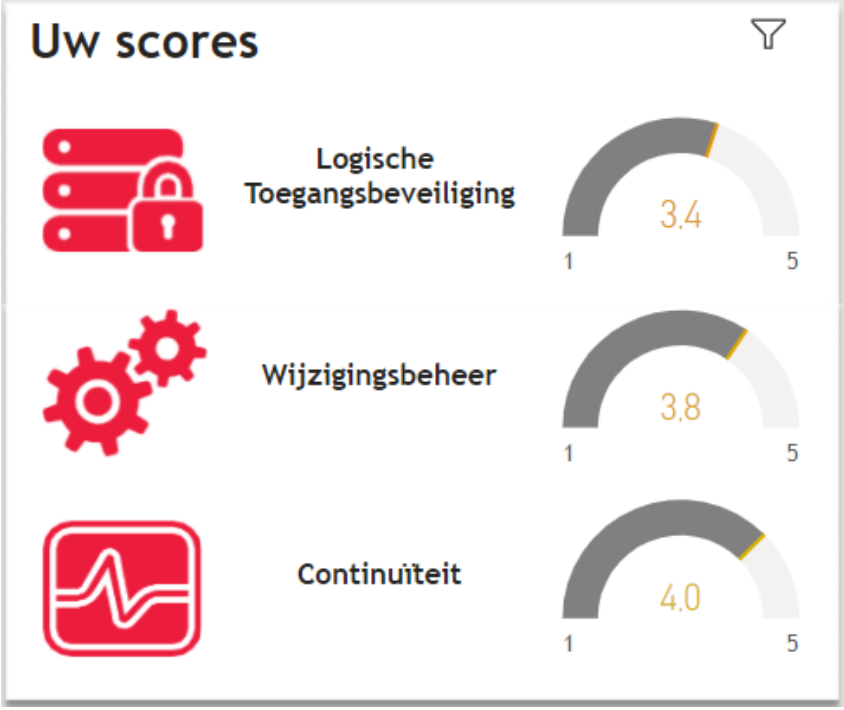
** = De BIO-normen zijn overgenomen uit het document 'Baseline Informatiebeveiliging Overheid v1.04zv' en hier kunnen geen rechten aan ontleend worden.*

5.5 IT-audit | Benchmark Overheid

Wij hebben een benchmark ontwikkeld welke uw scores afzet tegen het gemiddelde van onze klanten binnen de Overheidssector. Een impressie van deze benchmark is hier weergegeven.

In 2020 was alleen Key2Financiën in scope. Over 2021 is de gemiddelde score van Key2Financiën en Suite4Sociaaldomein opgenomen.





Uitleg Benchmark

Op basis van onze kennis en inzichten die wij hebben opgedaan bij de uitvoering van IT audits hebben wij een benchmark ontwikkeld. Deze benchmark geeft inzicht in de IT audit resultaten van uw organisatie afgezet tegen het gemiddelde van vijftig van onze klanten binnen de Overheidssector.
Bovendien laat deze benchmark zien hoe uw organisatie zich heeft ontwikkeld op het gebied van IT-beheersing over de afgelopen jaren. Hierin is een score van 1 tot en met 5 per norm weergegeven waarbij BDO een score van minimaal 4 toereikend acht.

Deze pagina geeft een korte impressie van onze interactieve benchmark. Graag presenteren wij u de aanvullende inzichten en gaan wij met u in gesprek over het vervolg.

6. Vooruitblik jaarrekening 2021

6.1 Vooruitblik jaarrekening 2021

6.1 Vooruitblik jaarrekening 2021

Aandachtspunten voor jaarrekeningcontrole 2021

Gemaakte afspraken voor jaarrekeningcontrole 2021

Wij hebben afgesproken om net als voorgaand jaar (ruim) voorafgaand aan de accountantscontrole een scan uit te voeren op het (digitale) jaarrekeningdossier ter beoordeling of de opgevraagde controledocumentatie is opgeleverd en een goede basis biedt voor de aanvang van onze werkzaamheden.

Wij onderkennen de volgende aandachtspunten voor de jaarrekeningcontrole 2021:

- Zichtbare follow-up van de bevindingen en aanbevelingen uit deze managementletter;
- Position paper ten aanzien van de financiële risico's en waarborgen rondom de coronacrisis (zie hoofdstuk 2.1);
- Position paper ter onderbouwing van de volledige, juiste en rechtmatige verantwoording van de gemeentelijke belastingen en heffingen in de jaarrekening (zie hoofdstuk 4.1);
- Actualisatie van de grondexploitatieopzetten per 31-12-2021 inclusief financiële doorrekeningen;
- Aanlevering van de spendanalyse over de gehele vierjaarsperiode 2018-2021 met een interne toetsing op de naleving van de Europese aanbestedingsregels. Hierbij dient rekening te worden gehouden met de aandachtspunten uit de notitie 'Uitvoering van controle op aanbestedingsrechtmatigheid bij jaarrekeningcontrole van decentrale overheden' van de NBA-SDO. Verder vragen wij uw specifieke aandacht voor de betrouwbaarheid van het gehanteerde lijstwerk om de volledigheid van de uitgevoerde spendanalyse te waarborgen;
- Aanlevering van een overzicht van de lasten Wmo per zorgaanbieder met de onderliggende productieverantwoordingen en bijbehorende controleverklaringen inclusief een verschillenanalyse. In dit kader hebben wij uw organisatie reeds gefaciliteerd met een format met de juiste documentatievereisten;
- Aansluiting tussen de saldi in de onderhoudsvoorzieningen per 31-12-2021 en de beheerplannen inclusief een verschillenanalyse;
- Aanlevering van de WNT-verantwoording en onderliggende brondocumentatie;
- Aanlevering van een volledige (concept) jaarrekening welke reeds intern is getoetst op de naleving van het BBV. Wij zullen u hiervoor de checklist 2021 nog aanreiken;
- Aanlevering van een kwalitatief en kwantitatief goed balansdossier waarop intern een zichtbare 'kwaliteitscheck' is verricht;
- De verantwoordingsinformatie inzake de gemeentelijke belastingen/heffingen vanuit TOG;
- Aanlevering van de 'tax letter' waarin de relevante informatie rondom de fiscaliteiten (Vpb, btw en LB) wordt vermeld. Wij zullen u hiervoor de template nog aanreiken.

Het is van belang dat uw organisatie stuurt op een tijdige realisatie van bovengenoemde afspraken. Dit komt ten goede aan de efficiëntie van het jaarrekeningproces en de jaarrekeningcontrole.

Detailbevindingen IT

Bevinding	PROCEDURE AUTORISATIEBEHEER & PERIODIEKE CONTROLE OP JUISTHEID INGERICHTE AUTORISATIES	Gerelateerde BIO-normen: 9.2.1 | 9.2.2.1 | 9.2.5.1 9.2.2.2 | 9.2.3.1	KANS: Middel
Jaar van constatering	2020 (en 2021)		IMPACT: Middel

	We hebben geconstateerd dat de volgende controles aanwezig zijn: ▶ Voor 1 gebruiker (K2F & S4SD) vastgesteld dat de aanvraag voor toekennen en intrekken structureel wordt vastgelegd in het ticketsysteem; ▶ Voor 1 gebruiker (K2F & S4SD) vastgesteld dat de juiste autorisaties worden toegekend door middel van het toekennen van een functiegroep o.b.v. de functie in de aanvraag. Vastgesteld op basis van inspectie en observaties rondom de procedure autorisatiebeheer (voor zowel K2F & S4SD) dat: ▶ Autorisaties worden toegekend door de applicatiebeheerder o.b.v. functiegroepen waarbij een duidelijke koppeling is tussen de functie en de toe te kennen autorisatiegroep. Daarnaast is er een normpositie beschikbaar, echter worden rechten toegekend o.b.v. eigen inzicht van de applicatiebeheer. Dit geeft vanwege de vaste groepen in tegenstelling tot aparte rollen geen verhoogd risico. Vastgesteld op basis van inspectie rondom de periodieke review dat: ▶ Voor K2F de juistheid van toegekende rollen/rechten en actualiteit van gebruikersaccounts aantoonbaar is gecontroleerd. ▶ Voor S4SD geen aantoonbare controle op rollen/rechten of actualiteit is uitgevoerd.
Risico/Gevolg	In algemene zin bestaat het risico dat bij het ontbreken van adequate naleving op gebruikersbeheerprocedures er mogelijk personen teveel of onterechte rollen/rechten bezitten en hierdoor de functie-scheidingsprincipes mogelijk doorbroken kunnen worden met het risico op ongeautoriseerde handelingen. Tevens bestaat het risico dat een medewerker na uitdiensttreding toegang behoudt tot de betreffende applicaties en hierin transacties kan uitvoeren.
Ons advies/ Uw aanvullende werkzaamheden	**Procedure autorisatiebeheer (bij toekennen van rechten)** Gemeente Goirle, Hilvarenbeek en Oisterwijk (samenwerking GHO) beschikt over een normpositie voor de Key2Financiën waarin de belangrijkste gewenste functiescheidingsprincipes zichtbaar zijn gemaakt. Om administratieve lasten te voorkomen raden we aan om voornamelijk te focussen op de belangrijkste functiescheidingen (en wijzigingen) in de systemen. In navolging hierop raden we aan om dit jaarlijks vooraf door het management te laten goedkeuren, zodat dit organisatie-breed wordt gedragen en baseline biedt. Aan de hand van deze normpositie dienen de verzoeken tot het aanvragen en muteren van gebruikers met rollen en rechten beoordeeld te worden alvorens deze autorisatiegroep/rechten worden toegekend. **Periodieke review (achteraf)** He verdient voor S4SD de aanbeveling om een periodieke review (bijv. halfjaarlijks, jaarlijks) uit te voeren waarin achteraf tegen de bovengenoemde normpositie wordt nagegaan of gebruikers teveel rollen/rechten toegekend hebben gekregen. Daarnaast zou u op basis van de uitdienstlijst periodiek achteraf een controle kunnen uitvoeren om na te gaan of alle uitdiensttreders (tijdig) zijn geblokkeerd voor de applicaties in scope.
Reactie management/ Opvolging	*Reactie 2020: De periodieke controle op autorisaties en actualiteit gaan we oppakken.*

Bevinding	IDENTIFICATIE VAN GEBRUIKERS	Gerelateerde BIO-normen: 9.2.1.1 & 9.2.1.2	KANS: Laag
Jaar van constatering	2021 (geen bevinding)		IMPACT: Laag

	Wij hebben vastgesteld dat aanwezige niet-persoonsgebonden (hierna: generieke) gebruikers binnen Key2Financiën verklaarbaar zijn vanuit gebruiksdoeleinden. ▶ Binnen applicatie Key2Financiën zijn er generieke accounts aanwezig binnen de 3 administraties, dit betreffen systeemaccounts en zijn verklaarbaar vanuit beheerdoeleinden. ▶ Binnen applicatie Suite4SociaalDomein zijn er generieke accounts aanwezig binnen de 3 administraties, dit betreffen systeemaccounts en zijn verklaarbaar vanuit beheerdoeleinden.
Risico/Gevolg	In algemene zin bestaat het risico op generiek genaamde accounts dat met deze accounts ongeautoriseerde wijzigingen worden doorgevoerd, waarnaar op basis van naamgeving niet te achterhalen is wie deze wijzigingen heeft doorgevoerd.
Ons advies/ Uw aanvullende werkzaamheden	Hoewel dit geen bevinding is, raden we in algemene zin Gemeente Goirle, Hilvarenbeek en Oisterwijk (samenwerking GHO) aan om: ▶ Het aantal generieke (beheer)accounts en generiek genaamde accounts binnen de applicatie zoveel mogelijk in te perken, door onnodige accounts te blokkeren of op naam te stellen; ▶ Generieke accounts (met superuser-rechten) waar mogelijk de rechten in te perken naar strikt noodzakelijk en eventueel na te gaan of kritieke handelingen (bijv. toekennen/intrekken van rollen/rechten, fiatteren van uitkeringen) gelogd kunnen worden.
Reactie management/ Opvolging	*Reactie 2020: Het systeemaccount moeten we behouden voor scripts van Equalit en dit blijft beperkt tot maximaal 2 beheerders (Equalit en Centric).*

Bevinding	WACHTWOORDBELEID	Gerelateerde BIO-normen: 9.4.3.1 - 9.4.3.5	KANS: N.V.T.
Jaar van constatering	2021		IMPACT: N.V.T.

Op basis van systeemwaarneming en inspectie van het ISAE3402 assurance-rapport hebben wij vastgesteld dat de volgende wachtwoordvereisten worden afgedwongen:

WACHTWOORDINSTELLINGEN	Key2Financiën (via SSO)	Suite4SociaalDomein (Goirle, Hilvarenbeek, Oisterwijk)
Minimale wachtwoordlengte	8 karakters	10 karakters
Maximale wachtwoordleeftijd	60 dagen	100 dagen
De laatste # wachtwoorden mogen niet hergebruikt worden	6 laatste wachtwoorden	3 laatste wachtwoorden
Het account wordt na # foutieve inlogpogingen geblokkeerd	3 foutieve inlogpogingen	3 foutieve inlogpogingen
Wachtwoordcomplexiteit *	Ingeschakeld	Ingeschakeld
Initiële wachtwoordwijziging	Afgedwongen	Afgedwongen

** = het wachtwoord dient minimaal 1 cijfer, 1 hoofdletter en 1 kleine letter te bevatten. Gebruik van speciale tekens wordt niet afgedwongen.*

Risico/Gevolg

Het potentiële risico op het niet streng genoeg instellen van de complexiteiteis waardoor wachtwoorden kunnen worden geraden na verloop van tijd, wordt gemitigeerd doordat de overige wachtwoordvereisten strenger zijn ingeregeld dan de BDO minimum best practice voorschrijft.

Ons advies/ Uw aanvullende werkzaamheden

Er wordt hiermee voldaan aan de minimale wachtwoordeisen. Ter informatie zijn deze hieronder opgenomen:

WACHTWOORDINSTELLINGEN	BDO best practice norm	BIO norm (excl. 2-factor authenticatie)*[2]
Minimale wachtwoordlengte	6 karakters	8 karakters (of 20 karakters)
Maximale wachtwoordleeftijd	180 dagen	180 dagen
De laatste # wachtwoorden mogen niet hergebruikt worden	3 wachtwoorden	*Niet expliciet benoemd (1 werkdag verschil)*
Het account wordt na # foutieve inlogpogingen geblokkeerd	7 foutieve inlogpogingen	10 foutieve inlogpogingen
Wachtwoordcomplexiteit	Ingeschakeld	Ingeschakeld (vervalt bij min. lengte van 20 karakters)

Dit wachtwoordbeleid dient periodiek te worden beoordeeld op naleving in de organisatie.

** [2]= De BIO-normen zijn overgenomen uit het document 'Baseline Informatiebeveiliging Overheid v1.04zv' en hier kunnen geen rechten aan ontleend worden.*

Reactie management / Opvolging

Reactie 2020: Geen.

Bevinding	SUPERUSER-RECHTEN	Gerelateerde BIO-normen: 9.2.3	KANS: laag
Jaar van constatering	2021		IMPACT: hoog

	Wij hebben vastgesteld dat onderstaande eindgebruikers beschikken over rollen/rechten om autorisaties toe te kennen (superuser-rechten): ▶ In Key2Financiën Goirle zijn 4 accounts aanwezig die beschikken over superuser-rechten. Dit zijn 1 systeemaccount en 4 applicatiebeheerders ▶ In Key2Financiën Hilvarenbeek zijn 4 accounts aanwezig die beschikken over superuser-rechten. Dit zijn 1 systeemaccount en 4 applicatiebeheerders ▶ In Key2Financiën Oisterwijk zijn 4 accounts aanwezig die beschikken over superuser-rechten. Dit zijn 1 systeemaccount en 4 applicatiebeheerders ▶ In Suite4SociaalDomein Goirle zijn 4 accounts aanwezig die beschikken over superuser-rechten. Dit zijn 1 leveranciersaccount en 2 applicatiebeheerders. ▶ In Suite4SociaalDomein Hilvarenbeek zijn 9 accounts aanwezig die beschikken over superuser-rechten. Dit zijn 1 koppelingsaccount, 5 applicatiebeheerders, 1 leveranciersaccount, 1 medewerker WMO en 1 medewerker uitkeringsadministratie. Functiescheiding is doorbroken omdat de medewerker WMO en uitkeringsadministratie (lijnorganisatie) beschikken over superuserrechten. ▶ In Suite4SociaalDomein Oisterwijk zijn 10 accounts aanwezig die beschikken over superuser-rechten. Dit zijn 6 applicatiebeheerders en 4 voormalig applicatiebeheerders. Gezien de voormalig applicatiebeheerders deze rollen/rechten niet meer nodig hebben vanuit hun functie is daarmee niet voldaan aan het least-privilege principe. Doordat het account gebruikt wordt door een medewerkers in de lijnorganisatie en met een voormalige functie als applicatiebeheerder, is de functiescheiding tussen lijnorganisatie en IT-organisatie doorbroken.
Risico/gevolg	Accounts met beheerrechten bezitten alle rechten en kunnen hiermee gewenste functiescheidingen doorbreken en eventueel ongeautoriseerde wijzigingen (bijvoorbeeld stamgegevens of financiële transacties) doorvoeren. Dit is een inherent risico van beheeraccounts. Echter wordt dit risico aanzienlijk verhoogd door deze accounts te beleggen in de lijnorganisatie. Tevens bestaat het risico op generiek en/of verouderde genaamde accounts dat met deze accounts ongeautoriseerde wijzigingen worden doorgevoerd, waarnaar op basis van naamgeving niet te achterhalen is wie deze wijzigingen heeft doorgevoerd.
Ons advies/ uw aanvullende werkzaamheden	Het verdient aanbeveling om een duidelijke functiescheiding aan te brengen tussen het gebruik en het (IT-)beheer binnen de applicatie (Suite4SociaalDomein). Dit bijvoorbeeld door de kritische applicatiebeheer processen (zoals o.a. het aanmaken, verwijderen, wijzigen van gebruikers en rechten, het wijzigen van systeeminstellingen zoals wachtwoordinstellingen, loginstellingen, het installeren van updates) te centraliseren bij de ICT-afdeling.
Reactie management/ opvolging	*Reactie 2020: Vanaf 1 maart 2021 zal de applicatiebeheerder met dubbelfunctie worden gewijzigd naar een fulltime applicatiebeheerdersrol, waardoor functiescheiding aanwezig is.*

Bevinding	WIJZIGINGENBEHEER UPDATES	Gerelateerde BIO-normen: 12.1.2 & 12.1.4	KANS: laag
Jaar van constatering	2021		IMPACT: middel

	We hebben geconstateerd dat de volgende controles aanwezig zijn: ▶ Wij hebben voor 1 doorgevoerde wijziging vastgesteld dat releasenotes worden ontvangen van de leverancier en beoordeeld door de applicatiebeheerders; ▶ De aanvraag bij Equalit wordt gedaan voor het doorvoeren installatie-updates worden vastgelegd in het ticketsysteem; ▶ Er wordt akkoord gegeven op de doorvoer van wijzigingen in de productieomgeving. ▶ De applicaties in scope beschikken over een logisch gescheiden test- en productie omgeving. Wij hebben voor 1 doorgevoerde wijziging per applicatie vastgesteld dat (generiek beoordeeld, verschillen per applicatie hieronder uitgelicht): ▶ De beoordeling van releasenotes niet inzichtelijk is. ▶ Testprotocollen door de applicatiebeheerder beschikbaar gemaakt worden voor Key-users welke eindgebruikers zijn. ▶ Testwerkzaamheden verricht worden door de Key-users. ▶ **K2F:** Testwerkzaamheden worden gedocumenteerd en uitgevoerd door eindgebruikers. ▶ **S4SD:** Testwerkzaamheden worden niet structureel gedocumenteerd en uitgevoerd door eindgebruikers. ▶ Applicatiebeheerders geven akkoord voor inproductiename aan partij Equalit.
Risico/Gevolg	In algemene zin bestaat het risico dat testwerkzaamheden niet op basis van specifieke criteria vanuit de lijnorganisatie worden uitgevoerd. Hierdoor wordt mogelijk niet effectief en efficiënt getest wat ten koste kan gaan van de kwaliteit van de testwerkzaamheden en de productiviteit. Indien de testresultaten voor het in productie nemen van de wijziging niet structureel worden vastgelegd, bestaat het risico achteraf niet kan worden vastgesteld of een softwarewijziging terecht in de productieomgeving is geplaatst. Als gevolg van de constatering van het actieve testaccount en de standaard toegang van de IT-leverancier Centric in de productieomgeving, bestaat het risico dat mogelijk verstoringen ontstaan doordat, zonder akkoord, onbeheerste wijzigingen worden doorgevoerd in de productieomgeving.
Ons advies/ Uw aanvullende werkzaamheden	In algemene zin verdient het de aanbeveling om een procedure voor wijzigingsbeheer te beschrijven en te hanteren. In deze procedure zijn een aantal (OTAP) fases van belang, namelijk: ▶ Aanvragen wijziging; ▶ Risico/impact analyse; ▶ Goedkeuring van wijzigingsverzoek; ▶ Testen in testomgeving (aanpak en resultaten); ▶ Goedkeuring voor in-productie name van wijziging; ▶ Migratie naar productie. We raden aan om bovengenoemde stappen structureel vast te leggen voor belangrijke wijzigingen en tenminste de belangrijkste functionaliteiten/handelingen conform een testscenario te testen. Voor kleinere wijzigingen (bijv. patches, bug-fixes) raden we aan de minimale stappen (testvastleggingen en akkoord) minimaal te documenteren. Het verdient aanbeveling om een duidelijke functiescheiding aan te brengen tussen het gebruik en het (IT-)beheer van applicaties Key2Financïen. Daarom raden we aan om de leveranciersaccounts alleen in te schakelen wanneer een inproductiename uitgevoerd dient te worden.
Reactie management/ Opvolging	*Reactie 2020: Nemen deze aanbeveling ter harte.*

Bevinding	IT CONTINUÏTEIT	Gerelateerde BIO-normen: 11.2| 12.3.1.1 - 12.3.1.4 | 12.3.1.5	KANS: laag
Jaar van constatering	20201 (geen bevinding)		IMPACT: laag

	We hebben geconstateerd dat de volgende controles aanwezig zijn:
	▶ De verantwoordelijkheid voor de back-ups en recovery ligt bij serviceorganisatie Equalit;
	▶ De verantwoordelijkheid voor de hosting van data van Key2Financiën ligt bij Equalit en sub-service organisatie KPN NL datacenter en Global-E en beschikt over een ISAE3402 verklaring type II;
	▶ Serviceorganisatie Equalit (en subserviceorganisatie KPN NLDC en Global) beschikt in opzet over:
	  ▶ Fysieke beveiligingsmaatregelen tot de serverruimte (UPS, brandmelder, blusser en temperatuurregeling);
	  ▶ Een ingericht back-upschema met bijhorende retentietijden en monitoring op foutieve back-ups;
	  ▶ Een periodieke restore-test van de productie-data uit de systemen.
	▶ Over de fysieke beveiligingsmaatrelen wordt per jaareinde zekerheid afgegeven over de effectiviteit van deze beheersmaatregelen middels de ISAE3402-assurance verklaring (werking over de gehele periode);
	
	▶ De assurance-rapportage stelt dat 'Beheersmaatregelen bij de deelnemer' inzake continuïteit dienen te zijn ingericht. Deze verantwoordelijkheden zijn niet formeel opgenomen in de Service Level Agreement met serviceorganisatie Equalit. Dit omvat onder andere maatregelen zoals een uitwijklocatie en Disaster recovery Plan voor de fysieke deelnemerlocatie van de Gemeente Goirle, Hilvarenbeek en Oisterwijk (en de samenwerking GHO)

Risico/Gevolg	Wanneer de uitwijktesten nog niet zijn uitgevoerd, bestaat het risico dat de kantoorruimte niet beschikbaar is in geval van nood. Het risico is echter beperkt vanwege het feit dat er tot op heden nog geen verstoringen hebben voorgedaan en een thuiswerkplek-faciliteiten zijn georganiseerd.
Ons advies/ Uw aanvullende werkzaamheden	*Dit punt behoeft nuancering vanwege het feit dat de ISAE3402-verklaring jaarlijks gepubliceerd wordt aan het begin van 2021.* Vanuit een kritische blik raden wij aan om per jaareinde de assuranceverklaring op te vragen bij de serviceorganisatie Equalit en na te gaan: ▶ Wat de scope van de assuranceverklaring betreft en of dit overeenkomt met de afgenomen diensten bij deze partij; ▶ Wat de periode van de assuranceverklaring betreft (gehele boekjaar of gedeelte van het jaar); ▶ In hoeverre de controlemaatregelen rondom fysieke toegangsbeveiliging, back-up/monitoring en periodieke restore-test toereikend zijn; ▶ Welke aanvullende controlemaatregelen (ref: beheersmaatregelen bij de deelnemer) worden verwacht van de samenwerking GHO. Wij raden aan om bijzonderheden ten opzichte van bovengenoemde aandachtspunten te bespreken met de serviceorganisatie, indien hier aanleiding toe is.
Reactie management/ Opvolging	*Reactie 2020: Nemen deze aanbeveling ter harte.*

bdo.nl