



MANAGEMENT LETTER

Gemeente Gouda

3 december 2019

IBDO

Aanbiedingsbrief

Gemeente Gouda
T.a.v. het college van B&W
Postbus 1086
2200 BB Gouda

Rotterdam, 3 december 2019

Kenmerk: MS/MF/RA11433

Ter informatie

De digitale versie van dit document is vanaf de inhoudsopgave interactief. Aan de hand van de navigatiebalk onderaan de pagina en/of de menustructuur bovenaan de pagina kan door het document genavigeerd worden.



VORIGE PAGINA



VOLGENDE PAGINA



DASHBOARD



AANBIEDINGSBRIEF

Geacht college,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2019 van de gemeente Gouda brengen wij u met deze management letter 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.

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 management letter is daarom van nature kritisch van aard. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelfcontrolerend vermogen van uw organisatie.

Wij vertrouwen erop u met deze management letter naar aanleiding van onze interim-controle 2019 van dienst te zijn geweest.

Wij willen de medewerkers in uw organisatie bedanken voor de prettige samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,

BDO Audit & Assurance B.V.
namens deze,

w.g. C.M. Steehouwer MSc RA



1. DASHBOARD



2. ONTWIKKELINGEN & AANDACHTSPUNTEN



3. BEVINDINGEN SIGNIFICANTE PROCESSEN



4. IT-BEHEERSING



5. BEVINDINGEN INTERNE CONTROLE



BIJLAGEN

1. Dashboard

1.1 Dashboard

1.1 Dashboard

ONTWIKKELINGEN PROCES JAARREKENINGCONTROLE		AANDACHTSPUNTEN	UW INTERNE BEHEERSING		
- De samenwerking tijdens de interim-controle is prettig en constructief verlopen. Wij merken dat de medewerkers binnen uw organisatie bezig zijn met verbeteren van de organisatie en openstaan voor advies ter verbetering van uw organisatie. Het beheer op de door ons gestelde vragen is goed. Er wordt actief gereageerd en documenten worden snel aangeleverd. - Ten aanzien van de planning van de controle van de grondexploitaties hebben wij nieuwe afspraken gemaakt. Wij zullen in januari al samenkomen om de belangrijkste ontwikkelingen te bespreken en de controle van de grondexploitaties eerder dan de reguliere start van de jaarrekeningcontrole te doen plaatsvinden (dit geldt ook voor de SiSa-controle). - Er zal op korte termijn een afstemmingsoverleg plaatsvinden, waarbij wij met uw organisatie de controle van de (Europese) aanbestedingen zullen bespreken.		- Wij vragen aandacht voor een tijdige taxatie van de NIEGG's (vóór jaareinde 2019). Verwerking van eventuele afwaardering is vereist in de jaarrekening 2019. - Het proces van inkopen en aanbesteden is eind 2018 gewijzigd. De nieuwe opzet zal moeten leiden tot een betere beheersing van alle inkopen van goederen en diensten. Wij vragen aandacht voor de monitoring van de implementatie en uitvoering van de nieuwe procedures. - Wij zien een afwijkend beeld van aanwezigheid van procesbeschrijvingen, instructies etc. Er zijn grote verschillen tussen processen en afdelingen wat betreft diepgang. Wij zijn van mening dat uw gemeente met soms minimale aanpassingen en inzet procesbeschrijvingen sterk kan verbeteren door toevoeging van risico-analyses per proces en beschrijven van IB-maatregelen. - Het opleveren van een volledige datadump (download administratie) met alle voor ons benodigde informatie.	- In het kader van onze controle hebben wij de effectiviteit van de voor onze controle relevante processen beoordeeld. - Voor een organisatie met de omvang van de gemeente Gouda zou de norm moeten zijn dat de processen in opzet, bestaan en werking (inclusief IT) effectief zijn en getoetst worden door de VIC. - Wij kunnen (nog) niet altijd steunen op de interne beheersing in de processen; de VIC en onze controle is daarmee hoofdzakelijk gegevensgericht en achteraf. - Voor de gedetailleerde procesbevindingen verwijzen wij naar hoofdstuk 3 van deze management letter. Deze liggen in lijn met de bevindingen uit de management letter 2017 en 2018. - Opstellen/ actualiseren van de frauderisicoanalyse en deze te implementeren in de procesbeschrijvingen.		
BEVINDINGEN SIGNIFICANTE PROCESSEN		BEHEERSING IT		VERBIJZONDERDE INTERNE CONTROLE	
- Twee processen vragen op korte termijn aandacht: memoriaalboekingen en factuuraafhandeling. In deze processen zijn tekortkomingen geconstateerd ten aanzien van de controletechnische functiescheidingen. - Het proces inzake inkopen en aanbesteden is aangepast en verbeterd. De uitkomsten zullen pas in 2020 zichtbaar zijn. Voor 2019 betekent dit dat gegevensgericht aan de hand van op te leveren spendanalyse aangetoond moet worden of contracten (Europees) zijn aanbesteed. - Ten aanzien van enkele processen dient nog VIC plaats te vinden. Belangrijkste processen zijn: parkeeropbrengsten, omgevingsvergunningen. - Er vindt onvoldoende vastlegging plaats van controle op prestatielevering in het primaire proces. Tevens vinden te weinig gegevensgerichte werkzaamheden plaats om vast te stellen dat prestatielevering voor de totale massa voldoende heeft plaatsgevonden.		<i>De IT-beheersing is in de basis op orde.</i> Wij beoordelen de betrouwbaarheid en continuïteit IT voor zover relevant voor de controle van de jaarrekening ten aanzien van logische toegangsbeveiliging, wijzigingsbeheer en continuïteit - Logische toegangsbeveiliging is nagenoeg toereikend - Change management is toereikend - Continuïteit is toereikend Ten aanzien van de IT hebben wij de volgende bevindingen: - Voor de applicaties in scope is nog geen formele normpositie opgesteld met de rollen per functionaris; - Er zijn er 3 niet-persoonsgebonden gebruikersaccounts in S4SD, waarvan het wachtwoord in 2019 niet is gewijzigd (waarvan 1 verklaarbaar is vanuit gebruikersdoeleinden).		- Onze conclusies in relatie tot de vereisten vanuit de controle-standaard (COS) 610 zijn in 2018 ongewijzigd. - Onze samenwerking met de VIC kan nog worden verbeterd. Tijdige afstemming werkzaamheden en selecties zorgen voor een betere controle. - De meerwaarde van de VIC voor de organisatie & onze controle kan nog worden vergroot door 'aan de voorkant' nog explicieter aandacht te geven aan de opzet en inrichting van de AO/IB per proces, alsmede de advisering daaromtrent. - In hoofdstuk 3 van deze management letter is aangegeven tot welke aanvullende werkzaamheden onze interim-bevindingen moeten leiden. Graag spreken wij af welke zaken primair door de VIC, en welke door ons worden opgepakt.	
DASHBOARD	AANDACHTSPUNTEN	SIGNIFICANTE PROCESSEN	IT-BEHEERSING	INTERNE CONTROLE	BIJLAGEN

2. Ontwikkelingen & Aandachtspunten

- 2.1 Ontwikkelingen in uw bedrijfsvoering
- 2.2 Actualiteiten BBV
- 2.3 Wet normering topinkomens
- 2.4 Aanbestedingsrechtmatigheid

2.1 Ontwikkelingen in uw bedrijfsvoering



Ongewijzigde
bedrijfsvoering

Ontwikkelingen in uw bedrijfsvoering

De interne beheersing van uw gemeente is relatief ongewijzigd ten opzichte van vorig jaar. Hierdoor blijft onze controle-aanpak ook voor 2019 hoofdzakelijk gegevensgericht zal zijn. De belangrijkste ontwikkelingen binnen uw gemeente die van belang zijn voor de jaarrekeningcontrole, hebben wij onderstaand opgenomen.

Belangrijke ontwikkelingen:

- ▶ Vanaf 2021 zal het college van burgemeester en wethouders een (onderbouwde) mededeling doen omtrent rechtmatig handelen. De gemeente heeft deze ontwikkeling reeds opgepakt en is al bezig met de voorbereidende werkzaamheden.
- ▶ De landelijke ontwikkelingen inzake het stikstofprobleem en de pfasproblematiek lijken de grondexploitaties van de gemeente Gouda vooralsnog op korte termijn niet te al te veel te beïnvloeden.

Ontwikkelingen ten aanzien van de jaarrekeningcontrole

De interne beheersing van uw gemeente is relatief ongewijzigd ten opzichte van vorig jaar. Hierdoor blijft onze controle-aanpak ook voor 2019 hoofdzakelijk gegevensgericht. De belangrijkste ontwikkelingen binnen uw gemeente die van belang zijn voor de jaarrekeningcontrole, hebben wij onderstaand opgenomen.

Belangrijke ontwikkelingen:

- ▶ De samenwerking tijdens de interim-controle is prettig en constructief verlopen. Wij merken dat de medewerkers binnen uw organisatie bezig zijn met verbeteren van de organisatie en openstaan voor advies ter verbetering van uw organisatie. Het beheer op de door ons gestelde vragen is goed. Er wordt actief gereageerd en documenten worden snel aangeleverd.
- ▶ Ten aanzien van de controle van de grondexploitaties hebben wij andere afspraken gemaakt t.a.v. de jaarrekeningcontrole. Wij zullen in januari al samenkomen om de belangrijkste ontwikkelingen te bespreken van de ontwikkelingen t.a.v. de grondexploitaties. De controle zal direct bij start van de eindejaarscontrole worden opgepakt.
- ▶ Wij zullen proberen de SiSa-controle eerder dan de reguliere start van de jaarrekeningcontrole te doen plaatsvinden.
- ▶ Er zal op korte termijn een afstemmingsoverleg plaatsvinden, waarbij wij met uw organisatie de controle van de (Europese) aanbestedingen zullen bespreken (op basis van de SDO notitie).
- ▶ Wij willen graag met uw organisatie in gesprek over de doorontwikkeling van het 'three lines of defence model'. Wij zien uitdagingen en kansen voor uw organisatie om de interne beheersing te verbeteren en de verbijzonderde interne controle effectiever uit te voeren.
- ▶ Diverse VIC-werkzaamheden moeten nog wel uitgevoerd worden. Wij zullen begin januari 2020 deze werkzaamheden reviewen.
- ▶ Aandachtspunt voor de organisatie blijft de wijze van opstellen van begrotingswijzigingen en investeringskredieten. Dit vindt vaak plaats in totaalbedragen. Voor inzichtelijkheid adviseren wij de gemeenteraad per investeringskrediet etc. een afzonderlijk besluit te nemen. Dit is voor reserves reeds door de gemeente aangepast vanaf het 2e ijkmoment 2019.
- ▶ Aandachtspunt voor de controle van de jaarrekening 2019 is een goede datadump van alle boekingen uit de grootboekadministratie. Het lijkt er op dat wij niet alle gegevens ontvangen, waardoor de waarde voor onze controle van deze dump zeer beperkt is. Wij hebben vernomen dat dit probleem waarschijnlijk eenvoudig op te lossen is, zonder dat de gemeente nog investeringen hoeft te doen in het boekhoudpakket dat vervangen zal worden.

Samenwerking met uw
gemeente is goed.

Afspraken voor de
jaarrekeningcontrole
zijn reeds gemaakt.

Aandachtspunt blijft de
transparantie van de
besluitvorming
voorgelegd aan de
raad.

2.2 Actualiteiten BBV (1/3)

Nog slechts 2 keer per jaar V&A van de commissie BBV

Voorziening voor achterstallig onderhoud verplicht

Meer aandacht voor registratie activa en asset management

BBV Actualiteiten

De wijzigingen in het Besluit Begroting en Verantwoording van gemeenten en provincies (BBV) lijken dit jaar beperkt. Wel gebruikt de commissie BBV vanaf 2019 een nieuwe website, wat ook gevolgen heeft voor het stellen van vragen en de beantwoording. De commissie heeft in 2018 besloten antwoorden op vragen per half jaar te publiceren. Elk halfjaar worden dan die vragen en antwoorden gepubliceerd, waarvan de commissie van mening is dat deze meerwaarde bieden voor iedereen ten opzichte van de notities. Wij lichten ter voorbereiding op het jaarrekeningtraject 2019 hieronder enkele BBV ontwikkelingen kort toe.

Achterstallig onderhoud

In geval van achterstallig onderhoud, waarbij sprake is van kapitaalvernietiging en/of onveilige situaties, moet op basis van artikel 44 lid 1a BBV een voorziening worden gevormd. Deze richtlijn is een aanscherping ten opzichte van eerder gepubliceerde notities. Deze bepaling treedt in werking met ingang van het begrotingsjaar 2019. Derhalve ligt meer nadruk op achterstallig onderhoud en de beheersplannen met betrekking tot de gemeentelijke activa (ofwel assets). In dit kader wordt de noodzaak van een adequaat asset management (nog) zichtbaarder. Onder asset management wordt verstaan “de systematische en gecoördineerde activiteiten waarmee een organisatie haar bedrijfsmiddelen optimaal beheert (vanaf de investering) en prestaties, risico's en kosten over de levensduur volgt met als doel een optimale bijdrage te leveren aan de strategie van de organisatie”.

Belangrijke vragen voor gemeenten vanuit het perspectief van assetmanagement en de notitie MVA betreffen:

- ▶ Zijn alle wezenlijke activa / assets geregistreerd in een activaregister, ook die eventueel off balance staan, geen boekwaarde meer hebben, in het verleden niet geactiveerd zijn en/of weinig tot geen boekwaarde meer hebben? In hoeverre zijn inventarisaties hiervan actueel?
- ▶ Bestaan er ten aanzien van deze assets actuele beheersplannen? Zo ja, van welk jaar dateren die, hoe worden die geactualiseerd en met welke frequentie?
- ▶ Leiden de beheersplannen tot een (materieel) goede inschatting van de lasten in de jaarrekening en/of begroting en wordt dit intern gemonitord?
- ▶ Zijn er adequate voorzieningen getroffen voor achterstallig onderhoud dan wel zijn de onderhoudskosten adequaat afgedekt in meerjarenperspectief?
- ▶ Zitten hier mogelijk nog (significant) risico's en mogelijke tekorten in?

ACTIEPUNT: Wij verzoeken u een goede analyse (position paper) te maken ter onderbouwing van uw standpunt dat u in de jaarrekening 2019 verwerkt, zowel ten aanzien van de voorziening achterstallig onderhoud (juistheid én volledigheid) als ten behoeve van de paragraaf onderhoud kapitaalgoederen.

2.2 Actualiteiten BBV (2/3)



Nieuwe notitie
grondexploitatie

Grondexploitatie

De commissie BBV heeft in juli 2019 een nieuwe notitie gepubliceerd; de notitie grondbeleid in begroting en jaarstukken (2019). Sinds de wijziging van het BBV in 2016 heeft de commissie BBV diverse uitingen gedaan en een veelheid aan vragen beantwoord over grond-exploitatie en grondbeleid en daarmee samenhangende problematiek. Om een en ander transparanter te maken is besloten de verschillende uitingen samen te voegen in één document. Daarbij zijn niet alleen de bestaande notities over grondexploitatie en faciliterend grondbeleid aangevuld en geactualiseerd, maar zijn ook hoofdstukken toegevoegd over het belang van het grondbeleid voor raadsleden en over de paragraaf grondbeleid en de overige paragrafen. Hiermee wordt specifiek ingegaan op de informatiebehoefte voor de raad.

2019 laatste jaar
overgangsregeling
NIEGG's

Oude NIEGG's

Voor de Niet In Exploitatie Genomen Gronden (NIEGG's) die per 1 januari 2016 uit exploitatie zijn genomen en rechtstreeks zonder afwaardering zijn omgezet naar een materieel vast actief (ingangsdatum Wijzigingsbesluit artikel 2 lid 2) is 2019 het laatste jaar van de overgangsbepaling. Deze overgangsbepaling heeft een looptijd van 4 jaar gehad. Uiterlijk 31 december 2019 moet een toets plaatsvinden op de marktwaarde van deze gronden tegen de geldende bestemming op het moment van de marktwaardetoets. Wordt daarbij een duurzame waardevermindering vastgesteld dan dient dit uiterlijk 31 december 2019 te leiden tot een afwaardering van deze gronden. Bij de interim-controle hebben we dit besproken en ons is medegedeeld dat enkele oud NIEGG's nog getaxeerd zullen worden vóór opstellen van de jaarrekening 2019.

ACTIEPUNT: indien deze marktwaardetoets in de achterliggende vier jaar niet heeft plaatsgevonden dient uiterlijk 31 december 2019 gezorgd te worden voor een actuele taxatie van deze strategische gronden. Een eventuele afwaardering dient in de jaarrekening 2019 te worden verwerkt.

1 nieuwe stellige
uitspraak

Warme gronden

Een nieuwe stellige uitspraak in het BBV heeft betrekking op de zogenaamde 'warme gronden'. Dit zijn gronden die door de gemeente zijn aangeschaft met oogmerk tot toekomstige ontwikkeling, maar nu nog geen operationele grondexploitatie zijn. Vanwege de grote opgaven in diverse regio's op het gebied van woningbouw, verwerven gemeenten soms gronden met het oog op gebiedsontwikkeling op langere termijn. Dergelijke gronden, waarvan op voorhand vaststaat dat deze als bouwgrond zullen gaan fungeren, maar waarvoor nog geen operationele grondexploitatie is vastgesteld, worden in de regel als 'warme grond' geduid. Deze gronden worden op de balans opgenomen onder de materiële vaste activa tegen verwervingskosten. Ingeval de gronden nog geen bestemming hebben gekregen als bouwgrond dient (tijdelijk) afwaardering plaats te vinden naar de waarde volgens de geldende bestemming.

2.2 Actualiteiten BBV (3/3)

Cumulatieve voorwaarden voor waardering tegen toekomstige bestemming

Aangezien het hierbij gaat om een naar verwachting tijdelijke en niet duurzame waardevermindering, mag onder voorwaarden bij de waardering worden uitgegaan van de grond tegen toekomstige bestemming in plaats van de huidige bestemming. Het betreft de volgende cumulatieve voorwaarden:

- ▶ de gronden moeten deel uitmaken van een door de gemeenteraad vastgestelde visie of masterplan voor (een) concrete en binnen afzienbare tijd te starten grondexploitatie(s), waarin de gebiedsontwikkeling van totaalplan naar deelgrondexploitaties is vastgelegd;
- ▶ de gebiedsontwikkeling mag niet zodanig conflicteren met de uitkomst van de inventarisatie van bedreigingen die de ontwikkeling in de weg kunnen staan, bijvoorbeeld op het gebied van milieu of bereikbaarheid;
- ▶ de visie / het masterplan mag niet strijdig zijn met beleid van de provincie en/of rijk;
- ▶ er is een betrokkenheid bij de gebiedsontwikkeling van provincie of rijksoverheid;
- ▶ het mag alleen gaan om gebiedsontwikkeling voor de bouw van woningen en niet voor bedrijfsterreinen;
- ▶ periodiek (minimaal eens in de 2 jaar) worden de gronden getaxeerd tegen de waarde volgens de toekomstige woningbouwbestemming met inachtneming van de inherente onzekerheden van de ontwikkelmogelijkheden.

Benadrukt wordt dat geen sprake is van een nieuwe categorie NIEGG-gronden.

In de verslaggeving moeten dergelijke gronden vanaf 2019 worden opgenomen onder materiele vaste activa, gronden en terreinen (artikel 52 lid 1 BBV). In de toelichting worden deze afzonderlijk vermeld als gronden, bestemd voor de gemeentelijke gebiedsontwikkeling en als zodanig toegelicht. Gronden die voor 2019 zijn verworven en die vanaf 2019 worden verantwoord als gronden bestemd voor de gemeentelijke gebiedsontwikkeling blijven gewaardeerd tegen de bestaande boekwaarde. Toegepaste afwaarderingen tot en met 2018 mogen niet worden teruggedraaid. Ingeval afwaardering heeft plaatsgevonden via een voorziening dan kan de voorziening wel worden aangepast.

ACTIEPUNT: Wij verzoeken de organisatie voor eind 2019 in kaart te brengen welke warme gronden / strategische gronden in bezit zijn en in hoeverre aan bovenstaande voorwaarden wordt voldaan om af te kunnen zien van een taxatie tegen marktwaarde.

Richtinggevende Notitie grondexploitaties

Naast de commissie BBV heeft ook de commissie BADO d.d. 3 september 2019 een notitie over grondexploitaties uitgebracht. De commissie BADO brengt richtinggevende notities uit met een nadruk op de hoe-vraag en de interpretatie van bestaande wet- en regelgeving. De notities worden gepubliceerd op de website van de commissie BADO. Maar ook de Nederlandse Beroepsgroep voor Accountants (NBA-Sectorcommissie Decentrale Overheden) en de VNG publiceren deze notities.

De meest recente notitie over grondexploitaties beschrijft het gehele proces van woningbehoefte tot het sluiten van een grondexploitatie. Door deze integrale schets ontstaat voor decentrale overheden een beeld over welke stappen zij kunnen zetten en wat de accountant per stap verwacht. De notitie is opgebouwd door middel van vier processtappen voor actief grondbeleid (start en verkenning, planontwikkeling, uitvoering en afsluiting) en vier processtappen voor faciliterend grondbeleid (voorbereiding, besluitvorming, uitvoering en afsluiting). Per processtap ligt in de notitie de focus op de interne documentatie die idealiter aanwezig is bij een gemeente. Het uiteindelijke doel van deze notitie is om de interne beheersing op grondexploitaties voor gemeenten te verbeteren. Vanuit deze optiek zijn ook verscheidene voorbeelden, 'lessen' en risico's (alsmede beheersmaatregelen) beschreven. Wij kunnen deze notitie bij u aanbevelen.

Commissie
Bedrijfsvoering
Auditing Decentrale
Overheden (BADO)
inzake
grondexploitaties

2.3 Wet normering topinkomens

Belangrijkste
wijzigingen 2019 WNT
en algemene
bevindingen vanuit
controle boekjaar 2018

Meer dan de helft van
de WNT-
verantwoordingen
onjuist/ onvolledig

Onze bevindingen bij
de concept WNT-
verantwoording 2018
van uw gemeente

Wet normering topinkomens

De regelgeving omtrent de WNT wordt ieder jaar aangepast en inmiddels is de regelgeving voor 2019 gepubliceerd. Hieronder hebben wij de belangrijkste wijzigingen en onze algemene aandachtspunten vanuit de WNT-controle boekjaar 2018 op een rij gezet:

- ▶ Het bezoldigingsmaximum van een topfunctionaris in fulltime dienstverband bedraagt per 1 januari 2019 € 194.000 (was € 189.000 in boekjaar 2018);
- ▶ Sinds 1 januari 2018 is bepaald dat een functionaris ondanks het neerleggen van zijn/haar functie als topfunctionaris voor een periode van vier jaar vanaf het tijdstip dat de functie niet langer wordt vervuld toch topfunctionaris blijft, indien aan specifieke voorwaarden wordt voldaan;
- ▶ De bezoldigingscomponenten zijn aangescherpt/ verduidelijkt wat onder andere betekent dat het werkgeversdeel van pensioenregelingen en het werkgeversdeel voor vervroegde uittradingen meetelt als WNT-bezoldiging en dat werkgeversbijdragen aan opleidingsfondsen en dergelijke niet meetellen als WNT-bezoldiging;
- ▶ Onderdeel van de WNT-bezoldiging zijn tevens alle belastbare onkostenvergoedingen. Uit de WNT-controle 2018 is gebleken dat niet voor alle Instellingen te allen tijde helder is wat belastbare en niet belastbare onkostenvergoedingen zijn. Belangrijk is dat de kostenvergoedingen fiscaal juist worden verwerkt. Enkel indien onkostenvergoedingen zijn aangewezen als eindheffingsloon ("onder de WKR zijn gebracht") tellen deze niet mee als WNT-bezoldiging. Tijdige en juiste fiscale behandeling is dus essentieel.

Uit de controle over 2018 van de aan ons aangeboden WNT-verantwoordingen van al onze klanten is gebleken dat meer dan de helft onjuist of onvolledig waren. Dit betrof een mix van tekstuele, formele, maar soms ook materiële financiële fouten. Tijdens de controle van de WNT-verantwoording 2018 van uw gemeente, hadden wij de volgende bevindingen:

- ▶ In de concept verantwoording WNT 2018 waren verkeerde omschrijvingen gebruikt; en
- ▶ Het bedrag van de controleberekening van de loonstaat met de concept WNT-verantwoording 2018 sloot niet aan en over de wijze van totstandkoming van de bedragen, opgenomen in de WNT-verantwoording zijn aanvullende vragen gesteld.

2.4 Aanbestedingsrechtmatigheid

Landelijk blijkt dat circa 15% van de controleverklaringen 2018 ten aanzien van rechtmatigheid niet goedkeurend is als gevolg van onrechtmatige aanbestedingen.

Risicogerichte inkoopanalyse in lijn met de SDO-Notitie.

Toenemende aandacht voor aanbestedingsrechtmatigheid

In het kader van de rechtmatigheidscontrole blijft de juiste toepassing van de Europese aanbestedingsrichtlijnen een belangrijk aandachtspunt. Landelijk blijkt dat circa 15% van de controleverklaringen 2018 (2017: 13%) ten aanzien van rechtmatigheid niet goedkeurend is als gevolg van onrechtmatige aanbestedingen. Er is dan ook in toenemende mate aandacht voor de borging van aanbestedingsrechtmatigheid bij gemeenten. Ook bij de gemeente Gouda hebben wij bij de jaarrekeningcontrole van 2018 onrechtmatige aanbestedingen geconstateerd en meegewogen in ons oordeel. Wij vragen dan ook extra aandacht voor aanbestedingsrechtmatigheid en onderstaande aandachtsgebieden en risico's in het bijzonder.

Risicogerichte inkoopanalyse t.b.v. de rechtmatigheidscontrole

Veelal blijkt dat het door de complexiteit van de aanbestedingswetgeving en de continue stroom aan jurisprudentie niet mogelijk is om de aanbestedingsrechtmatigheid te borgen in de reguliere administratieve organisatie en interne beheersing. In het kader van de jaarrekeningcontrole betekent dit dat er via controle achteraf vastgesteld dient te worden dat er geen onrechtmatige aanbestedingen hebben plaatsgevonden. Om gemeenten en accountants in de sector praktische handvaten te geven op het gebied van aanbestedingsrechtmatigheid heeft de NBA-Sectorcommissie Decentrale Overheden (SDO) de SDO-Notitie Uitvoering van de controle op aanbestedingsrechtmatigheid bij de jaarrekeningcontrole van decentrale overheden (Good practice, 17 januari 2019) uitgebracht. Naast een beschrijving van de uit te voeren werkzaamheden bij een risicogerichte inkoopanalyse, zijn in de notitie eveneens de volgende aandachtsgebieden benoemd:

- ▶ Subsidies versus overheidsopdrachten
- ▶ Publiek publieke samenwerking
- ▶ Raamovereenkomsten
- ▶ ICT-contracten
- ▶ Inhuur personeel
- ▶ Projectontwikkeling grondexploitatie en gebiedsontwikkeling
- ▶ Onderhandelingspositie zonder aankondiging
- ▶ Dynamisch aankoopstelsel
- ▶ Openhouse / bestuurlijke aanbestedingen

Wat kan er zoal mis gaan?

Uit onze rechtmatigheidscontroles blijken de volgende punten regelmatig mis te gaan, waardoor er onterecht niet Europees is aanbesteed:

- ▶ Het onterecht opknippen van opdrachten (verdelen over meerdere leveranciers / langere periode).
- ▶ Het ontbreken van een realistische raming (bijv. looptijd langer dan 4 jaar waarbij in de raming geen rekening is gehouden).
- ▶ Het onjuist aanbesteden van samengestelde / gemengde opdrachten (bv. een combinatie van investering en onderhoudscontracten).
- ▶ Een opdracht ten onrechte aanmerken als een quasi inbesteding.
- ▶ Een opdracht ten onrechte aanmerken als een sociale / specifieke dienst (Bijlage 14 bij richtlijn 2014/24).
- ▶ Een contract met een jaarlijks stilzwijgende verlengingsoptie niet aanmerken als een contract voor onbepaalde tijd.
- ▶ Het verlengen van een contract zonder verlengingsoptie.
- ▶ Het onjuist omgaan met significante wijzigingen van een contract gedurende de looptijd.

ACTIEPUNT: Wij verzoeken u, in aanvulling op onze eerdere bevindingen en aanbevelingen, deze Good practice van de SDO toe te passen bij de toetsing op de naleving van de EU Aanbestedingswet en de hiertoe door u aan te leveren spend-analyse.

3. Bevindingen significante processen

3.1 Onze controle nog transparanter

3.2 Effectiviteit processen

3.1 Onze controle nog transparanter (1/3)

Eisen aan accountants-
controle en onze
rapportages

Onderkende risico's:
► Management
override
► EU-aanbestedingen
► Waardering grex
► ICT

Wij beoordelen de
volgende processen

Inleiding

De afgelopen jaren is veel discussie (geweest) over de eisen die worden gesteld aan de accountantscontrole, wat direct en indirect ook gevolgen heeft voor de verwachtingen die wij als accountants hebben van onze klanten. 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 uw gemeente. Hierover hebben wij in onze managementletters van de afgelopen jaren uitgebreid gerapporteerd. Een goede interne beheersing, maakt immers ook dat de risico's voor de organisatie geringer zijn en de externe controle effectiever en efficiënter kan plaatsvinden. In deze management letter 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, belangrijkste processen, controleaanpak en afwegingen te beschrijven.

Onze inschatting van de risico's en belangrijkste processen

In het kader van de controle van de jaarrekening 2019 en onze aanpak hebben wij een zogenaamde initiële risico-inschatting gemaakt. Wij zien de volgende potentiële risico's in de controle van de jaarrekening van de gemeente Gouda:

- In onze controlestandaarden (NV COS) wordt expliciet het risico van management override (bewuste beïnvloeding door bestuur of management van de jaarcijfers) als belangrijk te onderkennen theoretisch risico benoemd. Als accountant moeten wij in onze werkzaamheden hier specifiek aandacht aan besteden. Wij zijn van mening dat binnen de gemeente de mogelijkheden, om buiten de getroffen interne beheersmaatregelen invloed uit te oefenen op de in de jaarrekening gepresenteerde uitkomsten, beperkt zijn. Om het resterende risico te beperken beoordelen wij schattingsprocessen en bijzondere journaalposten in detail.
- Het niet naleven van de Europese aanbestedingsregels.
- Onjuiste waardering bouwgronden in exploitatie (materiële post met verschillende schattingselementen).
- De gevolgen van ongeautoriseerde handelingen in de IT-systemen.

In onze aanpak is de insteek nog steeds, daar waar mogelijk te steunen op de interne beheersing in de significante processen van de gemeente. Daarbij maken wij, indien mogelijk, gebruik van uw eigen verbijzonderde interne controle (VIC).

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

- De interne Planning & Control-cyclus inclusief het proces van totstandkoming en boeken van memoriaalboekingen
- Het proces rondom totstandkoming van grondexploitatieberekeningen en realisatie van uitgaven en inkomsten grondexploitaties
- Het inkoopproces (incl. aanbestedingen)
- Het proces rondom factuurafhandeling en -betaling
- Het personeelsproces
- De processen rondom het sociaal domein (verdeeld in uitkeringen in geld, WMO uitkeringen en Jeugdverstrekkingen)
- Het subsidieproces
- Het parkeerproces
- Het heffen en innen van gemeentelijke belastingen en heffingen
- Het verhuur van vastgoed
- Het proces rondom verstrekken omgevingsvergunningen
- De beheersing van verbonden partijen

3.1 Onze controle nog transparanter (2/3)

Onderscheid systeem-
en gegevensgerichte
controleaanpak

Natuurlijk zijn er meerdere processen te onderkennen, ook met financiële gevolgen. Voorbeelden zijn het proces zoals het treasury-proces en diverse kleinere (schattings-)processen. Op basis van onze ervaring, de kwaliteit en omvang van deze processen en om efficiency redenen hebben wij deze echter niet procesmatig / systeemgericht getoetst, maar zullen wij (achteraf) gegevensgerichte werkzaamheden uitvoeren in de vorm van steekproeven / deelwaarnemingen, cijferanalyses, verbandscontroles, etc. Bij de voorbereiding van de jaarrekeningcontrole maken wij, evenals voorgaande jaren, afspraken over de resterende werkzaamheden, aanpak en de hiervoor benodigde informatie.

Onze aanpak afhankelijk van uw interne beheersing

Onze controle-aanpak bestaat uit systeemgerichte en/of gegevensgerichte werkzaamheden.

Een proces- of systeemgerichte aanpak is gericht op de interne beheersmaatregelen in de processen en daaraan gerelateerde IT-systemen. Deze aanpak stelt hoge eisen aan de interne controles in de processen, maar betekent ook dat de organisatie beter in control is en risico's eerder kan signaleren.

Een gegevensgerichte aanpak betekent dat wij de controle uitvoeren middels steekproeven, deelwaarnemingen etc. om vast te stellen of de posten in de jaarrekening getrouw en rechtmatig zijn. Met deze aanpak steunen wij niet op interne beheersingsmaatregelen in de organisatie en verrichten wij minimale werkzaamheden aan de interne beheersing.

De controle-aanpak die wij, al dan niet te onderscheiden per proces / post, hanteren, is afhankelijk van het niveau van uw interne beheersing. Om onze controle-aanpak te bepalen, toetsen wij de interne processen aan vier voorwaarden die wij hieronder uiteen hebben gezet. Vanzelfsprekend is ook een mix van deze aanpakken mogelijk, al dan niet te onderscheiden per proces / post.

Uitwerking controlestrategie per proces

Voor elk proces beoordelen wij de volgende onderdelen:

- ▶ **Controletechnische functiescheiding (CTFS):** Is er binnen de primaire processen sprake van voldoende functiescheiding?
- ▶ **AO/IB:** Is sprake van een actuele en toereikende procesbeschrijving met voldoende beheersmaatregelen?
- ▶ **IT-maatregelen:** Zijn in en rondom het systeem voldoende waarborgen getroffen t.a.v. de betrouwbaarheid van de gegevensverwerking?
- ▶ **VIC:** Heeft de VIC de interne beheersmaatregelen getoetst en kunnen wij daar gebruik van maken?

Indien al deze vragen positief kunnen worden beantwoord, is de organisatie optimaal in control en kunnen ook wij gebruik maken van uw eigen interne beheersing. De vaak tijdrovende en gedetailleerde gegevensgerichte werkzaamheden (die ook nog eens achteraf plaatsvinden), kunnen dan beperkt blijven tot een minimum.

Criteria:

- Voldoende functiescheiding
- Voldoende beheersmaatregelen
- IT-beheersing op orde
- Toetsing door verbijzonderde interne controle

3.1 Onze controle nog transparanter (2/2)

De beheersorganisatie
is in opzet voldoende
tot goed

Samenvatting effectiviteit van de processen

In het overzicht op de volgende pagina geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook hoofdstuk 4 t.a.v. IT-omgeving) en welke detailbevindingen wij per proces hebben geconstateerd. Voor een uiteenzetting van onze detailbevindingen verwijzen wij naar de tabel in **hoofdstuk 3.3 Bevindingen per proces**.

Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat de beheersorganisatie van de gemeente (voor zover relevant voor de controle van de jaarrekening) per proces een wisselend beeld laat zien, rekening houdend met de uitkomsten van de werkzaamheden van de VIC. Sommige processen verdienen nog veel aandacht, andere processen zijn (nagenoeg) gereed om systeemgericht te kunnen controleren. Met soms enkele kleinere aanpassingen in de AO/IB (met name gericht op uiteenzetten van de IB-maatregel) kan het proces al verbeterd worden. Uit onze gesprekken die wij per proces hebben gevoerd met de medewerkers van uw organisatie blijkt dat er diverse interne beheersingsmaatregelen in de processen aanwezig zijn, maar dat deze niet verankerd zijn in de AO/IB beschrijvingen en/of niet goed vastgelegd worden.

Omdat de AO/IB en IT General Controls niet altijd goed zijn opgezet of goed werken, kunnen wij voor wat betreft de insteek van onze controle nog niet altijd op de processen steunen en zullen wij voor de controle 2019 voornamelijk gegevensgerichte controles gaan uitvoeren, waarbij wij gebruik zullen maken van de uitvoering van de verbijzonderde interne controle.

De gemeente Gouda onderkent ook zelf het belang van een goede AO/IB-beschrijving en onderkent ook het belang van een goede procesopzet, met name voor de invoering van de rechtmatigheidsverklaring voor het college vanaf 2021. Aan de hand van het 'Three Lines of Defense-model' (3LoD) zal de gemeente op korte termijn de IC en VIC nader gaan optimaliseren, waarbij ook beoordeeld zal worden of en hoe gebruik kan worden gemaakt van de 1^e lijn (opzet AO/IB en toetsing van de werking van de AO/IB). Vanuit onze natuurlijke adviesfunctie zijn wij altijd bereid om met uw organisatie mee te denken dit proces tot een succes te maken.

3.2 Effectiviteit processen (1/2)

PROCES	CTFS	AO/IB	ITGC'S	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Planning & Controle (begroting en - wijzigingen)					Totstandkoming van begroting en begrotingswijzigingen is niet formeel vastgelegd in een AO/IB. IB maatregelen worden niet vastgelegd. Wel voldoende betrokkenheid. Gemeente voert budgetgesprekken die van meerwaarde kunnen zijn indien deze goed vastgelegd worden in een verslag met actiepunten. VIC kan een rol krijgen bij beoordeling budgetgesprekken (follow up) en toetsing van juiste raadsstukken
Memoriaalboekingen					Er is onvoldoende controletechnische functiescheiding aanwezig (geen 4-ogenprincipe). Procedure is niet beschreven en IB-maatregelen zijn niet onderkend. Er vindt geen VIC plaats op de memoriaalboekingen.
Grondexploitatie					Proces is te splitsen in Grex Westergouwe en overige grex-en. In opzet zijn beide van voldoende niveau. Formeel liggen deze niet vast in AO/IB maatregelen. Wel vindt voldoende controle in de lijn plaats. VIC-controle dient nog nader opgezet, uitgewerkt en uitgevoerd te worden.
Inkopen & Aanbestedingen					Vanaf 1 november 2019 is dit proces gewijzigd. Proces is in opzet nader uitgewerkt en verbeteringen worden doorgevoerd zoals een beter beheer op (juistheid en volledigheid) van het contractenregister. In het zaakstelsel is een betere koppeling gelegd tussen de verplichtingenadministratie en het resultaat van het inkooptraject.
Factuurafhandeling en betaling					Onvoldoende functiescheiding aanwezig inzake bestellen/inkopen en goedkeuren facturen voor prestatielevering. Hierdoor verhoogde kans op een frauderisico. Gemeente voert wel een VIC uit maar de aantallen die hiervoor gehanteerd worden zijn te weinig om een goed oordeel te kunnen geven over dit proces.
Personeel					Er is voldoende functiescheiding in het proces aanwezig. Ook zijn er in het proces voldoende interne beheersingsmaatregelen gedefinieerd en worden achteraf nog interne controlewerkzaamheden uitgevoerd. Dit proces dient alleen nog zichtbaar vastgelegd te worden.
Sociaal Domein - uitkeringen					Binnen dit proces zijn voldoende interne beheersingsmaatregelen en (verbijzonderde) interne controlemomenten aanwezig. Instructies zijn aanwezig. De AO/IB beschrijving kan nog iets verbeterd worden (onderkennen risico's en vastleggen van IB-maatregelen).
Sociaal Domein -WMO					Binnen dit proces zijn voldoende interne beheersingsmaatregelen en (verbijzonderde) interne controlemomenten aanwezig. Instructies zijn aanwezig. De AO/IB beschrijving kan nog iets verbeterd worden (onderkennen risico's en vastleggen van IB-maatregelen).
Sociaal Domein - Jeugd					Binnen dit proces zijn voldoende interne beheersingsmaatregelen en (verbijzonderde) interne controlemomenten aanwezig. Instructies zijn aanwezig. De AO/IB beschrijving kan nog iets verbeterd worden (onderkennen risico's en vastleggen van IB-maatregelen).
Subsidieverstrekingen					Voldoende controletechnische functiescheiding in het proces aanwezig. Aandacht verdient de beschrijving van de AO/IB, de rol van de subsidiecoördinator en de sociale hygiëne van het proces (zoals langdurige betrokkenheid van medewerkers bij subsidierelaties).

■ 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.

3.2 Effectiviteit processen (2/2)

PROCES	CTFS	AO/IB	ITGC'S	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Parkeren					Dient nog nader afgestemd te worden met uw gemeente. Er is geen AO/IB, ook de VIC speelt (nog) geen rol in dit proces. Dient op korte termijn nader vormgegeven te worden om volledigheid te kunnen waarborgen voor de jaarrekeningcontrole.
Belastingen & heffingen					Het opleggen, innen en afdragen van gemeentelijke belastingen is uitbesteed aan BSGR. Gemeente doet alleen de afstemming met de BSGR n.a.v. ontvangen (bestuurlijke) rapportages. Aandachtspunt voor onze controle is de precariobelasting (op ondergrondse leidingen).
Verhuur van vastgoed					Opzet van de AO -procedures is aanwezig (inclusief instructies). Deze zijn nog niet van voldoende omvang dat ook interne beheersingsmaatregelen zijn opgenomen (inclusief onderkende risico's). VIC heeft nog niet plaatsgevonden en moet nog worden uitgezet en uitgevoerd.
Omgevingsvergunningen					Proces is voor een groot gedeelte uitbesteed aan ODMH, echter een gedeelte van dit proces vindt nog plaats bij de gemeente Gouda. Er is geen OA/IB beschrijving, gemeente doet geen VIC op de juistheid en volledigheid.
Verbonden partijen					Er is geen procesbeschrijving inclusief IB-maatregelen aanwezig bij de gemeente. Geen vastleggingen voor beoordeling van inhoudelijke en financiële informatie van deze verbonden partijen. VIC vindt wel plaats maar moet nader worden uitgewerkt en aangevuld.



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.

3.3 Bevindingen per proces

Proces	Bevinding	Impact op controle	Advies	Follow-up 2018
Planning en Control (totstandkoming begroting en begrotingswijzigingen)	Gemeente Gouda heeft aan de hand van een gesprek duidelijk uiteengezet welke werkzaamheden en acties worden verricht om tot een goede begroting en juiste begrotingswijzigingen te komen. Er is sprake van voldoende functiescheiding en controlemomenten (collegiale toetsing) alleen worden deze momenten in het proces niet formeel vastgelegd. Wel bestaat de zogenaamde 'lijst der lijsten', waarmee de organisatie inzichtelijk heeft welke acties en begrotingswijzigingen er nog doorgevoerd dienen te worden. Het betreft veelal 'handmatige' acties en controles (zoals vullen van de lijst der lijsten) die een foutgevoeligheid hebben. Naast totstandkoming van de begroting hebben wij tevens vastgesteld dat er maandelijks budgetgesprekken plaatsvinden tussen de financieel consultant en de budgethouders. De financieel consultant lijkt in deze een grote faciliterende rol te hebben in uitzoeken, voorbereiden en verklaren van afwijkingen. Er wordt geen verslag en actiepuntenlijst gemaakt van deze gesprekken.	Weinig impact op onze controle. Interne beheersingsmaatregelen zijn niet vastgelegd in dit proces. Budgetgesprekken vinden plaats maar zijn inzake de follow up niet door ons te controleren. Dit betekent dat wij de begroting niet als leidraad kunnen gebruiken voor eventuele cijferanalyses (uitgaven t.o.v. de begroting en afwijkingen beoordelen). Dit kan niet omdat wij de betrouwbare totstandkoming van de begroting niet hebben kunnen vaststellen. Wij zullen derhalve gegevensgericht meer werkzaamheden uitvoeren (conform voorgaande jaren).	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB maatregelen beschreven worden (wie controleert wat etc.); • Budgetgesprekken als IB-maatregel gedefinieerd worden en worden vastgelegd waarbij follow up te volgen is; • De huidige rol van de financieel consultant nader uiteengezet wordt (adviserende/ controlerende rol i.p.v. faciliterende rol).	Nieuw punt ML 2019.
Memoriaalboekingen	Memoriaalboekingen worden door één functionaris in de organisatie geboekt. Ook controle op juistheid en volledigheid van de aangeleverde memoriaalboeking wordt door deze functionaris uitgevoerd. Er vindt geen controle plaats op de werkzaamheden van deze functionaris. Daarnaast is dit proces niet beschreven in een formele AO/IB beschrijving, waarbij uiteengezet is welke controles dienen uitgevoerd te worden door wie, op welke wijze, wanneer en hoe deze vastgelegd moeten worden. Ook een verbijzonderde interne controle op de doorgevoerde memoriaalboekingen vindt niet plaats.	Het ontbreken van een goede functiescheiding in het proces, het ontbreken van goede beschreven en geïmplementeerde IB-maatregelen en het feit dat er geen verbijzonderde interne controle plaatsvindt op de memoriaalboekingen betekent dat wij dit proces als niet effectief beschouwen. Vanuit onze rol als accountant is vanuit dit proces al een significant risico onderkend op een zogenaamd risico voor managementoverride. Dit risico wordt niet verlaagd door interne beheersingsmaatregelen die uw organisatie heeft ingesteld om dit risico te mitigeren.	Wij adviseren op korte termijn de AO/IB voor dit proces op te zetten en minimale functiescheiding in het proces aan te brengen (muteren en controleren). Tevens adviseren wij u voor de memoriaalboekingen, die reeds allemaal zijn verwerkt in 2019, een VIC te doen uitvoeren waarbij per memoriaalboeking vastgesteld dient te worden dat deze boeking juist is (op basis van aanwezige documenten).	Nieuw punt ML 2019.
Grondexploitaties	De grondexploitaties zijn te verdelen in grex Westergouwe en de overige grex-en. Beide zijn door ons met de verantwoordelijke projectleiders en besproken. Voldoende functiescheiding aanwezig. Beheersing van alle grondexploitaties is aanwezig maar wordt niet formeel vastgelegd waardoor wij gebruik kunnen maken van de interne beheersingsmaatregelen. Tevens vindt er (nog) geen verbijzonderde interne controle plaats op dit proces. Wij vragen aandacht voor minimale uitvoering van VIC-werkzaamheden op de mutaties in de grex-en. Tevens vragen wij aandacht voor een tijdige taxatie van de oud NIEGG's (moet dit jaar conform BBV uitgevoerd zijn).	Weinig tot geen impact. Dit proces wordt door ons al als een significant proces beschouwd met significante risico's voor de waardering. De gemeente heeft aangegeven second opinions aan te vragen ter onderbouwing van de waardering. Wij vragen aandacht voor een voldoende uitvoering van de VIC op mutaties in deze grondexploitaties.	Vastleggen van de huidige procedure in AO/IB beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • voortgangsgesprekken als IB-maatregel gedefinieerd worden en worden vastgelegd waarbij follow up te volgen is. • Uitvoeren van second opinion en vastlegging van de beoordeling van deze door de gemeente.	Geen wijzigingen t.o.v. 2018.

3.3 Bevindingen per proces

Proces	Bevinding	Impact op controle	Advies	Follow-up 2018
Inkopen goederen en diensten	Dit proces is in 2019 aangepast, waardoor deze uitgaven beter door de gemeente beheerst kunnen worden en de rechtmatigheid van de aanbestedingen gewaarborgd kunnen worden. Belangrijke ontwikkelingen hierbij zijn: • Verplichting tot aanmaken van een verplichtingnummer (zonder nummer geen betaling van factuur) • Afdwingen van betrokkenheid van inkoopadviseurs bij afwijkingen van de inkoopprocedures. Een formele AO/IB-beschrijving (voorzien van risicoanalyse) is nog niet aanwezig. Gemeente beschikt over een contractenregister in Verseon met als voornaamste doel grip op de contracten: 1) Signalering bij aflopen van het contract zodat een eventuele aanbesteding tijdig zou kunnen worden opgestart 2) Vindbaarheid van contracten op een centrale plaats voor iedereen raadpleegbaar. Contracten van POR, huurcontracten en personeel blijven buiten de contractenbank.	De nieuwe procesopzet heeft nog geen invloed op onze controle van de jaarrekening 2019. Deze zal pas zijn beslag krijgen op de controle van 2020. Voor 2019 zal met name gegevensgericht gecontroleerd worden, waarbij het opstellen van een spendanalyse op de uitgaven per crediteur zal moeten worden uitgevoerd waarbij de uitgaven per leverancier over de afgelopen vier jaar in kaart worden gebracht. Alle uitgaven per crediteur groter dan € 200.000 moeten worden geanalyseerd of contract is aanbesteed of aanbesteed had moeten worden. Tevens zal er een steekproef uitgevoerd moeten worden op de facturen die behoren tot de crediteuren < € 200.000, waarbij vastgesteld dient te worden of deze kosten terecht niet Europees aanbesteed zijn. Wij zullen het (aangepaste) werkprogramma voor het uitvoeren van de spendanalyse binnenkort met de medewerkers van uw organisatie bespreken.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Integratie van de verplichtingenadministratie. Naast de reguliere AO/IB-beschrijving vragen wij aandacht voor de totstandkoming van een volledig contractenregister waarbij gewaarborgd dient te worden dat: • deze volledig is (vanuit de huidige organisatie) • Volledig blijft (procedures opstellen).	Proces-aanpassingen zijn gemaakt. Voor 2019 zullen wij hiervan nog geen gebruik kunnen maken.
Factuurafwikkeling en -betaling	De huidige grootboekadministratie in Decade laat niet toe dat binnen de workflow er voldoende functiescheiding aanwezig is tussen inkopen/bestellen, goedkeuring factuur voor prestatielevering (aantallen en prijs) en goedkeuring factuur voor juiste uitnutting van budget. Het is goed mogelijk dat alle handelingen in één hand aanwezig zijn, waardoor de gemeente een verhoogd risico loopt op fraude (bestelling en accordering van goederen t.l.v. de rekening van de gemeente zonder dat deze goederen bestemd zijn voor de gemeente). Ten aanzien van het betaalproces hebben wij geen bevindingen. Wijzigingen in crediteurenstamgegevens worden niet gecontroleerd bij mutaties maar worden integraal gecontroleerd a.d.h.v. het betaalvoorstel, waarbij alle betalingen gecontroleerd worden met de gegevens op de factuur.	De medewerkers van uw gemeente hebben aangegeven de bevinding te herkennen maar vanwege het feit dat de gemeente zich oriënteert op een nieuw boekhoudpakket dit nu niet meer te gaan aanpassen. Wij kunnen ons vinden in deze besluitvorming. De verbijzonderde interne controle voert wel steekproeven uit om vast te stellen dat de prestatielevering heeft plaatsgevonden. De aantallen die de gemeente uitvoert zijn echter te weinig, waardoor wij geen gedegen controle kunnen uitvoeren ten aanzien van dit proces en er aanvullende steekproeven uitgevoerd moeten worden. Naast de controle van de prestatielevering dient tevens door de uitvoering van de verbijzonderde interne controle vastgesteld te worden dat de factuur ten laste van het juiste budget is geboekt en dat de betaling juist heeft plaatsgevonden.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Ieder deelproces binnen dit proces op een andere wijze gecontroleerd kan worden. Door aanpassing van de AO/IB is het wellicht mogelijk om de betalingen van de facturen, de accordering voor het budget en de controle door de financieel medewerker van de factuur als interne beheersingsmaatregel (werking) te betrekken in de uitvoering van de VIC.	Geen wijzigingen t.o.v. 2018.

3.3 Bevindingen per proces

Proces	Bevinding	Impact op controle	Advies	Follow-up 2018
Personeel	Binnen het proces van personeel is voldoende controletechnische functiescheiding aanwezig. Mutaties t.a.v. van de salarisadministratie dienen altijd door twee functionarissen in functiescheiding opgesteld en goedgekeurd te worden. Tevens is het afdelingshoofd verantwoordelijk voor de definitieve goedkeuring van de mutatie. Naast de hierboven beschreven controles in het proces vindt er achteraf ook interne controle plaats t.a.v. een aantal mutaties. Bovengenoemde interne beheersingsmaatregelen liggen niet vast (a.d.h.v. de zogenaamde wie, doet wat, waarmee, wanneer en hoe wordt dit vastgelegd vragen).	Door het ontbreken van een goede AO/IB-beschrijving kunnen wij (nog) geen gebruik maken van de IB-maatregelen en moeten wij dit proces gegevensgericht controleren. De interne controle voert zelfstandig diverse controles uit maar deze (V)IC werkzaamheden zijn niet met ons afgestemd.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Interne controle wordt betrokken. • VIC op IB maatregelen mogelijk is. De interne controle voert diverse bruto/netto berekeningen uit. Wij adviseren deze te beperken tot een tweetal momenten in het jaar (wanneer de premiepercentages wijzigen) en hiervan dan vast te stellen dat mutaties juist en volledig zijn doorgevoerd in de applicatie (en vaststelling hiervan a.d.h.v. één bruto-netto berekening per mutatiemoment). Op korte termijn in onderling overleg treden over de aanpak van de interne controle, waarbij risicogericht gecontroleerd kan worden op mutaties.	Nieuw punt ML 2019.
Sociaal domein - Uitkeringen - WMO - Jeugd	Binnen deze processen vinden diverse controles plaats, zowel in de lijn als achteraf. Enkele voorbeelden zijn 100% collegiale toetsing bij afgifte beschikking, interne controle door kwaliteitsmedewerker op geselecteerde werkprocessen als verbijzonderde interne controle door een VIC-medewerker achteraf. De AO/IB is voor een groot gedeelte beschreven. Wij zijn van mening dat uw gemeente dit proces door de diverse controlemomenten in control heeft. Wel vragen wij aandacht voor de vastlegging van de foutevaluatie wanneer mogelijk fouten worden aangetroffen in de interne controle of verbijzonderde interne controle vertaald naar de massa.	Wij zijn van mening dat door een snelle aanpassing van de AO/IB (en dan met name uiteenzetten van IB-maatregelen en VIC-maatregelen in de AO) wij gebruik kunnen maken van deze interne beheersingsmaatregelen zoals uitgevoerd door uw gemeente. Dit betekent dat wij de werking gaan vaststellen van de maatregelen, waarbij als vaststaat dat deze werken, wij gegevensgericht minder werkzaamheden zullen uitvoeren. Wij zullen op korte termijn met uw medewerkers een afspraak plannen om dit proces onderling af te stemmen. Hierbij kan ook gedacht worden aan een andere rol voor de VIC, waarbij de VIC vaststelt dat interne beheersingsmaatregelen in deze processen werken.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Interne controle wordt betrokken. • VIC op IB maatregelen mogelijk is. Tevens vragen wij aandacht voor de vastlegging van de foutevaluatie wanneer mogelijk fouten worden aangetroffen in de interne controle of verbijzonderde interne controle vertaald naar de massa (wanneer worden welke acties ondernomen door de gemeente en hoe wordt een tekortkoming gewogen).	Nieuw punt ML 2019.

3.3 Bevindingen per proces

Proces	Bevinding	Impact op controle	Advies	Follow-up 2018
Subsidie-verstrekkings	De gemeente heeft aanpassingen gemaakt in het proces, zodat sprake is van een controle-technische functiescheiding (4-ogenprincipe). Gemeente hanteert hiervoor zogenaamde 'op de minuut' als geleideformulier. Deze functiescheiding kan tevens als IB-maatregel gelden als de gemeente dit verankert in haar AO/IB beschrijving. Er vindt voldoende gegevensgerichte controle plaats op de subsidies door uw VIC-medewerker. Aantallen worden met BDO afgestemd. Uitwerking is voornamelijk gegevensgericht. De subsidiecoördinator vervult een belangrijke rol in het gehele subsidieproces (eerste beoordeling binnengekomen stukken, doorzetten van stukken naar beleidsmedewerkers, managen van het gehele proces dat alles op tijd verstuurd en ontvangen wordt etc.). Voor zover wij vernomen hebben is minimale vervanging aanwezig.	Op dit moment zal de controle nog volledig gegevensgericht plaatsvinden, waarbij er diverse subsidieverleningen en -vaststellingen worden gecontroleerd. Uw gemeente kan het met enkele wijzigingen mogelijk maken dat de werking van uw proces getoetst kan worden, waarbij vastgesteld zou kunnen/moeten worden dat er gegevensgericht (veel) minder werkzaamheden nodig zijn.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Interne controle wordt betrokken. • VIC op IB maatregelen mogelijk is. Tevens vragen wij aandacht voor: • Mogelijkheid van langdurige betrokkenheid van medewerkers bij subsidierelaties (geen beleid aanwezig) • Nevenfuncties niet bekend (geen beleid van ingezien) • Afhankelijkheid van subsidiecoördinator (veel in handen van deze functionaris, afhankelijkheid is groot).	Collegiale toetsing wordt zichtbaar vastgelegd op de zogenaamde geleide-formulier 'op de minuut'.
Parkeren	Er is geen enkele procesbeschrijving voor parkeren aanwezig. Op basis van een gesprek dat wij met uw medewerkers hebben gevoerd blijkt dat: • veel taken van de gemeenten zijn uitbesteed bij derden, waarvoor met deze derden afspraken zijn gemaakt ter waarborging van volledigheid, juistheid en rechtmatigheid • Ten aanzien van processen waarbij de gemeente wel betrokken is, zoals verstrekken van uitrijkaarten en versturen van data van opgelegde naheffingsaanslagen, er geen inzicht is in hoeverre de gemeente hierbij een verhoogd (fraude)risico loopt • Er geen controle plaatsvindt op volledige opbrengstverantwoording van alle betaalpalen straatparkeren (genereren alle palen opbrengsten) • Verbijzonderde interne controle geen rol heeft in dit proces.	Op basis van het gesprek dat wij hebben gevoerd, moeten wij concluderen dat veel taken van de gemeente zijn uitbesteed bij derden (zoals beheer van straatparkeren, betaalmogelijkheden garage, mobiel betalen etc.). Op basis van de interim controle moeten wij vaststellen dat wij nog geen basis zien om de volledigheid van de opbrengsten te kunnen vaststellen op dit moment. De gemeente zal op korte termijn actie moeten ondernemen om dit proces vast te leggen en risico's te benoemen en deze te mitigeren. Ook de VIC zal voor de jaarrekeningcontrole een controle dienen uit te voeren op het boekjaar 2019.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Verbijzonderde interne controle wordt betrokken. Uitvoeren van verbijzonderde interne controle voor aanvang van de jaarrekeningcontrole waarbij: • Juistheid van de tarieven vastgesteld wordt • Volledigheid van betaalpalen op straat (genereren van opbrengsten) • Beoordelen van gegevens ontvangen van derden (is dit voldoende om te waarborgen dat opbrengsten volledig zijn) • Beoordelen van mogelijke (fraude)risico's en het vaststellen dat zich deze niet hebben voorgedaan.	De gemeente vraagt per eindejaar een controle-verklaring op bij de samenwerkende organisaties.

3.3 Bevindingen per proces

Proces	Bevinding	Impact op controle	Advies	Follow-up 2018
Gemeentelijke belastingen en heffingen	Het heffen, innen en afdragen van gemeentelijke belastingen is uitbesteed aan BSGR (in mandaat). De gemeente blijft zelf wel verantwoordelijk voor de juistheid en volledigheid van de opbrengsten. Gemeente ontvangt jaarlijks een IASE 3402 type 2 verklaring van BSGR. Daarnaast wordt de BSGR als verbonden partij ook door de gemeente betrokken in het proces van beheersing van verbonden partijen. Dit proces is nog niet vastgelegd (zie verbonden partijen). Punt van aandacht is verwerking van de precario-belasting (op ondergrondse leidingen). Ten tijde van de controle hebben wij nog geen inzicht gekregen in het heffen, innen en ontvangen van deze middelen. BSGR legt de aanslag op en int deze ook. Vóór het opleggen van de aanslagen wordt de betreffende grondslag opgevraagd bij de belastingplichtigen (Tennet, Oasen en Stedin). Gemeente bepaald derhalve of deze juist is.	De gemeente ontvangt van BSGR een IASE type 2 verklaring, waarvan wij gebruik hopen te maken (hangt van de mogelijke bevindingen af). Voorgaande jaren bleken geen bevindingen, waardoor wij ervan uitgaan dat dit jaar ook geen bevindingen bekend zullen worden. Ten aanzien van de controle van de precariobelasting dienen nog aanvullende afspraken met uw gemeente gemaakt te worden aan de hand van de opzet van het proces en de mogelijke rol die uw VIC daarin zal gaan vervullen.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Verbijzonderde Interne controle wordt betrokken. Tevens op korte termijn uiteenzetten van proces van precariobelasting (met name voor ondergrondse leidingen). Naast de reguliere belastingen adviseren wij periodiek (eens per 3 jaar) ook niet significante heffingen onderdeel van de VIC te laten zijn zoals marktgelden en havengelden.	Nieuw punt ML 2019.
Verhuur van vastgoed	De gemeente beschikt over AO-beschrijvingen voor aanmaken huurovereenkomst, mutaties in Planon (vastgoedmodule), factureren van verhuur-opbrengsten etc. Deze AO-beschrijvingen missen echter nog de risico's en de onderkende interne beheersingsmaatregelen die dit risico mitigeren, waardoor de twee belangrijkste risico's: juistheid van vastgestelde verhuurtarief en volledigheid van de verhuur-opbrengsten niet afgedekt lijkt. Er vinden diverse controles plaats, maar het is thans onduidelijk of deze op basis van de huidige situatie ook de risico's afdekken: - onjuiste/ onrechtmatige verhuurprijs - Panden wel verhuurd, maar niet in rekening gebracht.	Vooralsnog zal de controle volledig gegevensgericht plaatsvinden net als voorgaande jaren, waarbij nog veel input nodig is van de afdeling en er een goede VIC uitgevoerd zal moeten worden waarbij een x aantal keer vastgesteld moet worden dat het verhuurtarief juist en rechtmatig tot stand is gekomen en is gefactureerd. Tevens zal er op basis van het activabezit, planon en de belastingaanslagen/ BAG registratie vastgesteld moeten worden dat al het vastgoed bezit van de gemeente Gouda bekend is en welk vastgoed voor verhuur in aanmerking komt en tot verhuuropbrengsten heeft geleid. Voor de panden die niet hebben geleid tot verhuuropbrengsten moet vastgesteld worden dat dit terecht is.	Vastleggen van de huidige procedure in AO/IB beschrijving waarbij: • IB maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Verbijzonderde interne controle wordt betrokken. Wij adviseren op korte termijn een VIC uit te voeren waarbij: • Juistheid en rechtmatigheid van gehanteerde tarieven • Vaststellen van volledigheid van de opbrengstverantwoording	De organisatie stelt 2x per jaar aansluiting verhuurregistratie met activabezit op en sluit vastgoedregistratie aan met belastingaanslagen. Het proces van vastgoedverhuur zal in 2020 nader beschreven worden en voorzien worden van een risico-inventarisatie en een testsheet, op basis waarvan een interne controle en een verbijzonderde interne controle kan worden uitgevoerd.

3.3 Bevindingen per proces

Proces	Bevinding	Impact op controle	Advies	Follow-up 2018
Omgevings-vergunningen	Dit proces is voor een groot gedeelte uitbesteed aan ODMH. ODMH bepaalt de leges (op basis van de door de gemeenteraad vastgestelde legestabel). De gemeente blijft verantwoordelijk voor de juistheid en rechtmatigheid van het tarief en het feit dat alle leges ook daadwerkelijk opgelegd worden en op een juiste wijze in de jaarrekening van de gemeente opgenomen is. Gemeente Gouda ontvangt maandelijks een excel-bestand met verstrekte vergunningen per e-mail van ODMH. BSGR factureert de verstrekte vergunning. Gegevens worden per e-mail ontvangen en zijn dus bewerkelijk alvorens deze tot opbrengsten leiden. Het is van belang dat de gemeente Gouda de opgelegde leges aansluit met de primaire registratie (Squit) in beheer van ODMH.	Er is geen vastgestelde AO/IB-beschrijving en ook de vastlegging van de aansluiting tussen de (beperkt) toegankelijke subadministratie van ODMH en de grootboekadministratie van de gemeente Gouda is niet beschreven. Dit dient op korte termijn opgepakt te worden (wat is wel en niet mogelijk). Tevens dient er een controle plaats te vinden op de juistheid van de opgelegde (bouw)leges en de wijze waarop deze vastgesteld kan worden. Van ODMH wordt namelijk geen controleverklaring of ISAE3402-verklaring ontvangen. Er zal voor de start van de jaarrekeningcontrole nog een uitvoerige verbijzonderde interne controle dienen plaats te vinden voor dit proces.	Vastleggen van de huidige procedure in AO/IB beschrijving waarbij: • IB maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Uitvoering van de verbijzonderde interne controle. Naast de reguliere AO/IB beschrijving vragen wij aandacht voor de uitvoering van de VIC voor 2019: • Vaststellen van hantering juiste tarief en • Vaststellen van de volledigheid van de opbrengstverantwoording. • Controle op aansluitingen tussen subadministraties (gemeente en ODMH).	Nieuw punt ML 2019.
Verbonden partijen	Er is geen procesbeschrijving voor verbonden partijen. Interne beheersingsmaatregelen zijn niet bekend en/of beschreven. Er zijn geen standaard formats voor beoordeling van (tussentijdse) informatie. Hoe vastgesteld wordt dat beleidsdoelstellingen worden behaald is thans onbekend. De medewerker concernstafstelt een overzicht vast van alle verbonden partijen t.b.v. de jaarrekening.	Ontbreken van deze AO/IB levert op dat wij meer gegevensgerichte werkzaamheden moeten uitvoeren voor zowel de balanscontrole (klopt de nog te betalen of te ontvangen post) als de controle van de staat van baten en lasten (zijn alle bijdragen juiste en volledig verwerkt). De verbijzonderde interne controle zal ter voorbereiding van de jaarrekeningcontrole deze informatie moeten verzamelen en vaststellen dat deze juist is verwerkt.	Vastleggen van de huidige procedure in AO/IB-beschrijving waarbij: • IB-maatregelen beschreven worden (wie controleert wat etc.); • risico's worden gedefinieerd. • Uitvoering van de verbijzonderde interne controle. Verbijzonderde interne controle moet vaststellen dat: • Alle verbonden partijen juist en volledig zijn verwerkt in de jaarrekening • Er geen transacties met verbonden partijen hebben plaatsgevonden die niet behoren tot de dagelijkse uitvoering en het beleid van de gemeente.	Nieuw punt ML 2019.

4. IT-beheersing

- 4.1 IT-beheersing en onze controlerende rol
- 4.2 Bevindingen IT-beheersing | Overall beeld per applicatie
- 4.3 Actuele IT ontwikkelingen vanuit onze natuurlijke adviesrol

4.1 IT-beheersing



Wij beoordelen de betrouwbaarheid en continuïteit IT voor zover relevant voor de controle van de jaarrekening

Beoordeelde systemen:

- Decade
- Verseon
- Suite4SociaalDomein

Detailbevindingen
IT weergegeven in
Bijlage B

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 ICT-systemen en applicaties en het gebruik daarvan 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 en het optreden van verstoringen met impact op de gegevensverwerking.

De bevindingen zoals gerapporteerd in deze management letter zijn gericht geweest op het beoordelen van de opzet en het vaststellen van het bestaan van algemene IT-beheersmaatregelen. Wij hebben in samenwerking met onze IT-auditors een aantal van deze maatregelen beoordeeld voor Decade Financials (hierna: Decade), Verseon en Suite4SociaalDomein. Dit om de impact van de risico's van ongeautoriseerde wijzigingen, ongeautoriseerde handelingen en verstoringen te kunnen vaststellen voor die systemen die gekoppeld zijn aan de voor ons relevante processen en posten (zie hoofdstuk 3).

In dit hoofdstuk geven wij allereerst een samenvatting van onze bevindingen voor de genoemde applicaties. De detailbevindingen rondom deze systemen zijn opgenomen in **Bijlage B**.

Daarna gaan wij, vanuit onze natuurlijke adviesfunctie, in op een aantal actuele ontwikkelingen ten aanzien van de Baseline Informatievoorziening Overheden (BIO), het project GGI- veilig en data-analyse.

4.2 Bevindingen IT-beheersing | Decade

Logische toegangs-beveiliging (criteria 1) nog deels ontoereikend (criteria 2-5) toereikend.

Change management (criteria 6) toereikend.

Continuïteit (criteria 7) toereikend.

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

PROCES	2019	2018
1. <u>Procedure autorisatiebeheer</u>		
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	

onvoldoende

verbeterpunten

voldoende

KORTE OMSCHRIJVING RESULTATEN	
1	Voor de applicaties in scope is nog geen formele normpositie opgesteld, waarin de rollen per functionaris worden weergegeven.
2	Er wordt een review uitgevoerd op de juistheid van rollen en actualiteit van gebruikers door het afdelingshoofd.
3	Akkoord, generieke accounts zijn verklaarbaar vanuit gebruikersdoeleinden.
4	Akkoord. De wachtwoordeisen in Decade voldoen aan de minimale te stellen eisen (2-factor authenticatie).
5	Akkoord. Alleen medewerkers uit de IT beheer-organisatie beschikken over superuserrechten, waardoor functiescheiding niet doorbroken is.
6	Akkoord. Testwerkzaamheden en een akkoord zijn aantoonbaar vastgelegd.
7	Akkoord. Er zijn maatregelen getroffen ten aanzien van continuïteit.

*₁ = Hoewel dit punt toereikend is, zijn in bijlage B zijn aanbevelingen opgenomen.

4.2 Bevindingen IT-beheersing | Verseon

Logische toegangs-beveiliging (criteria 1) nog deels ontoereikend (criteria 2-5) toereikend.

Change management (criteria 6) deels ontoereikend.

Continuïteit (criteria 8) toereikend.

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

PROCES	2019	2018
1. <u>Procedure autorisatiebeheer</u>		
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)	*1	
7. Continuïteit (fysieke toegang, back-up, monitoring en restoretest).	*2	

Legend: onvoldoende verbeterpunten voldoende

KORTE OMSCHRIJVING RESULTATEN	
1	Voor de applicaties in scope is nog geen formele normpositie opgesteld waarin de rollen per functionaris worden weergegeven.
2	Er worden ad-hoc reviews uitgevoerd op de juistheid van autorisaties en actualiteit van gebruikers voor de applicaties in scope.
3	Akkoord, generieke accounts zijn verklaarbaar vanuit gebruikersdoeleinden.
4	Akkoord. De wachtwoordeisen in Decade voldoen aan de minimale te stellen eisen (2-factor authenticatie).
5	Akkoord. Alleen medewerkers uit de IT beheer-organisatie beschikken over superuserrechten, waardoor functiescheiding niet doorbroken is.
6	Er bestaat geen gescheiden test- en productie omgeving. <i>Zie opmerking.</i>
7	Akkoord. Er zijn maatregelen getroffen ten aanzien van continuïteit.

*1 = Dit punt heeft nuancering gezien het bestaan niet beoordeeld kon worden, omdat er gedurende het boekjaar geen wijzigingen zijn doorgevoerd in de productie-omgeving van Verseon.
*2 = Hoewel dit punt toereikend is, zijn in bijlage B zijn aanbevelingen opgenomen.

4.2 Bevindingen IT-beheersing | Suite4SociaalDomein

Logische toegangs-beveiliging (criteria 1,4) nog deels ontoereikend (criteria 2,3 en 5) toereikend.

Change management (criteria 6) toereikend.

Continuïteit (criteria 7) toereikend.

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

PROCES	2019	2018
1. <u>Procedure autorisatiebeheer</u>		
2. Periodieke controle op juistheid ingerichte autorisaties		
3. Identificatie van gebruikers voor toegang tot systemen en data	* ₁	
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	

onvoldoende

verbeterpunten

voldoende

KORTE OMSCHRIJVING RESULTATEN	
1	Voor de applicaties in scope is nog geen formele normpositie opgesteld waarin de rollen per functionaris worden weergegeven.
2	Er wordt een review uitgevoerd op de juistheid van rollen en actualiteit van gebruikers door het afdelingshoofd.
3	Akkoord, generieke accounts zijn verklaarbaar vanuit gebruikersdoeleinden.
4	De wachtwoordeisen in S4SD voldoen aan de minimale te stellen eisen. Echter zijn er zijn 3 niet-persoonsgebonden gebruikersaccounts waarvan het wachtwoord in 2019 niet is gewijzigd (waarvan 1 verklaarbaar is vanuit gebruikersdoeleinden).
5	Akkoord. Alleen medewerkers uit de IT beheer-organisatie beschikken over superuserrechten, waardoor functiescheiding niet doorbroken is.
6	Akkoord. Testwerkzaamheden en een akkoord zijn aantoonbaar vastgelegd.
7	Akkoord. Er zijn maatregelen getroffen ten aanzien van continuïteit.

*₁ = Hoewel dit punt toereikend is, zijn in bijlage B zijn aanbevelingen opgenomen.

4.3 Actuele IT- ontwikkelingen en onze natuurlijke adviesrol (1/5)



IT en onze natuurlijke adviesrol

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

Systeemvervanging van Verseon (en Decade)

Aandachtspunten bij selectieproces

Aandachtspunten bij inrichting

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 Gouda 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. Naast de ITGC-aspecten (in het kader van de jaarrekeningcontrole) zien wij ook dat u bezig bent met belangrijke onderwerpen zoals de implementatie van de BIO en verder uitrollen van nieuwe systemen.

Systeemvervanging van Verseon (en Decade)

Gemeente Gouda heeft aangegeven dat per 2020 een selectieproces zal worden gestart voor een nieuw systeem voor het registreren en goedkeuren van de inkoopfacturen. Wij willen benadrukken dat belangrijke onderdelen functiescheiding (4-ogenprincipe) tussen codeur en fiatteur, een adequate workflow-inrichting en toereikende wachtwoordeisen mooie kansen biedt om verder in-control te komen. Een aantal belangrijke stappen bij een systeemselectie en -implementatie zijn:

- ▶ Het definiëren van de te behalen doelen;
- ▶ Het opstellen van een Request for Proposal;
- ▶ Het selecteren van een softwareleverancier;
- ▶ Het overeenkomen van een contract met deze leverancier;
- ▶ Het opstellen en uitvoeren van een project-, conversie- en implementatieplan;
- ▶ Het laten uitvoeren van een onderzoek naar de betrouwbaarheid van de al dan niet uitgevoerde conversie alsook naar een adequate inrichting en werking van het nieuwe systeem.

Vanuit controleperspectief willen wij graag een aantal belangrijke aandachtspunten meegeven die hier bijdragen aan een effectieve inrichting:

- ▶ Bepalen van functiescheiding in de gebruikers rollen/autorisaties in het nieuwe systeem (zie bijlage B voor aanbevelingen);
- ▶ Inrichting van adequate wachtwoordeisen voor (betreft: 2-factor, single-Sign-On, geen accounts vrijgesteld van verplicht wachtwoord wijzigen);
- ▶ Inrichten van audit-trails op mutaties aan workflow-inrichting en fiatteerregels per bestelling/factuur;
- ▶ Afscherming en betrouwbaarheid van de gegevensuitwisseling (referentie: Interfaces) tussen de financiële administratie systeem (Decade) en vanuit de scan-software naar dit systeem;
- ▶ Periodieke controle op facturen die niet conform het reguliere inkoopproces zijn gelopen;
- ▶ Integratie van inkoopregistratie met het contractmanagement (tbv spend-analyses).

Naast bovengenoemde aandachtspunten raden we aan om de ITGC's waar mogelijk van opvolging te voorzien (zie bijlage B), wat dient als randvoorwaarden voor het effectieve gebruik van de informatiesystemen. 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.

4.3 Actuele IT- ontwikkelingen en onze natuurlijke adviesrol (2/5)



E-facturering
betekent directe
koppeling
bronsystemen
aanbestedende
diensten

Aantal belangrijke
stappen in
e- facturering

E-facturering

Vanaf 18 april 2019 dienen alle aanbestedende diensten de benodigde voorzieningen te hebben getroffen om e-facturen te kunnen ontvangen en verwerken. E-facturatie houdt in dat alle facturen digitaal uitgewisseld worden in de vorm van een (XML-)bestand, waarbij de facturen elektronisch van het ene (bron)systeem worden verwerkt in het andere (doel)systeem zonder tussenkomst van een functionaris. Het adequaat inrichten van het e-facturatieproces brengt diverse vraagstukken met zich mee omtrent projectmanagement, de inrichting en beheersing van processen (o.a. authenticatie en autorisatie), de automatisering (koppelingen) en de betrouwbaarheid van de systemen (o.a. beveiliging).

De staatssecretaris heeft aangegeven te willen weten wat op dit moment de stand van zaken bij gemeentes is. Daarom moesten de gemeentes voor 1 juli 2018 aan het PIANOo-programmabureau doorgeven in welke fase de organisaties zich bevinden: zijn ze al gestart, hoe ver staat het met de voorbereiding, is het project al klaar of staat het on hold. Het is ook onze ervaring dat bij veel overheids-organisaties de IT General Controls nog niet zodanig op orde zijn, dat e-facturatie zonder veel moeite geïmplementeerd kan worden (zie voor onze bevindingen bij de gemeente verder in dit hoofdstuk).

Een aantal belangrijke stappen om het e-facturatieproces adequaat in te richten zijn:

- ▶ Het in kaart brengen van de risico's en impact van e-facturatie op organisatorische processen, werkwijzen, bemensing en IT-systemen;
- ▶ Het opstellen van een projectplan voor het implementeren van e-facturatie (mogelijk icm vorige slide);
- ▶ Het selecteren van een softwareleverancier;
- ▶ Het opstellen en uitvoeren van een projectplan;
- ▶ Het laten uitvoeren van een onderzoek naar de betrouwbaarheid van de systemen (beveiliging).

Wij hebben geconstateerd dat vanuit de gemeente Gouda dat e-facturatie mogelijk wordt met de implementatie van een nieuw inkoop-systeem (zie voorgaande pagina); daarmee wordt verwacht dit per 2020 geïmplementeerd te hebben en hiermee wordt voldaan aan de wettelijke verplichting om e-facturen te kunnen ontvangen en verwerken.

4.3 Actuele IT- ontwikkelingen en onze natuurlijke adviesrol (3/5)



Eén uniform kader voor informatiebeveiliging

Focus op risico-afwegingen en management

Uitdagingen

Baseline Informatiebeveiliging Overheid

In het afgelopen jaar hebben diverse ontwikkelingen plaatsgevonden, waaronder de aangescherpte privacywetgeving, de toenemende behoefte om informatie via internet uit te wisselen, alsook de ontwikkelingen op het gebied van Internet of Things, Cloud, Smart Cities en een verhoogde (digitale) interactie met burgers. Deze ontwikkelingen hebben ertoe geleid dat overheidsinstanties strengere eisen moeten stellen aan informatiebeveiliging. Het hebben van een adequate informatiebeveiliging is geen vrijblijvendheid meer, maar een harde noodzaak.

Daarom dienen vanaf 1 januari 2020 alle overheidsinstanties de benodigde voorzieningen te hebben getroffen om te voldoen aan de nieuwe vereisten van Baseline Informatiebeveiliging Overheid (BIO). Met de komst van de BIO zullen de bestaande baselines voor gemeenten, provincies, waterschappen en het rijk worden vervangen en zal een actueel en uniform normenkader geïntegreerd worden binnen de gehele overheid. De baseline zorgt voor één gezamenlijk en eenduidig normenkader binnen de gehele overheid gebaseerd op de internationaal erkende en actuele ISO-normatiek (ISO 27001:2017).

In het BIO-normenkader zullen risicoafwegingen en risicomanagement de basis vormen voor de manier en diepgang van de invulling van informatiebeveiliging voor overheidsorganisaties en hun onderlinge ketensamenwerking. Daarnaast vereist de BIO een expliciete betrokkenheid en verantwoordelijkheid van het lijnmanagement voor het implementeren en monitoren van informatiebeveiliging.

Een aantal belangrijke stappen om de BIO te implementeren zijn:

- ▶ 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 (omtrekt 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.

Wij hebben van gemeente Gouda begrepen dat BIO momenteel onder handen is. We hebben vernomen dat een overkoepelend informatiebeveiligingsbeleid (strategisch) bestaat met onderliggend de specifieke domeinen. Dit is bij de werkgroep informatiebeveiliging & privacy belegd, waarin per domein (bestaande uit CISO, HR, IT, Sociaal Domein, BAG/BGT, BRP, Inkoop, Privacy Officer en FG) een domeinspecialist is toegewezen. We raden aan om deze lijn door te zetten en dit de aandacht te geven die het verdient. Graag denken wij tijdig met u mee over de gevolgen van de BIO voor de interne beheersing van de processen.

4.3 Actuele IT- ontwikkelingen en onze natuurlijke adviesrol (4/5)



Veiliger samenwerken
door GGI

Landelijk project VNG
op het vlak van
Informatiebeveiliging

Mogelijke onderzoeken
en testen ten aanzien
van
informatiebeveiliging

GGI-Veilig

De toenemende noodzaak om informatiebeveiliging op orde te hebben, tezamen met de wens om slimmer en meer samen te werken, heeft ertoe geleid dat vanuit de Vereniging Nederlandse Gemeenten (VNG) een initiatief is gestart om een Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) op te zetten. Deze GGI creëert een veilige, samenhangende digitale infrastructuur, waardoor samenwerken tussen lokale overheden en andere overheden beter, veiliger en gemakkelijker wordt.

Om ervoor te zorgen dat GGI voldoet aan de veiligheidsnormen, is landelijk het project GGI-Veilig in het leven geroepen. GGI-Veilig heeft als doel de digitale weerbaarheid van gemeenten te verhogen door op een ontzorgende manier te ondersteunen bij de invulling van informatie-beveiliging. Dit wordt gerealiseerd door onder meer de verwerving van een collectieve SIEM/SOC-voorziening (Security Information Event Management / Security Operation Center).

Om de informatiebeveiliging optimaal in te richten en te beheersen is daarnaast een groot aantal maatregelen en testen mogelijk zoals compliance scans, pentesten (ethical hacking) en kwetsbaarheid scans.



Compliance

*Uitvoeren van compliance scans/
assessments/audits op
aandachtsgebieden BIO, BIG, AVG,
ENSIA, ISO-900x en -270x*



Pentesten

*Uitvoeren van Ethical Hacking tests
om mogelijke kwetsbaarheden in
informatie systemen inzichtelijk te
maken*



Netwerk hardening

*Onderzoeken van en adviseren over
robuustheid van ICT-infrastructuren
in gebruik bij lokale overheden*



Vulnerability

*Uitvoeren van vulnerability scans/
assessments op (het beheer van) de
ICT-infrastructuur van lokale
overheid*



Forensics

*Levering van ondersteuning bij
forensisch onderzoek n.a.v. security
incidenten*



SIEM

*Bieden van ondersteuning bij
inrichting en uitvoering van SIEM-
proces binnen lokale overheden*

4.3 IT-beheersing en onze natuurlijke adviesrol (5/5)



Data-analyse en process mining als mogelijke innovaties in de interne en externe controle

Voordelen en randvoorwaarden

Laagdrempelige en visuele data-analyses bieden nieuwe perspectieven op het proces

Data-analyse en process mining

In de praktijk zien wij dat steeds vaker dat de interne en/of externe controle gebruik maakt (of wil gaan maken) van geautomatiseerde controles. Data-analyse en process mining zijn voorbeelden van geautomatiseerde en gegevensgerichte controles die grote hoeveelheden data uit de geautomatiseerde systemen kunnen analyseren en controleren. Bij data-analyse ligt de nadruk op de kenmerken en afwijkingen in de gegevens, terwijl bij process mining het accent ligt op het proces dat de data hebben doorlopen.

Daarnaast zijn er (verschillende soorten) nieuw ontwikkelde technieken op basis van het zogenaamde machine learning, waarbij zonder manuele tussenkomst gegevens volledig worden geïnterpreteerd, geanalyseerd en gecontroleerd. De interne of externe controle kan zich dan richten op de gerapporteerde uitzonderingen en mogelijke risico's in de data.

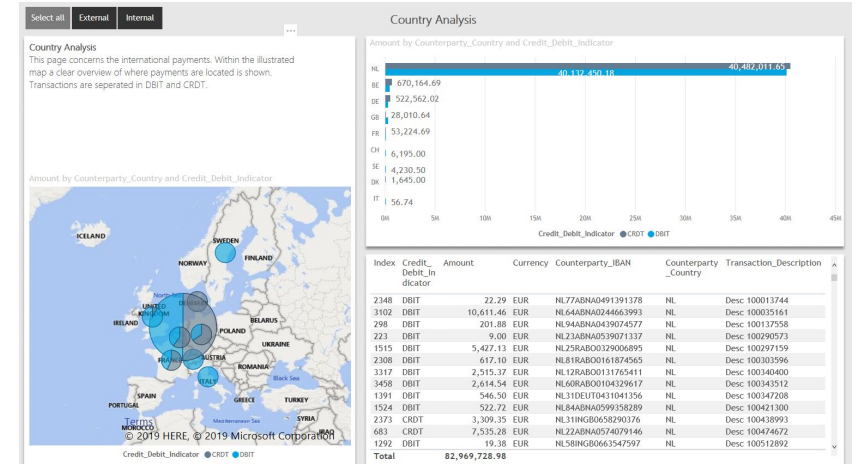
Het grote voordeel van data-analyse is dat de interne / externe controle niet plaatsvindt door middel van statistische steekproeven / deelwaarnemingen, maar dat alle data integraal kunnen worden geanalyseerd en gecontroleerd.

Afhankelijk van de in te zetten data-analyses zijn een aantal randvoorwaarden vereist om de betrouwbaarheid en juistheid van de data te waarborgen. In de basis dienen minimaal de IT General Controls rondom administrators en superusers, identificatie en wachtwoordinstellingen adequaat te zijn ingericht.

Wij hebben diverse data-analyses ontwikkeld op de veel voorkomende systemen bij gemeenten, zoals Key2Financien, Proactive, BNG en werken aan een data-analyse op Suite4Sociaal Domein.

Daarnaast werken wij aan innovaties, waarbij grote handmatige steekproeven deels of volledig kunnen worden geautomatiseerd.

Het plaatje hiernaast geeft een voorbeeld van een visueel weergegeven data-analyse van betalingsgegevens, waaronder bijvoorbeeld het inzicht in buitenlandse betalingen.



Wij gaan graag met u in gesprek over de toepasbaarheid van data-analyse, process mining, etc. in uw organisatie en uw ambities hierin.

5. Bevindingen interne controle

5.1 Verbijzonderde interne controle

5.1 Verbijzonderde interne controle (1/5)

Met ingang van verslagjaar 2021 moet het college een (onderbouwde) mededeling doen omtrent rechtmatig handelen

Mededeling door college vraagt om aanscherpingen in de interne beheersing t.a.v. rechtmatigheid

Vernieuwing accountantscontrole - rechtmatigheidsverklaring college

In het VNG-rapport 'Vernieuwing accountantscontrole gemeenten' (juli 2015) is benadrukt dat het college primair verantwoordelijk is voor de naleving van wet- en regelgeving en dat de gemeenteraad verantwoordelijk is voor het toezicht hierop. In de huidige situatie, waarin de accountant een rechtmatigheidsverklaring verstrekt, lijkt de verantwoordelijkheid bij de accountant te liggen of lijkt het erop dat het college zich moet verantwoorden aan de accountant. Om daar verandering in aan te brengen heeft commissie Depla de aanbeveling gedaan dat het college een rechtmatigheidsverklaring opneemt in de jaarrekening. In de mei-circulaire 2018 van het gemeentefonds (paragraaf 5.10) is aangegeven dat dit naar verwachting met ingang van verslagjaar 2021 zal worden ingevoerd.

Belangrijk argument om de bedoelde vernieuwing door te voeren is het democratisch proces. Het college is immers uiteindelijk verantwoordelijk voor de naleving van de wet- en regelgeving en dan is het zinvol de discussie over de rechtmatigheid hiervan te laten plaatsvinden tussen college enerzijds en gemeenteraad anderzijds. Het ministerie wil dit najaar starten met een pilot. Mede afhankelijk van de resultaten van de pilot wordt besloten of en op welke wijze de rechtmatigheidsverantwoording zal worden ingevoerd. Het ministerie van Binnenlandse Zaken zal de commissie BBV, de VNG, het IPO en de NBA betrekken in de nadere uitwerking van deze verplichting.

Om deze verplichting te kunnen invoeren moet de Gemeentewet, het Besluit Accountantscontrole Decentrale Overheden (BADO), de Kadernota rechtmatigheid, etc. nog worden aangepast. Uitgaande van de invoeringsdatum 2021, betekent dit dat er nog ruim twee jaren zijn om dit voor te bereiden. Dat betekent ook dat voor wat betreft de accountantscontrole de rechtmatigheidscontrole nog tenminste voor de boekjaren 2019 en 2020 in scope zal zijn.

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

Wij denken graag met u mee over de opzet van een projectplan, gericht op de invoering van deze In Control Statement/ rechtmatigheidsverklaring, mede in relatie tot de Verbijzonderde Interne Controle (VIC) bij de gemeente Gouda (zie ook hierna).

5.1 Verbijzonderde interne controle (2/5)

Three Lines of Defense-model als referentiekader

Wij onderschrijven de door het management gemaakte keuzes en herkennen de 3LoD

Three Lines of Defense-model

In de theorie van governance, bedrijfsvoering en risicomanagement wordt vaak het zogenaamde Three Lines of Defense-model (3LoD) als referentie- en inrichtingsmodel gehanteerd. Dit referentie-model is meer dan alleen een organisatiestructuur en het benoemen van rollen. Het is een (internationaal gangbare) manier van (samen)werken en denken die kan bijdragen aan het versterken van de interne beheersing en het managen van risico's, inclusief het verlagen van de 'cost of control'.

Op de volgende pagina geven wij een nadere toelichting op het Three Lines of Defense-model.

Ons beeld

De huidige opzet van de 3LoD is in de huidige structuur te onderkennen en in opzet aanwezig. Daarmee onderschrijven wij de beschreven keuzes, waarbij wij (hierna) nog wel een aantal afwegingen en adviezen geven t.a.v. de 3e lijn; de VIC.

Vanzelfsprekend toetsen wij de structuur en taken niet specifiek, maar beoordelen wij de ondersteunende processen en adviseren wij (vanuit onze natuurlijke adviesrol) over planning & control en risicomanagement. Middels deze management letter beogen wij daarnaast op het niveau van processen en de jaarrekening een bijdrage te kunnen leveren aan de optimalisering van de interne beheersing in alle drie de lijnen.



5.1 Verbijzonderde interne controle (3/5)

Wat is het Three Lines of Defence-model?

Onze controleaanpak is, naast het controleren van de jaarrekening, gericht op het verbeteren van uw bedrijfsvoering inclusief digitalisering hiervan. In onze controle hanteren wij daarvoor het Three Lines of Defence-model. Dit model geeft handvatten om te beoordelen waar in de interne beheersingsrisico's worden ondervangen:

1st Line of Defence

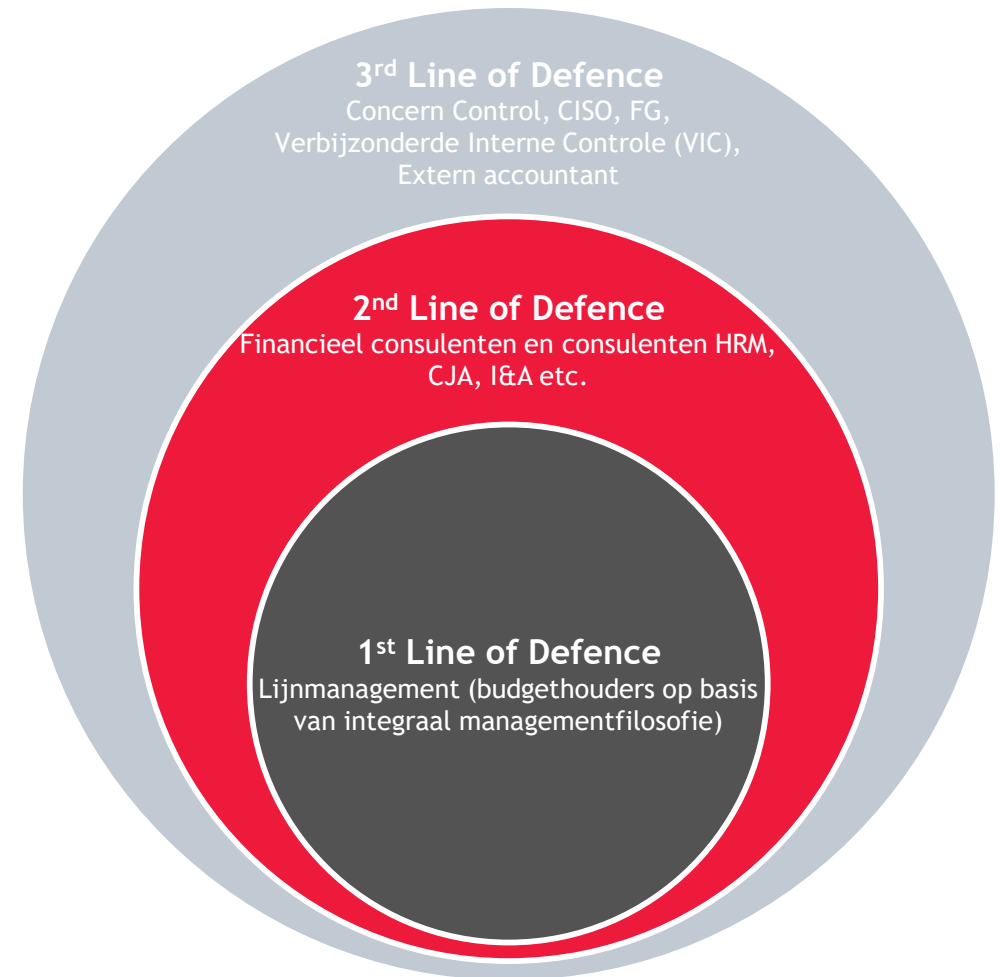
Uitgangspunt van het 3LoD-model is dat het lijnmanagement verantwoordelijk is voor haar eigen (operationele) processen. Om te borgen dat de uitvoering van processen adequaat verloopt (rechtmatig en getrouw) worden interne beheersmaatregelen uitgevoerd door de functionarissen, die betrokken zijn bij de uitvoering van de dagelijkse activiteiten in de organisatie en het lijnmanagement. Deze beheersmaatregelen - uitgevoerd door bestuur, management en uitvoerende functionarissen - vormen de eerstelijnscontroles.

2nd Line of Defence

Daarnaast moet er wel een functie zijn die de 1^e lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. In het geval van de gemeente Gouda de interne beheerscyclus, uitmondend bij de financieel consulenten en consulenten HRM, CJA, I&A etc. . De planning- & controlcyclus en het risico-management zijn daarbij belangrijke instrumenten.

3rd Line of Defence: Concern Control, VIC en externe audit

Tenslotte kan het wenselijk zijn dat er binnen de organisatie een functie bestaat die controleert of de 1^e lijn haar taken goed uitvoert en beoordeelt of het samenspel tussen de 1^e en 2^e lijn soepel functioneert. De derde lijn is niet verantwoordelijk voor het nemen van de beslissingen (eerste lijn) en evenmin voor het ontwerpen en implementeren van de systemen voor de beheersing van bedrijfsprocessen (tweede lijn). De 3^e lijn zou daarover objectief en onafhankelijk een oordeel moeten vellen en adviezen tot verbetering geven. Eventueel kan ook de externe accountant als 3^e lijn worden gezien, maar die staat meer op afstand en controleert primair de jaarrekening.



5.1 Verbijzonderde interne controle (4/5)

BADO notitie
verbijzonderde interne
controle decentrale
overheid

Vier varianten van VIC:

- Instrument
aanlevering van
stukken
- Onderdeel van het
interne
beheersingskader
- Interne
beheersmaatregel
- Interne auditfunctie
(Standaard 610)

Verbijzonderde Interne Controle

De afgelopen jaren is veel discussie geweest over de eisen die gesteld moeten worden aan de onafhankelijkheid, positie en kwaliteit van de Verbijzonderde Interne Controle (VIC) en de wijze waarop accountants gebruik kunnen maken van de VIC. De commissie Bedrijfsvoering, Auditing Decentrale Overheden (BADO) heeft op 14 februari 2019 de notitie De verbijzonderde interne controle bij decentrale overheid uitgebracht met als doel een handreiking te bieden aan decentrale overheden ten aanzien van de inrichting van de verbijzonderde interne controle en de mogelijkheden voor de accountant om hiervan gebruik te kunnen maken.

Samenvattend worden in de notitie vier varianten beschreven:

1. de VIC als instrument om de aanlevering van stukken aan de accountant te verbeteren;
2. de VIC als onderdeel van het interne beheersingskader om toezicht te houden op de uitvoering van interne beheersingsmaatregelen;
3. de VIC als interne beheersingsmaatregel, waarop de accountant kan steunen bij zijn organisatiegerichte werkzaamheden;
4. de VIC als interne auditfunctie (IAF, zoals bedoeld in Standaard 610).

1. Aanlevering stukken

Allereerst kan de VIC behulpzaam zijn bij het verzamelen van allerlei gegevens en onderliggende stukken, die nodig zijn voor de controle door de accountant. Door bijvoorbeeld tijdig een kwaliteitstoets uit te voeren op de volledigheid van de stukken, kan een positieve invloed worden uitgeoefend op de doorlooptijd van de controle. Voorts kan een goede aanlevering van stukken, een bijdrage leveren aan de efficiency van de accountantscontrole.

2. Interne beheersingskader

In deze situatie gebruikt de accountant de VIC als een van de belangrijke informatiebronnen om kennis te verkrijgen van de organisatie en zo richting te geven aan zijn controle. Op deze wijze worden risico's geïdentificeerd en ingeschat, om een basis voor het opzetten en uitvoeren van verdere controlewerkzaamheden te verkrijgen. De accountant zal in deze situatie kennisnemen van de geaccordeerde jaarplannen van de VIC en de werkzaamheden en de bevindingen van de VIC.

3. De VIC als interne beheersingsmaatregel, waarop de accountant kan steunen bij zijn organisatiegerichte werkzaamheden

De derde variant is de situatie waarin de accountant kan en wil steunen, op de interne beheersingsmaatregelen van de decentrale overheid. De VIC omvat interne beheersingsmaatregelen, die de accountant kan toetsen in het kader van zijn organisatie- en procesgerichte werkzaamheden.

4. De VIC als interne auditfunctie

In deze situatie concludeert de accountant op basis van zijn werkzaamheden, dat de VIC voldoet aan de eisen die Standaard 610 bevat voor de interne auditfunctie (IAF: zie de paragraaf over de drie verdedigingslijnen). Dit veronderstelt het volgende:

- dat de organisatorische positie en relevante beleidslijnen, alsmede procedures van de interne auditfunctie, op adequate wijze de objectiviteit van de interne auditors ondersteunen;
- het competentieniveau van de interne auditfunctie gewaarborgd is;
- dat binnen de interne auditfunctie een systematische en gedisciplineerde benadering gehanteerd wordt, inclusief de kwaliteitsbeheersing.

5.1 Verbijzonderde interne controle (5/5)

Ons beeld van de VIC

Ons beeld van de VIC

De VIC beoogt het vergroten van de transparantie met betrekking tot de wijze waarop de gemeente Gouda haar bedrijfsvoering ingericht heeft. De VIC is gericht op de werking van de financiële bedrijfsprocessen en heeft als primair doel vast te stellen of de administratieve organisatie en de daarin vervatte maatregelen van interne controle voldoende waarborgen dat de financiële informatievoorziening juist en volledig is, materieel niet afwijkt van de werkelijkheid en dat wordt voldaan aan de van toepassing zijnde wet- en regelgeving.

Uit het intern controleplan 2019/2020 Verbijzonderde interne controle blijkt dat de VIC-werkzaamheden door twee medewerkers van concernstaf worden uitgevoerd (medewerker concernstaf en de controller). De VIC voert haar onderzoeken onafhankelijk van het betreffende lijnmanagement uit op basis het door het college vastgestelde en aan de gemeenteraad ter informatie verstrekte, intern controleplan 2019/2020 Verbijzonderde Interne controle. Op basis van vooral wet- en regelgeving worden onderzoeken uitgevoerd in het kader van doelmatigheid, doeltreffendheid en rechtmatigheid.

De eisen die Standaard 610 stelt aan de externe accountant bij de beoordeling van de objectiviteit en competentie van de internal audit functie zijn (zeer) hoog. Volgens Standaard 610 moet de VIC voldoen aan het kwaliteitsniveau dat ook voor de controlerend accountants zelf geldt. Dit impliceert interne kwaliteitseisen zoals het vierogenprincipe bij de uitvoering van de VIC, een zichtbaar detailreview van alle uitgevoerde werkzaamheden en permanente educatie.

De geplande onderzoeken komen tot stand op basis van risico-inschatting, actualiteit en bestuurlijke relevantie. Volgens het intern controleplan 2019/2020 richt de VIC zich op de onderdelen inkoop en aanbestedingen, inkoop en factuurcontrole, HRM proces, Jeugdzorg, WMO, Werk en Inkomen, Subsidieproces, Grondexploitaties, verbonden partijen en Borg en garantstellingen, verhuuropbrengsten, grondexploitaties, grondverkoop en IT-Omgeving. In bijlage 3 van het intern controleplan 2019/2020 Verbijzonderde interne controle is opgenomen welke 'testsheets' (werkprogramma's) nog in ontwikkeling zijn. Diverse werkprogramma's zijn nog in ontwikkeling en zullen in 2020 beschikbaar komen. Het is van belang dat deze aansluiten op de huidige AO/IB (is testen van IB-maatregelen op werking mogelijk). Indien testen van werkzaamheden niet mogelijk is dan zullen de werkzaamheden gegevensgericht dienen plaats te vinden aan de hand van wet- en regelgeving zoals opgenomen in het normenkader. De werkprogramma's moeten dan aansluiten op de wetteksten en verordeningen, waarbij het uitgangspunt de financiële rechtmatigheid is waarbij artikelen voor toetsing in aanmerking komen indien sprake is van 'recht, hoogte en duurbepalingen'.

Wij concluderen dat het op dit moment niet realistisch is om te voldoen aan de eisen van de COS 610 c.q. dit op korte termijn ook niet het streven is / moet zijn. Wel is de kwaliteit zodanig dat, in goede samenwerking, in belangrijke mate gebruik kan worden gemaakt van de door de VIC (in overleg met ons) voorbereide werkzaamheden; ofwel de derde variant. In 2019 rapporteren wij vanuit dit uitgangspunt met betrekking tot de Verbijzonderde Interne Controle (VIC) van de gemeente Gouda.

5.1 Verbijzonderde interne controle (5/5)

Variant: VIC toetst interne beheersmaatregelen

Aanbevelingen

Wij constateren dat de VIC in de uitvoering van haar werkzaamheden nu primair gericht is op het uitvoeren van de in het jaarplan opgenomen (gegevensgerichte) test aantallen. In onze optiek kan de meerwaarde van de VIC voor de organisatie nog worden vergroot door 'aan de voorkant' nog meer expliciet aandacht te geven aan de opzet en inrichting van de AO/IB per proces, alsmede de advisering daaromtrent (systeem-procesgericht).

Toelichting:

Wij hebben een opzetgesprek gevoerd inzake de uitkeringen zoals deze vallen onder het sociaal domein. Belangrijkste bevindingen ten aanzien van dit proces zijn:

- ▶ *Er is sprake van controletechnische functiescheiding binnen het proces. Iedere verstrekking van een beschikking dient door een tweede collega te worden gecontroleerd (aan de hand van een checklist) en hiervoor dient getekend te worden (IB-maatregel)*
- ▶ *Maandelijks vinden er door interne controle/ kwaliteitsmedewerker een aantal controles plaats op de doorlopen werkprocessen die maand*
- ▶ *De verbijzonderde interne controle voert een review uit op de werkzaamheden van de interne controle medewerker.*

Wij zijn van mening dat de gemeente Gouda op korte termijn de AO/IB moet aanvullen, zodat alle interne beheersingsmaatregelen goed zijn beschreven. De verbijzonderde interne controle zal dan onder aansturing van de controller vaststellen dat:

- ▶ *De onderkende interne beheersingsmaatregelen in het proces werken (toetsing juiste toepassing 4-ogen)*
- ▶ *De interne controle/ kwaliteitsmedewerker de testwerkzaamheden juist heeft uitgevoerd en de foutevaluatie goed heeft uitgevoerd en*
- ▶ *Zelfstandig nog enkele dossiercontroles uitvoert op dossiers die geen onderdeel hebben gemaakt van de kwaliteitscontrole. Daarnaast kunnen er vanuit het college/directie nog risicogebieden onderkend worden waarop een verbijzonderde interne controle dient plaats te vinden (onderkende risico's, leemten AO/IB etc.).*

Kort samengevat zouden wij verwachten dat de VIC zich, alvorens over te gaan tot het uitvoeren van de test aantallen, ook richt op het vastleggen / uitwerken van de procesbeschrijvingen en het uitvoeren en documenteren van de omvattende lijncontroles per proces. De testwerkzaamheden zouden zich vervolgens liefst 1:1 moeten verhouden tot de binnen de verschillende processen geïdentificeerde 'key-controls' of beheersmaatregelen. Een key-control is een control die de betrouwbare procesgang borgt en waarop gesteund kan worden voor de interne en externe controle. Indien het testen van de werking niet mogelijk is omdat interne beheersingsmaatregelen niet aanwezig zijn, zijn gegevensgerichte werkzaamheden de enige mogelijkheid.

Wij willen graag naar aanleiding van deze managementletter, het interne controleplan 2019/2020 Verbijzonderde Interne Controle en het opgestelde memo aan de directie inzake toepassing van het 'three lines of defence model', met uw organisatie in gesprek om de verbijzonderde interne controle voor 2019 vorm te geven (aantallen) maar met name te richten op de ontwikkelingen en mogelijkheden voor de toekomst.

A. Detailbevindingen IT

Bevinding	PROCEDURE AUTORISATIEBEHEER & PERIODIEKE CONTROLE OP JUISTHEID INGERICHTE AUTORISATIES	KANS: Middel
Jaar van constatering	2019	IMPACT: Middel
	We hebben geconstateerd dat de volgende controles aanwezig zijn: ▶ Voor 1 gebruiker per applicatie vastgesteld dat de aanvraag voor toekennen en intrekken worden structureel vastgelegd; ▶ Voor 1 gebruiker per applicatie vastgesteld dat dit account tijdig geblokkeerd is bij uitdiensttreding; ▶ Voor 1 periodieke controle per applicatie is vastgesteld dat een review is uitgevoerd op de juistheid van rollen en actualiteit van gebruikers door het afdelingshoofd. Vastgesteld op basis van inspectie en observaties rondom de procedure autorisatiebeheer dat: ▶ Rollen in de applicaties worden aangevraagd op basis van inzicht van de leidinggevende en/of applicatiebeheerder. Hierdoor bestaat het risico dat een leidinggevende naar eigen inzicht mogelijk onterecht teveel rollen/rechten aanvraagt*; ▶ Rollen worden niet toegekend op basis van een formele normpositie, die goedgekeurd is door het management van gemeente Gouda. <i>* Dit punt behoeft nuancering gezien bij Decade en Suite4SociaalDomein maar één menu(-rol) of gebruikersrol per gebruiker toegekend kan worden.</i>	
Risico/Gevolg	Door het ontbreken van adequate naleving op gebruikersbeheerprocedures bestaat het risico dat personen teveel of onterechte rollen/rechten bezitten en hierdoor de functiescheidingsprincipes van de gemeente Gouda mogelijk doorbroken kunnen worden met het risico op ongeautoriseerde handelingen.	
Ons advies/ Uw aanvullende werkzaamheden	Het verdient de aanbeveling om een formele normpositie voor de applicaties in scope op te stellen welke applicatie overstijgend is zodat de belangrijkste gewenste functiescheidingsprincipes zichtbaar zijn gemaakt. Om administratieve lasten te voorkomen raden we aan om voornamelijk te focussen op de belangrijkste functiescheidingen 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 rollen/rechten worden toegekend. Er wordt reeds een periodieke controle op gebruikers en rollen uitgevoerd. Hierbij verdient het de aanbeveling om de periodieke review 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 een controle kunnen uitvoeren om na te gaan of alle uitdiensttreders (tijdig) zijn geblokkeerd voor de applicaties in scope.	
Reactie management/ Opvolging		

Bevinding	IDENTIFICATIE VAN GEBRUIKERS	KANS: Middel
Jaar van constatering	2019	IMPACT: Laag
	Wij hebben vastgesteld dat niet-persoonsgebonden (hierna: generieke) gebruikers in de applicaties in scope verklaarbaar zijn vanuit gebruikersdoeleinden. <i>Hoewel dit geen directe impact heeft op de controle van de jaarrekening, is geconstateerd dat er bij de applicaties in scope een aantal niet-persoonsgebonden accounts bestaan, die beschikken over fiatteer-rechten. We raden vanuit gebruikershygiëne aan om deze accounts op naam te stellen.</i>	
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	We raden gemeente Gouda aan om: ► Generieke accounts 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		

Bevinding	WACHTWOORDBELEID		KANS: middel
Jaar van constatering	2019		IMPACT: hoog
	Op basis van systeemwaarnemingen hebben wij vastgesteld dat de volgende wachtwoordvereisten worden afgedwongen voor de applicaties in scope:		
	WACHTWOORDINSTELLINGEN	Decade & Verseon (2-factor authenticatie via Active Directory)	S4SD
	Minimale wachtwoordlengte	7 karakters	11 karakters
	Maximale wachtwoordleeftijd	90 dagen	100 dagen*
	De laatste # wachtwoorden mogen niet hergebruikt worden	3x laatste ww	3x laatste ww
	Het account wordt na # foutieve inlogpogingen geblokkeerd	5 foutieve inlogpogingen	8 foutieve inlogpogingen
	Wachtwoordcomplexiteit	2-factor authenticatie is ingesteld.	Ingeschakeld
	Initiële wachtwoordwijziging	Afgedwongen	Afgedwongen
NB. De dikgedrukte tekst in de tabel behoeft verbetering. * Op basis van inspectie van de S4SD-gebruikerslijst vastgesteld dat er 3 niet-persoonsgebonden gebruikersaccounts zijn, waarvan het wachtwoord in 2019 niet is gewijzigd (waarvan 1 verklaarbaar is vanuit gebruikersdoeleinden).			
Risico/Gevolg	Gemeente Gouda loopt op basis van het ontbreken van adequate wachtwoordinstellingen in de applicaties het risico dat wachtwoorden door onbevoegden worden achterhaald en kunnen worden misbruikt. Hierdoor zouden mogelijk de functiescheidingsprincipes doorbroken kunnen worden en ongeautoriseerde handelingen worden uitgevoerd.		
Ons advies/ Uw aanvullende werkzaamheden	Het verdient aanbeveling om de wachtwoord instellingen te evalueren. Wij bevelen aan om, daar waar technisch mogelijk, de volgende wachtwoordeisen in te stellen:		
	WACHTWOORDINSTELLINGEN	BDO best practice norm	BIO norm (excl. 2-factor authenticatie)* ²
	Minimale wachtwoordlengte	8 karakters	8 karakters (of 20 karakters)
	Maximale wachtwoordleeftijd	90 dagen	180 dagen
	De laatste # wachtwoorden mogen niet hergebruikt worden	12 wachtwoorden	Niet expliciet benoemd
	Het account wordt na # foutieve inlogpogingen geblokkeerd	5 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 v1.03 ’ en hier kunnen geen rechten aan ontleend worden.			
Reactie management / Opvolging			

Bevinding	SUPERUSER-RECHTEN	KANS: middel
Jaar van constatering	2019	IMPACT: hoog
	We hebben geconstateerd dat de volgende controles aanwezig zijn: ► Wij hebben vastgesteld dat voor de applicaties in scope een functiescheiding bestaat tussen lijnorganisatie en IT- beheer organisatie. <i>Geen verdere bevindingen.</i>	
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 van applicaties. 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		

Bevinding	WIJZIGINGENBEHEER UPDATES	KANS: middel
Jaar van constatering	2019	IMPACT: hoog
	We hebben geconstateerd dat de volgende controles aanwezig zijn: ▶ Wijzigingsaanvragen voor Decade en S4SD worden structureel vastgelegd; ▶ Wij hebben voor 1 doorgevoerde wijziging voor Decade en S4SD vastgesteld dat testwerkzaamheden (op basis van een testscenario) en akkoord zijn vastgelegd; ▶ Decade en S4SD beschikken over een logisch gescheiden test- en productie omgeving. <i>Het bestaan van testwerkzaamheden een akkoord bij een doorgevoerde wijziging in Verseon kon niet worden beoordeeld, omdat er gedurende het boekjaar geen wijzigingen zijn doorgevoerd in de productie-omgeving van Verseon vanwege de uitfasering. Derhalve is er door gemeente Gouda ook geen separate test-omgeving ingericht.</i>	
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 dat achteraf niet kan worden vastgesteld of een softwarewijziging terecht in de productieomgeving is geplaatst.	
Ons advies/ Uw aanvullende werkzaamheden	Het verdient aanbeveling om een procedure voor wijzigingsbeheer te beschrijven en te hanteren voor de applicaties in scope. In deze procedure is 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.	
Reactie management/ Opvolging		

Bevinding	IT CONTINUÏTEIT	KANS: laag
Jaar van constatering	2019	IMPACT: Middel
	We hebben geconstateerd dat de volgende controles aanwezig zijn: ▶ Fysieke beveiligingsmaatregelen tot de serverruimte (UPS, brandmelder, blusser en temperatuurregeling); ▶ Een ingericht back-upschema met bijhorende retentietijden en monitoring op foutieve back-ups; ▶ Een uitwijktest is uitgevoerd op de productie-data uit de systemen; <i>Hoewel dit geen directe impact heeft op de controle van de jaarrekening, is geconstateerd dat er bij toegangslijsten tot de serverruimtes in totaal 1 raadslid en 2 niet-persoonsgebonden calamiteitspassen bestaan, die toegang hebben tot de serverruimte.</i>	
Risico/Gevolg	Door een te hoog aantal personen met toegang tot de serverruimte bestaat het risico dat kritieke data of apparatuur beschadigd en/of ontvreemd worden.	
Ons advies/ Uw aanvullende werkzaamheden	Het verdient aanbeveling om de toegang tot de serverruimte tot de strikt noodzakelijke medewerkers te beperken. We raden aan om de passen na te gaan en waar nodig te beperken.	
Reactie management/ Opvolging		