

Aan het college van burgemeester en wethouders
van de gemeente Heemstede
Postbus 352
2100 AJ HEEMSTEDE

Datum
12 november 2019

Behandeld door
J. Trompert

Ons kenmerk
2019-ML-30000701

Onderwerp
Managementletter 2019

Geacht college,

Als onderdeel van de jaarrekeningcontrole 2019 hebben wij in oktober 2019 de tussentijdse controle voor uw gemeente uitgevoerd. Deze tussentijdse(interim) controle is vooral gericht op onderwerpen die van belang zijn voor een goede en betrouwbare jaarverslaggeving. Naar aanleiding van deze interimcontrole informeren wij u in deze managementletter over onze belangrijkste bevindingen.

Wij vertrouwen erop dat wij met deze rapportage een zinvolle bijdrage leveren aan het (verder) verbeteren van de interne beheersing van het planning & controle-instrumentarium binnen uw gemeente.

In deze managementletter hanteren wij de volgende indeling:

1. Inleiding;
2. Conclusie en samenvatting;
3. Heemstede, in control;
4. Bevindingen interimcontrole 2019;
5. Actualiteiten en aandachtspunten jaarrekeningcontrole 2019.

Bijlage 1 : Follow-up bevindingen voorgaande jaren

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

Met vriendelijke groet,

Astrium Overheidsaccountants B.V.

Was getekend,
Drs. R.A.D. Knoester RA

1. Inleiding

Deze interimcontrole is afgesloten met een afzonderlijke managementletter. De bevindingen in deze managementletter stellen u in staat om, daar waar van toepassing, maatregelen te nemen om de interne beheersing te verbeteren en daarmee de betrouwbaarheid van de financiële informatie te borgen en/of te optimaliseren. Als medegebruiker van uw financieel informatie-systeem richten wij ons bij de interimcontrole voornamelijk op de opzet, het bestaan en de werking van het stelsel van administratieve organisatie en maatregelen van de interne beheersing.

Ons tussentijds onderzoek strekt zich niet verder uit dan noodzakelijk is om tot een oordeel te komen over de jaarrekening 2019. Daarbij beoordelen wij voornamelijk de opgenomen maatregelen van administratieve organisatie en interne beheersing binnen de processen, die zijn gericht op het waarborgen van een betrouwbare informatievoorziening zowel binnen uw gemeente als naar buiten toe aan derden.

Wij beseffen ons dat onze managementletter in beginsel positief-kritisch is. Wij rapporteren immers voornamelijk over de eventuele leemten of mogelijkheden ter verbetering van de financiële en administratieve processen, de administratieve organisatie daarvan en daarin opgenomen maatregelen van interne beheersing. Wij geven in onze managementletter (op hoofdlijnen) aan op welke wijze verbeteringen van de administratieve organisatie en daarin opgenomen maatregelen van interne beheersing kunnen worden doorgevoerd. Wij zijn graag bereid u te ondersteunen in het uitwerken van beheersingsmaatregelen in relatie tot de aanbevelingen en oplossingsrichtingen zoals beschreven in deze managementletter.

2. Conclusie en samenvatting

2.1 Conclusie ‘administratieve organisatie en interne beheersing’

Ons beeld is dat de administratieve organisatie en interne beheersing (de controles in de lijn, gecombineerd met de verbijzonderde interne controles) van de gemeente Heemstede **voldoet aan de daaraan te stellen eisen**.

De medewerkers die wij gesproken hebben, zijn betrokken en hebben veel kennis van het taakveld waarin zij werkzaam zijn. Ten aanzien van de processen waarbij in het proces zelf nog onvoldoende interne controlehandelingen zijn ingebouwd zijn op een goede manier aanvullende verbijzonderde interne controlewerkzaamheden ingeregeld. Bij de uitvoering van onze controlewerkzaamheden kunnen wij hierdoor goed gebruik maken van deze uitgevoerde aanvullende werkzaamheden. Daarnaast concluderen we dat er stappen vooruit zijn gemaakt op basis van de aanbevelingen uit voorgaande rapportages. Deze ontwikkelingen zijn de in bijlage toegevoegd.

2.2 Samenvatting managementletter

De managementletter kan in de volgende tabel worden samengevat met daarin onze bevindingen.

Bevinding (verwijzing naar managementletter)	Prioriteit	Advies
<p>Hoofdstuk 3.3</p> <p><i>In de optimale situatie zijn interne controlehandelingen ingericht in de lijn van de processen. In de huidige situatie zijn de interne controlehandelingen belegd bij controlemedewerkers.</i></p>	<p>Middel</p>	<p>De verwachting is dat vanaf 2021 het college een rechtmatigheidsverantwoording af moet leggen in de jaarrekening. De politieke aanspreekbaarheid voor het college inzake rechtmatigheid wordt hiermee vergroot. De inrichting van interne controlehandelingen in de lijn draagt bij aan de beheersing van processen door het management (inclusief college) en de beheersing van de uitkomsten in de rechtmatigheidsverantwoording. Daarnaast wordt het door interne controlehandelingen in de lijn te organiseren voor de controlemedewerkers buiten de lijn mogelijk om te toetsten op deze handelingen (verbijzonderde interne controle). De uitkomsten van deze toetsen geeft het college de juiste tools om de rechtmatigheidsverantwoording af te kunnen leggen.</p> <p>Wij adviseren u derhalve om de interne controlehandelingen in de lijn te organiseren en de uitkomsten van deze handelingen zichtbaar vast te laten leggen, waardoor achteraf verbijzonderde interne controle kan plaatsvinden op de uitgevoerde werkzaamheden.</p>
<p>Hoofdstuk 3.4</p> <p><i>Binnen de gemeente worden interne controlehandelingen uitgevoerd door een controlemedewerker buiten de lijn. Wij hebben kennis genomen van het interne controleplan (IC-plan) en de interne controle (IC) werkzaamheden. Wij stellen vast dat in het plan nog onvoldoende aandacht is voor de koppeling van risico's aan processen.</i></p>	<p>Middel</p>	<p>Wij adviseren het IC-plan risicogericht in te kleden. Door de risico's te koppelen aan de interne controlehandelingen is zichtbaar met welke doel de interne controlehandelingen worden uitgevoerd</p> <p>Wij adviseren ter verbetering van de IC werkzaamheden om de volgende processen in de IC te betrekken:</p> <ul style="list-style-type: none"> - Memoriaalboekingen; - Investeringskredieten; - Voorzieningen; - IT, waaronder inrichting van autorisaties in de applicaties; Prestatielevering WMO en Jeugdzorg.

Bevinding (verwijzing naar management-letter)	Prioriteit	Advies
<p>Hoofdstuk 4.2.1</p> <p><i>In 2019 heeft de gemeente een aanbestedingstraject doorlopen voor de outsourcen van een groot deel van de IT-beheeractiviteiten. Het beheer van de database wordt geoutsourcet naar een externe partij. Door deze outsourcing is het noodzakelijk dat een datamigratie plaatsvindt van de servers van de gemeente naar de server van de externe partij.</i></p>	Hoog	<p>Uit de door ons gevoerde gesprekken bij de interimcontrole (eerste helft oktober 2019) hebben wij vastgesteld dat onderstaande punten nog niet uitgewerkt en afgerond zijn:</p> <ul style="list-style-type: none"> • Opstellen van een testplan inzake de waarborging van de continuïteit en betrouwbaarheid van de geautomatiseerde omgeving. • Opstellen van een plan van aanpak ten behoeve van de interne beheersing van dit traject. • Opstellen van een plan inzake het verwijderen van de gegevens van de huidige servers na afronding van een succesvolle datamigratie.
<p>Hoofdstuk 4.2.2</p> <p><i>De gemeente heeft een controleplan opgesteld ter beheersing van de processen in de administratieve organisatie. De rol van informatiesystemen wordt binnen organisaties steeds groter.</i></p>	Hoog	<p>De outsourcing van het IT-beheer vraagt een andere aanpak van de beheersing van general IT controls door de gemeente.</p> <p>Advies: Het is noodzakelijk dat de gemeente anticipeert op de veranderingen in het proces van systeembeheer en de processen zodanig inricht teneinde inzicht te blijven houden over de effectiviteit van de general IT controls.</p>
<p>Hoofdstuk 4.3</p> <p><i>De jaarstukken van de gemeente zijn onderhevig aan verschillende posten met schattingselementen. Deze schattingselementen zijn gevoelig voor beïnvloeding door het management en vormen het risico tot management override.</i></p>	Middel	<p>Wij adviseren om de beheersing van schattingselementen in de financiële cijfers te verwerken in de planning- & control cyclus en gedurende het jaar interne controlewerkzaamheden te verrichten.</p>

Bevinding (verwijzing naar management-letter)	Prioriteit	Advies
<p>Hoofdstuk 4.4.1</p> <p><i>Aanbesteding. Er is geen totaaloverzicht van de inkoop van de gemeente gedurende het jaar, waardoor de gemeente het risico loopt dat verschillende budgetbeheerders bij dezelfde leverancier inkoop en onrechtmatige bestedingen worden gedaan.</i></p>	Middel	<p>Verkrijg op basis van een contractenregister inzicht in het totaal van bestedingen van de gemeente. Daarnaast adviseren wij u te overwegen om een centrale inkooporganisatie in te stellen.</p>
<p>Hoofdstuk 4.4.2</p> <p><i>Onrechtmatigheid inzake niet naleving Europese aanbestedingsregels.</i></p>	Hoog	<p>In 2019 zijn de niet aanbestede inhuuractiviteiten van het IT personeel gecontinueerd. De verwachte omvang van deze inhuur over 2019 is naar schatting € 520.000. Deze inhuur is onrechtmatig en zal worden verwerkt in het rechtmatigheidsoordeel over de jaarrekening 2019.</p> <p>Middels deze managementletter geven wij een ‘early-warning’ af dat zeer waarschijnlijk in 2019 niet op alle onderdelen de Europese aanbestedingsrichtlijnen zijn nageleefd. De gemeente is inmiddels op basis van de opgestelde spendanalyse intern een nader onderzoek gestart inzake de rechtmatigheid voor vier andere dossiers. In aanvulling op dit onderzoek worden ook de lopende onderhoudscontracten beoordeeld. Wij zullen de deze analyse de komende periode met uw organisatie beoordelen en evalueren. Indien de totaal niet Europees aanbestede lasten onze goedkeuringstolerantie (lees materialiteit) overschrijden, zal dit gevolgen hebben voor de strekking van ons rechtmatigheidsoordeel bij de jaarrekening 2019</p>
<p>Hoofdstuk 4.5</p> <p><i>Het verhuurproces is belegd bij verschillende personen binnen de gemeente. Er is geen totaaloverzicht van de verhuurbare eenheden.</i></p>	Laag	<p>Verkrijg een centrale registratie van alle contracten en de verhuurcapaciteit</p>
<p>Hoofdstuk 4.6</p> <p><i>Fraude- en corruptierisico</i></p>	Middel	<p>Verwerk de beheersing van fraude- en corruptierisico’s in de planning- & control cyclus.</p>

Bevinding (verwijzing naar management-letter)	Prioriteit	Advies
<p>Hoofdstuk 4.7</p> <p><i>Bij de gemeente ligt de primaire verantwoordelijkheid voor budgetbeheersing bij de budgethouder en budgetbeheerders. Het risico bestaat dat door het 'parkeren' van mutaties op tussenrekeningen gedurende het jaar een onjuiste weergave is van het budget en begrotingswijzigingen niet tijdig worden gecommuniceerd.</i></p>	Middel	<p>Verwerk de beheersing van tussenrekeningen in de planning- & control cyclus.</p>
<p>Hoofdstuk 4.9</p> <p><i>De gemeente beschikt niet over een centrale registratie waarin alle subsidieaanvragen en – vaststellingen worden bijgehouden. Door het ontbreken van een centrale registratie heeft de gemeente geen totaaloverzicht van subsidieverstrekkingen en centrale aansturing voor het treffen van beheersingsmaatregelen.</i></p>	Middel	<p>Registreer centraal subsidieaanvragen, (beslis)termijnen, verstrekkingen en vaststelling.</p> <p>Leg werkinstructies vast ter borging van kennis en beheersing van de processen</p>

3. Administratieve organisatie en interne beheersing

3.1 Interne beheersing

De interne beheersing binnen de gemeente is georganiseerd langs de volgende lijnen:

1. Administratieve organisatie en interne beheersing (AO/IB) in de processen in de lijnorganisatie en IT-systemen.
2. (Verbijzonderde) Interne controle uitgevoerd door medewerkers van de gemeente.
3. Externe controle (accountant).

Voor Heemstede constateren wij, zoals eerder aangegeven, dat de administratieve organisatie en interne beheersing (AO/IB) in de processen in de lijnorganisatie en IT-systemen voldoet aan de daaraan te stellen eisen. Gegeven de aard en omvang van de gemeente is het logisch dat niet alle (theoretische) functiescheidingen en controles in de lijn (punt 1 van bovenstaande punten) binnen de gemeente aanwezig zijn. Dit betekent dat achteraf controles (punt 2) noodzakelijk zijn en ook daadwerkelijk door de organisatie voor de bedrijf kritische processen worden uitgevoerd. Deze controle verricht Heemstede binnen de (verbijzonderde) interne controle. Hierdoor borgt Heemstede dat de belangrijkste risico's die niet in de procesvoering zelf worden geborgd, middels een interne controle alsnog worden ondervangen.

3.2 Kwaliteit van de processen

In het kader van de controle van de jaarrekening controleren wij de opzet en het bestaan van de AO/IB van de processen die resulteren in posten in de jaarrekening. Onderstaand hebben wij ons totaalbeeld van de interne beheersing van de gemeente Heemstede per proces (voor zover gecontroleerd gedurende de interimcontrole) weergegeven.

Wij attenderen u daarbij op het feit dat dit beeld gebaseerd is op de beoordeling van de opzet en het bestaan van de beheersingsmaatregelen van de processen per heden. De beoordeling kan afwijken op het moment dat wij hebben beoordeeld of de beheersingsmaatregelen gedurende het gehele jaar hebben.

Leeswijzer bij de procesmonitor:

De effectiviteit van een proces wordt op basis van onze beroepsregels op 'goed' gekwalificeerd indien de interne beheersingsmaatregelen zodanig zijn ingedeeld dat de accountant hierop kan steunen bij zijn organisatiegerichte werkzaamheden. Op grond van de omvang van uw gemeente (en het overgrote deel van de gemeenten in Nederland) is dit op basis van de 'kosten-batenanalyse' niet mogelijk. **Een voldoende is voor uw gemeente derhalve een goed resultaat.**

Ten aanzien van onderstaande indeling geldt enige mate van subjectiviteit. Voor het bepalen van de effectiviteit hebben wij gekeken naar de opzet van het proces tot en met kunnen steunen op de beheersingsmaatregelen. Bij een ontoereikende opzet scoort het proces onvoldoende.

Voor de alle processen hebben wij geconstateerd dat een toereikende opzet aanwezig is, echter hebben wij bij het functioneren van het proces bevindingen geconstateerd waardoor deze naar de onderkant van een voldoende bewegen (o.a. afhankelijk van inhoud bevinding). Naarmate wij in een proces meer kunnen steunen op beheersingsmaatregelenmaatregelen gaan deze richting de bovenkant voldoende of bij een volledige beheersing naar goed.

Proces	Onvoldoende	Voldoende	Goed
Planning & Control Cyclus		<input checked="" type="checkbox"/>	
Fraude-, integriteit & corruptierisico's		<input checked="" type="checkbox"/>	
Financiële verslaggeving en administratie		<input checked="" type="checkbox"/>	
Inkopen inclusief betalingsverkeer		<input checked="" type="checkbox"/>	
Aanbestedingswetgeving		<input checked="" type="checkbox"/>	
Personeelsproces inclusief inhuur en WNT		<input checked="" type="checkbox"/>	
Sociaal domein		<input checked="" type="checkbox"/>	
Systeembeheer		<input checked="" type="checkbox"/>	
AVG		<input checked="" type="checkbox"/>	
Subsidieverstrekking		<input checked="" type="checkbox"/>	
Treasury		<input checked="" type="checkbox"/>	
Omgevingsvergunningen		<input checked="" type="checkbox"/>	
Verhuur		<input checked="" type="checkbox"/>	

Kwalificatie	Toelichting
Onvoldoende	Bij een niet toereikende opzet en ontbreken van mitigerende aanvullende verbijzonderde interne controle (VIC) maatregelen scoort het proces onvoldoende.
Voldoende	De opzet en het bestaan van de administratieve organisatie en interne beheersing hebben wij als voldoende beoordeeld indien: <ul style="list-style-type: none"> • Binnen het proces minimale functiescheiding aanwezig is en de interne beheersingsmaatregelen in opzet toereikend aanwezig zijn; • Indien wij geconstateerd hebben dat de hiervoor genoemde voorwaarden niet binnen het proces aanwezig zijn, maar de belangrijkste risico's binnen het proces worden gemitigeerd door aanvullende maatregelen, zoals verbijzonderde interne controlewerkzaamheden.
Goed	De effectiviteit van een proces wordt op basis van onze beroepsregels op 'goed' gekwalificeerd indien de interne beheersingsmaatregelen zodanig binnen de processen zijn ingeregeld dat de accountant hierop kan steunen voor zijn controlewerkzaamheden. De controleaanpak van de accountant kan in dit geval systeemgerichte ingestoken worden. Gegeven de aard en omvang van de gemeente zijn niet alle (theoretische) functiescheidingen en verwachte interne beheersingsmaatregelen binnen de processen van uw gemeente aanwezig. Dit betekent dat de kwalificatie 'goed' vanuit 'kosten-baten' oogpunt vrijwel niet haalbaar is voor een gemeente van uw omvang. Dit geldt overigens voor het overgrote deel van de gemeenten in Nederland.

3.3 Verbijzonderde interne controle

In de optimale situatie zijn interne controlehandelingen ingericht in de lijn van de processen. De manager is verantwoordelijk voor de lijn en treft middels de interne controlehandelingen beheersingsmaatregelen te beheersing van het proces. In de huidige situatie bij de gemeente Heemstede zijn de interne controlehandelingen belegd bij controlemedewerkers. Deze controlemedewerkers zitten niet in de lijn en voeren steekproefsgewijs interne controlehandelingen uit. Deze interne controlehandelingen worden achteraf uitgevoerd.

Verbijzonderde interne controlehandelingen zijn controlehandelingen waarbij de controlemedewerkers achteraf toetst of interne controlehandelingen in de lijn zijn uitgevoerd. Zoals gesteld voert op dit moment een controlemedewerker van de gemeente interne controlehandelingen uit. De controlemedewerker toets niet of interne controlehandelingen in de lijn zijn uitgevoerd. Dit betekent dat de controlemedewerker van de gemeente geen verbijzonderde interne controlehandelingen uitvoert, maar interne controlehandelingen.

De verwachting is dat vanaf 2021 het college een rechtmatigheidsverantwoording af moet leggen in de jaarrekening. De politieke aanspreekbaarheid voor het college inzake rechtmatigheid wordt hiermee vergroot. De inrichting van interne controlehandelingen in de lijn draagt bij aan de beheersing van processen door het management (inclusief college) en de beheersing van de uitkomsten in de rechtmatigheidsverantwoording. Daarnaast wordt het door interne controlehandelingen in de lijn te organiseren voor de controlemedewerkers buiten de lijn mogelijk om te toetsten op deze handelingen (verbijzonderde interne controle).

De uitkomsten van deze toetsen geeft het college de juiste tools om de rechtmatigheidsverantwoording af te kunnen leggen.

Wij adviseren u derhalve om de interne controlehandelingen in de lijn te organiseren en de uitkomsten van deze handelingen zichtbaar vast te laten leggen, waardoor achteraf verbijzonderde interne controle kan plaatsvinden op de uitgevoerde werkzaamheden.

3.4 Interne controleplan

Binnen de gemeente worden interne controlehandelingen uitgevoerd door een controlemedewerker buiten de lijn. Wij hebben kennis genomen van het interne controleplan (IC-plan) en de interne controle (IC) werkzaamheden. Wij adviseren het IC-plan risicogericht in te kleden. Door de risico's te koppelen aan de interne controlehandelingen is zichtbaar met welke doel de interne controlehandelingen worden uitgevoerd. Door het aantal interne controlehandelingen statistisch te onderbouwen middels een steekproef kan de gemeente concluderen of de verschaft informatie uit de interne controlehandelingen de exposure van de risico's hebben verlaagd naar een gewenst niveau.

Wij adviseren ter verbetering van de IC werkzaamheden om de volgende processen in de IC te betrekken:

- Memoriaalboekingen;
- Investerings en investeringskredieten;
- Voorzieningen;
- IT, waaronder inrichting van autorisaties in de applicaties; Prestatielevering WMO en Jeugdzorg.

4. Bevindingen interimcontrole 2019

4.1 Inleiding

De kwaliteit van de administratieve organisatie en de (verbijzonderde) interne controleonderzoeken vormen tezamen de twee belangrijkste onderdelen voor een optimaal interne beheersingssysteem. Hieronder gaan wij nader in op onze bevindingen inzake de interimcontrole 2019. In bijlage 1 van deze managementletter is de status van de openstaande bevindingen uit het voorgaande jaar opgenomen.

Overeenkomstig het merendeel van gemeenten liggen de verantwoordelijkheden voor de uitvoering en beheersing van interne processen in de organisatie zelf (c.q. in de lijn). Bij de uitvoering van onze werkzaamheden hebben wij overeenkomstig onze opdracht een focus op de financiële uitkomsten van de processen zelf. Bij de uitvoering van onze werkzaamheden, maar ook bij de implementatie van onze bevindingen wordt van nature direct een link gelegd met de ondersteunende afdeling Financiën en ondersteunende organisatie Stichting RIJK.

Belangrijk hierbij is dat deze ondersteunende afdeling / organisatie dienen ter ondersteuning. De uiteindelijke verantwoordelijkheid voor een goede beheersing van de processen blijft in de lijn bij de manager liggen. De organisatie zelf moet er derhalve voor zorgen dat zij het proces in control hebben.

4.2 Geautomatiseerde gegevensverwerking

4.2.1 Outsourcing (continuïteitsmanagement en informatiebeveiliging)

In 2019 heeft de gemeente een aanbestedingstraject doorlopen voor de outsourcen van een groot deel van de IT-beheeractiviteiten. Het beheer van de database wordt geoutsourcet naar een externe partij. Door deze outsourcing is het noodzakelijk dat een datamigratie plaatsvindt van de servers van de gemeente naar de server van de externe partij.

Uit de door ons gevoerde gesprekken bij de interimcontrole (eerste helft oktober 2019) hebben wij vastgesteld dat onderstaande punten nog niet uitgewerkt en afgerond zijn:

- Opstellen van een testplan inzake de waarborging van de continuïteit en betrouwbaarheid van de geautomatiseerde omgeving. Wij adviseren om na datamigratie de servers van de gemeente tijdelijk te blijven onderhouden totdat uit de testrapporten blijkt dat de datamigratie voor alle applicaties succesvol is geweest.
- Opstellen van een plan van aanpak ten behoeve van de interne beheersing van dit traject. Wij adviseren om hierbij onder andere aandacht te geven aan de volgende punten:
 - Informatielandschap van de gemeente, waarin een volledig overzicht is opgenomen van welke systemen, netwerken en databases gebruik wordt gemaakt.
 - Toekennen van verantwoordelijkheden binnen de gemeente inzake het toezicht houden op de activiteiten van de serviceorganisatie aan wie het systeembeheer is uitbesteed.
- Opstellen van een plan inzake het verwijderen van de gegevens van de huidige servers na afronding van een succesvolle datamigratie. Na een succesvol uitgevoerde datamigratie zullen de servers van de gemeente niet meer worden gebruikt. Het is noodzakelijk dat voorafgaand aan het vervreemden van de servers van de gemeente een plan wordt opgesteld en uitgevoerd om de gegevens van de servers te verwijderen.

4.2.2 General IT controls in de planning & control cyclus

De gemeente heeft een controleplan opgesteld ter beheersing van de processen in de administratieve organisatie. De rol van informatiesystemen wordt binnen organisaties steeds groter. Het systeem- en applicatiebeheer is ‘de spin in het web’ voor de beheersing van een proces. De outsourcing van het IT-beheer vraagt een andere aanpak van de beheersing van general IT controls door de gemeente.

Advies: Het is noodzakelijk dat de gemeente anticipeert op de veranderingen in het proces van systeembeheer en de processen zodanig inricht teneinde inzicht te blijven houden over de effectiviteit van de general IT controls.

4.3 Schattingen

De jaarstukken van de gemeente zijn onderhevig aan verschillende posten met schattingselementen. De belangrijkste posten in de balans van de gemeente zijn de ‘voorzieningen ter egalisatie van kosten’. Schattingsposten zijn gevoelig, aangezien een kleine aanpassing in een veronderstelling van een schattingselement kan leiden tot een groot verschil in omvang van een jaarrekeningpost. De beheersing van schattingselementen is een proces dat bestaat uit preventieve maatregelen, zoals het bepalen van veronderstellingen en het toetsen van gemaakte schattingen uit voorgaande periode met gerealiseerde uitkomsten en repressieve maatregelen. Een goede beheersing van de schattingselementen gedurende het boekjaar zorgt voor een nauwkeurige inschatting van de baten en lasten in de tussentijdse financiële rapportages. Hierbij kan onder andere gedacht worden aan het periodiek gedurende het jaar (bij het opstellen van de P&C-rapportages) toetsen van de schattingselementen aan de werkelijke uitkomsten voor de ‘voorzieningen ter egalisatie van kosten’.

Advies: Wij adviseren om de beheersing van schattingselementen voor de ‘voorzieningen ter egalisatie van kosten’ onderdeel te maken van de planning- & control cyclus en gedurende het jaar interne controlewerkzaamheden hierop te verrichten.

4.4 Aanbestedingsbeleid

4.4.1 Preventieve maatregelen naleving aanbestedingswetgeving

De gemeente Heemstede maakt gebruik van expertise van Stichting Rijk voor de begeleiding bij een aanbestedingstraject. Stichting Rijk neemt voorafgaand aan het begrotingsjaar een interview af met de budgetbeheerders. Op basis van de informatie voortvloeiend uit deze interviews stelt Stichting Rijk een inkoopjaarplan op.

Het is de verantwoordelijkheid van de budgethouder en budgetbeheerder om nieuwe aanbestedingstrajecten tijdig te signaleren en te communiceren naar Stichting Rijk, zodat deze worden verwerkt in het inkoopjaarplan. Budgetbeheerders hebben niet het totaaloverzicht van inkopen van de gemeente, maar alleen van hun eigen budget. Doordat geen totaaloverzicht is van de inkopen van de gemeente gedurende het jaar loopt de gemeente het risico dat verschillende budgetbeheerders bij dezelfde leverancier inkopen en onrechtmatige bestedingen worden gedaan. De aanwezigheid van een centraal contractenregister zou dit kunnen voorkomen.

Wij adviseren om op basis van een contractenregister inzicht te verkrijgen in potentiële aanbestedingstraject en controle op potentiële aanbestedingstrajecten te verwerken in de planning- & control cyclus. Daarnaast adviseren wij u te overwegen om een centrale inkooporganisatie in te stellen.

4.4.2 Early-warning niet naleving van aanbestedingswetgeving in 2019

In 2017 is de gemeente Heemstede een contract aangegaan voor de inhuur van IT-personeel. Wij hebben bij de controle van de jaarrekening vastgesteld dat dit contract onterecht niet Europees is aanbesteed. Destijds was het de verwachting dat het contract ultimo 2018 beëindigd zou zijn. Derhalve is deze onrechtmatigheid voor de jaren 2017 en 2018 meegenomen in het rechtmatigheidsoordeel over de jaarstukken 2017. In 2019 zijn de inhuuractiviteiten van het IT personeel echter gecontinueerd. De verwachte omvang van deze inhuur over 2019 is naar schatting € 520.000. Deze inhuur is onrechtmatig en zal worden verwerkt in het rechtmatigheidsoordeel over de jaarrekening 2019.

Middels deze managementletter geven wij een ‘early-warning’ af dat zeer waarschijnlijk in 2019 niet op alle onderdelen de Europese aanbestedingsrichtlijnen zijn nageleefd. De gemeente is inmiddels op basis van de opgestelde spendanalyse intern een nader onderzoek gestart inzake de rechtmatigheid voor vier andere dossiers. In aanvulling op dit onderzoek worden ook de lopende onderhoudscontracten beoordeeld. Wij zullen de deze analyse de komende periode met uw organisatie beoordelen en evalueren. Indien de totaal niet Europees aanbestede lasten onze goedkeuringstolerantie (lees materialiteit) overschrijden, zal dit gevolgen hebben voor de strekking van ons rechtmatigheidsoordeel bij de jaarrekening 2019.

4.5 Verhuur

Het verhuurproces is belegd bij verschillende personen binnen de gemeente. Er is geen totaaloverzicht van de verhuurbare eenheden.

Advies: Wij adviseren een centrale registratie van de verhuurbare eenheden bij te houden middels een contract- of capaciteitsregister.

4.6 Op fraude en corruptie gerichte controlemaatregelen

Bij de uitvoering van onze interimcontrole hebben wij vastgesteld dat de VIC heeft vastgesteld dat een medewerker een factuur heeft geautoriseerd in plaats van de betrokken budgetbeheerder. Hierbij heeft de medewerker handmatig ingegrepen waardoor de factuur welke was aangeboden aan de budgetbeheerder, onterecht is geautoriseerd door de medewerker. Deze handeling is in beginsel een voorbeeld van management override, wat altijd een frauderisico is voor de gemeente.

Uit onze aanvullende werkzaamheden op deze constatering hebben wij vastgesteld dat aan deze handeling geen fraude ten grondslag heeft gelegen en dat deze actie is gedaan door de medewerker om de factuur tijdig te kunnen betalen. Wel zullen wij op basis van deze constatering bij de eindejaarscontrole een integrale analyse doen op inkopen welke niet zijn geautoriseerd door budgetbeheerder.

Het is voor de interne beheersing van belang om op bestuurlijk niveau, op reguliere basis en op een gestructureerde manier aandacht te besteden aan het onderwerp fraude en corruptie. Een periodieke fraude- en corruptierisicoanalyse en evaluatie van de risicostrategie (waaronder de acceptatie van restrisico's) en risicorespons (waaronder de effectiviteit van beheersingsmaatregelen) met betrekking tot fraude- en corruptierisico's maken hier deel van uit. Op dit moment is de rapportering over de fraude- en corruptierisico's nog niet betrokken in de planning- & controlcyclus.

Advies: Het is noodzakelijk dat rapportering over fraude- en corruptierisico wordt betrokken in de planning- & controlcyclus.

4.7 Tussenrekeningen

In de administratie zijn in de balans tussenrekeningen opgenomen ten behoeve van een juiste afgrenzing van lasten en opbrengsten. Deze afgrenzing is noodzakelijk voor een juiste weergave van de budgetbesteding. Bij de gemeente ligt de primaire verantwoordelijkheid voor budgetbeheersing bij de budgethouder en budgetbeheerders. Het risico bestaat dat door het 'parkeren' van mutaties op tussenrekeningen gedurende het jaar een onjuiste weergave is van het budget en begrotingswijzigingen niet tijdig worden gecommuniceerd.

Advies: Het is noodzakelijk dat controlemaatregelen worden getroffen op het periodiek monitoren van saldi op tussenrekeningen.

4.8 Subsidieverstrekingen

4.8.1 Centrale registratie

Wij hebben geconstateerd dat binnen de gemeente aandacht is voor verbeteringen binnen het subsidieverstrekking proces.

De gemeente beschikt niet over een centrale registratie waarin alle subsidieaanvragen en – vaststellingen worden bijgehouden. Door het ontbreken van een centrale registratie heeft de gemeente geen totaaloverzicht van subsidieverstrekingen en centrale aansturing voor het treffen van beheersingsmaatregelen.

Advies: Wij adviseren voor alle subsidieaanvragen een centrale registratie bij te houden waaruit blijkt welke aanvragen zijn ingediend, binnen welke termijn deze moeten worden afgehandeld, of subsidie wordt verstrekt, binnen welke termijn de subsidie moet worden vastgesteld en of de subsidie is vastgesteld.

4.8.2 Stel werkinstructies op

De gemeente werkt met een vaste groep medewerkers met jarenlange ervaring bij de gemeente. Hierdoor is de behoefte aan het opstellen van werkinstructies klein. Bij personeelswijzigingen loopt de gemeente het risico op verlies van kennis en procesbeheersing.

Advies: Wij adviseren werkinstructies op te stellen ter borging van de kennis over en beheersing van het proces.

5. Actualiteiten en aandachtspunten jaarrekeningcontrole 2019

5.1 Kaderstelling accountantscontrole (controleprotocol en normenkader)

Wij voeren onze controle onder ander uit op basis van het door de gemeente vastgestelde (accountants)controleprotocol en het normenkader. De gemeente heeft een controleprotocol voor de accountantscontrole 2016-2018 vastgesteld en een normenkader voor 2018. Het controleprotocol en normenkader voor 2019 moet nog worden opgesteld en vastgesteld. Wij wijzen u erop om deze documenten tijdig vast te stellen, zodat wij tijdig de reikwijdte van onze controle en controlewerkzaamheden kunnen bepalen.

5.2 Rechtmatigheidsverantwoording door het college

Recent is er overleg geweest tussen de VNG, de commissie Bado, de commissie BBV en de NBA over de rechtmatigheidsverantwoording die het college vanaf 2021 dient te gaan verstrekken. Concreet is besproken dat de rechtmatigheidsverantwoording van het college onderdeel gaat uitmaken van de jaarrekening en daarmee tevens valt onder de controleverklaring die de accountant bij de jaarrekening verstrekt. Tevens is de voorkeur geuit om een ruimer foutenpercentage en rapporteringstolerantie toe te laten dan de 1% die de accountant tot nu toe moet hanteren bij zijn rechtmatigheidscontrole. Dat laatste betekent dat de gemeente de controle op rechtmatigheid met minder diepgang zou mogen uitvoeren.

Wij merken op dat de formele besluitvorming en benodigde wetswijzigingen nog niet zijn doorgevoerd en dat bovenstaande uitkomst mogelijk nog kan wijzigen. Desalniettemin adviseren wij u al spoedig de (verbijzonderde) interne controleplannen te gaan voorbereiden die de gemeente zal gaan uitvoeren om het college over 2021 in staat te stellen een rechtmatigheidsverantwoording te kunnen verstrekken. Vragen die bij de voorbereiding aan bod komen zijn onder andere welke controles zullen zichtbaar worden vastgelegd, wie zal de controles uitvoeren, hoe zal (tussentijds) worden gerapporteerd over de bevindingen, afwijkingen en mogelijk te nemen reparatieacties, hoe zal de communicatie met de raad hierover plaatsvinden.

Naast bovenstaande vragen die de gemeente moet gaan beantwoorden, hebben de accountants nog vragen welke diepgang zij moeten gaan hanteren bij de controle op de rechtmatigheidsverantwoording van het college. Mogen zij voor hun controleverklaring steunen op de controles die de gemeente zelf heeft uitgevoerd op de rechtmatigheid, indien de gemeente een hoger foutenpercentage en rapporteringstolerantie voor haar verantwoording mag hanteren dan de accountant.

Hoewel nu nog diverse onduidelijkheden moeten worden opgelost, gaan wij er van uit dat de rechtmatigheidsverantwoording van het college inderdaad vanaf 2021 zijn intrede doet. Het is zaak dat u zich daar tijdig op gaat voorbereiden, aangezien het voor de gemeente betekent dat vanaf begin 2021 de eigen interne controles moeten worden uitgevoerd.

5.3 Nieuw wettelijk normenkader informatiebeveiliging 2020 (BIO)

In 2020 geldt voor de gehele Nederlandse overheid één uniform normenkader voor informatiebeveiliging, de Baseline Informatiebeveiliging Overheid (BIO). Voorheen hanteerden gemeenten de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG) als normenkader. Het jaar 2019 staat in het teken van de overgang van BIG naar BIO.

De nieuwe baseline is het nieuwe normenkader voor alle overheden. Gemeenten hanteren vanaf 1 januari 2020 samen met de rijksoverheid, de waterschappen en de provincies dit uniforme normenkader voor informatiebeveiliging. De BIO bevat een normenkader met betrekking tot de sturing op informatiebeveiliging. De BIO bevat ook maatregelen ten aanzien van privacybescherming. De BIO is van toepassing voor alle verwerkingen van persoonsgegevens die onder de verantwoordelijkheid van gemeenten uitgevoerd worden. De BIO is terug te vinden op de website van de Informatiebeveiligingsdienst voor gemeenten (<https://www.informatiebeveiligingsdienst.nl>) samen met handreikingen voor het inrichten van specifieke informatiebeveiligingsmaatregelen. Wij verwijzen naar de website voor concrete stappen die de gemeente kan nemen bij de overgang naar BIO.

Het blijven voldoen en up-to-date houden van eigen verordeningen is een belangrijk aspect van de rechtmatigheidscontrole. De gemeente Heemstede heeft hier voldoende aandacht voor. De verordeningen van de gemeente hieromtrent zijn op orde. De gemeente stelt daarnaast jaarlijks in januari het normenkader vast. In dit normenkader wordt naar (sub)activiteit uitgesplitst welke wet- en regelgeving van toepassing is (juistheid en volledigheid).

Wij vertrouwen erop u met deze managementletter van dienst te zijn en zijn graag bereid u nadere toelichting te verstrekken.

Met vriendelijke groet,

Astrium Overheidsaccountants B.V.

Was getekend,

Drs. R.A.D. Knoester RA

Verspreidingskring en disclaimer gebruik managementletter

Deze managementletter is alleen bestemd voor het college en mag niet in zijn geheel of gedeeltelijk worden verstrekt of aangehaald zonder onze schriftelijke toestemming vooraf. Er wordt geen verantwoordelijkheid aan een derde partij geaccepteerd, omdat deze managementletter daar niet voor opgesteld en bedoeld is. Dientengevolge nemen wij geen enkele verplichting of plicht van zorg aan ieder ander persoon aan wie deze managementletter getoond of in zijn handen komt op ons. De in deze managementletter aan de orde gestelde onderwerpen zijn door ons geconstateerd gedurende onze controleopdracht waarvan wij van mening zijn dat zij uw aandacht behoeven. Het is geen allesomvattende managementletter van alle geconstateerde zaken en in het bijzonder kunnen wij niet verantwoordelijk worden gesteld voor het rapporteren van alle bedrijfsrisico's of tekortkomingen in het systeem van interne beheersing. Elke conclusie, opinie of opmerking in deze managementletter is verstrekt in de context van onze controleverklaring over de jaarrekening als geheel, welke zal worden verstrekt in onze controleverklaring.

Evenzo geldt dat de opmerkingen, bevindingen en aanbevelingen met betrekking tot het systeem van interne beheersing niet gelezen dienen te worden als een afzonderlijke opinie van het systeem van interne beheersing en haar werking.

Bijlage 1: Follow-up bevindingen voorgaand jaar

Verwijzing management-letter	Advies	Reactie college	Prioriteit	Status
<u>3.3 General IT controls</u>	<p>Wij adviseren de interne controle afdeling om periodiek de effectiviteit van de general IT controls te toetsen. De interne controleafdeling kan dit doen middels afstemming tussen de GRIT, applicatiebeheerder en afdeling P&O over:</p> <ul style="list-style-type: none"> • Personeelsmutaties (functiewijzigingen, in- en uitdienst) -> hebben bijvoorbeeld de juiste personen, met de juiste rechten toegang tot applicaties; • Nieuwe releases in de applicatie -> zijn bijvoorbeeld alle nieuwe releases geïmplementeerd; • Back-up resultaten -> zijn backups gemaakt overeenkomstig de geldende voorwaarden binnen de gemeente. 	<p><i>Het uitgangspunt is dat onze (financiële) informatiesystemen (met name het financieel systeem, het uitkeringsstelsel en het salarissysteem) betrouwbare informatie genereren. Om dit te waarborgen zijn zogenoemde general IT controls noodzakelijk. Een belangrijk IT control is een onderbouwde toekenning (van verschillende rollen) en beheer van de autorisaties. De primaire verantwoordelijkheid hiervoor ligt bij het lijnmanagement. De interne controle afdeling toetst dit. Voor de eindcontrole van de jaarrekening 2018 wordt een nulmeting gemaakt van de stand van zaken m.b.t. de onderbouwing en beheer van de autorisaties en worden zo nodig verbeterpunten geformuleerd.</i></p>	Hoog	<p>Deels gereed:</p> <p>Processen in het systeembeheer en functioneel beheer zijn ingericht met controlehandelingen wat betreft change management en continuïteitsmanagement. Deze interne controlehandelingen worden niet getoetst in de verbijzonderde interne controle.</p>
4.3.1 Applicatiebeheerder Civision Samenleving (2018)	<p>Formaliseer overeenkomstig de procedures bij de Gemeenschappelijke Regeling Informatietechnologie (Hierna: GRIT) een change management procedure. Dit houdt in dat het uitvoeren van changes in de database worden getest in een testomgeving en door meerdere IT-personeel worden geaccordeerd voordat de change in productie wordt genomen.</p>	<p><i>Wij onderkennen het risico en zullen eventuele changes in de database eerst testen, laten accorderen en vastleggen alvorens wij de changes in productie nemen.</i></p>	Hoog	<p>Gereed</p> <p>Proces is geformaliseerd en wordt vastgelegd in Topdesk</p>

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
4.3.2. Outsourcing (2018)	<p>Stel ten behoeve van de interne beheersing van de outsourcing van systeembeheer voorafgaand een plan van aanpak op, waarin aandacht onder andere aandacht is voor onderstaande punten:</p> <ul style="list-style-type: none"> • Informatielandschap van de gemeente, waarin een volledig overzicht is opgenomen van welke systemen, netwerken en databases gebruik wordt gemaakt. <p>Toekennen van verantwoordelijkheden binnen de gemeente inzake het toezicht houden op de activiteiten van de serviceorganisatie aan wie het systeembeheer is uitbesteed.</p>	<p><i>De Europese aanbesteding is in maart 2019 in een afrondende fase beland. Op 4 maart zijn er drie rechtsgeldige inschrijvingen ontvangen. Deze worden o.b.v. vooraf gedefinieerde gunningscriteria beoordeeld door een beoordelingsteam van 4 personen. Op 20 maart worden de vier beoordelingen afgestemd in een concensusmeeting. Vervolgens wordt het gunningsbesluit op 2 april vastgesteld door het college van Heemstede (centrumgemeente) en voor akkoord vastgesteld in het college van Bloemendaal. Daarna gaat deze besluiten ook ter kennisname aan de Raad of ter besluitvorming als blijkt dat sprake is van structurele budgetverhoging. Dit kan pas worden bepaald als begin maart de offertemodellen van de drie partijen zijn beoordeeld.</i></p>	Midden	<p>Deels gereed:</p> <p>De gemeente heeft het informatielandschap bepaald en de IT-infrastructuur gedeeld met de nieuwe systeembeheerder. De nieuwe systeembeheerder is de datamigratie aan het voorbereiden. De inrichting van verantwoordelijkheden binnen de gemeente vindt plaats na de datamigratie.</p>
4.4 Contractmanagement (2018)	<p>Organiseer het contractbeheer centraal en voer het uiteindelijke contractmanagement (proces afsluiten contracten etc.) uit in de lijn, waarmee uiteindelijk een totaaloverzicht gerealiseerd kan worden.</p>	<p><i>Het contractbeheer wordt geïmplementeerd in het zaaksysteem Mozard. Het proces is ontworpen zodat contracten vanuit de lijn kunnen worden bewaakt. De lijn wordt tijdig actief gesignaleerd indien een contract gaat verlopen. Dit proces is klaar voor gebruik. Vanaf 1 april 2019 wordt Mozard door de hele organisatie in gebruik genomen. Vanaf dat moment worden ook alle nieuwe contracten in Mozard vastgelegd. Er is formatie beschikbaar in de vorm van een contractbeheerder die de lijn kan signaleren, ondersteunen en adviseren.</i></p>	Hoog	<p>Deels gereed:</p> <p>In het zaaksysteem is het contractbeheer geïmplementeerd. In het zaaksysteem zijn nog niet alle contracten opgenomen. Hierdoor is het contractbeheer nog niet van een kwaliteit dat output een volledig beeld geeft van de contractverplichtingen van de gemeente.</p>

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
4.4 Contract-management (2018) vervolg		<i>Tegelijkertijd vindt een update plaats van de inventarisatie van de huidige contracten. Deze worden ook in mozaïek vastgelegd indien ze doen aan een aantal criteria met betrekking tot omvang en duur.</i>		
4.5 Memoriaalboekingen (correctieboekingen) (2018)	Wij adviseren om voor memoriaalboeking autorisaties in te richten in Key2 Financiën, opdat wordt afgedwongen dat bevoegde functionarissen de memoriaalboekingen autoriseren.	<i>In eerste instantie zijn er alleen bevoegden binnen het team Financieel beheer. De overige gebruikers hebben geen mutatierechten op memoriaalboekingen. Correctieboekingen vinden plaats binnen het financiële pakket. De opdracht voor de boeking kan wel afkomstig zijn van een andere afdeling. In verband met de overgang van een aantal processen van Financieel beleid naar Financieel beheer is een aantal memoriaalboekingen nog door een financieel beleidsmedewerker gedaan. Vanaf 1 januari 2019 worden die rechten bij de financieel beleidsmedewerkers weggehaald.</i> <i>Op 1 financieel beleidsmedewerker na zijn de rechten weggehaald. Een medewerker heeft deze rechten voor dit jaarrekeningtraject nog behouden onder andere in verband met het verwerken van btw-posten. Deze medewerker heeft daarnaast incidenteel nog enkele memorialen geboekt.</i>	Midden	Deels gereed Administratieve organisatie is ingericht dat alleen bevoegd functionarissen memoriaalboeking kunnen verwerken. De inrichting van processen dwingt nog geen dubbele autorisatie af op memoriaalboekingen.

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
4.6 Omgevingsvergunningen (2018)	Wij adviseren om periodiek (per kwartaal) de werkzaamheden van de GBKZ te monitoren en aansluiting te maken met de opgelegde leges.	<i>Het proces begint zoals aangegeven bij de afdeling Bouw en woningtoezicht (BWT) die ook eigenaar van het proces is. De afdeling BWT gaat in samenwerking met de afdeling GBKZ en het team Financieel beheer werken aan een vernieuwde procesbeschrijving zodat ze onderling weten op welke momenten er verwachtingen naar elkaar zijn.</i>	Midden	Gereed De gemeente monitort tussentijds opgelegde aanslagen en aansluitingen met GBKZ.
4.7 Jaarrekening (2018)	Wij adviseren om jaarlijks te evalueren of de voordelen van het opstellen van de jaarrekening in Excel nog opwegen het opstellen van de jaarrekening in een jaarverslaggevingspakket.	<i>De jaarrekening wordt opgesteld in het financieel systeem. De jaarstukken ten behoeve van de raad worden opgesteld in Excel. De cijfers hiervoor komen uit het financieel systeem. Het alternatief is dat een nieuw softwarepakket wordt aangeschaft om de jaarstukken op te stellen. Dit brengt kosten met zich mee. We onderzoeken op welke wijze het proces op beste wijze kan worden ondersteund.</i>	Laag	In ontwikkeling De gemeente inventariseert op welke wijze het proces op beste wijze kan worden ondersteund.
<i>Audit commissie Vraag 1: Bij de controle 2017 zijn er fouten geconstateerd ten aanzien van de Europese aanbestedingen. Is het inkoopproces en de daarbij behorende procedures voldoende ingericht ter voorkoming van onrechtmatigheden?</i>	Wij adviseren u om de workshop periodiek te organiseren en om de te onderzoeken of in Key2 Financiën de ontwikkelde toolkit opgenomen en verplicht afgedwongen kan worden.”	<i>Periodiek zullen, in navolging van de geslaagde workshop van 3 oktober 2018., samen met het regionaal inkoopbureau stichting Rijk workshops inkopen & aanbesteden worden georganiseerd. De toolkit inkopen & aanbesteden is voor iedere medewerker beschikbaar op het intranet en op het gebruik hiervan zal door het lijnmanagement actief worden gestuurd.</i>	Hoog	Deels gereed De gemeente heeft preventieve beheersingsmaatregelen getroffen door een voorafgaand aan het begrotingsjaar een inkoopplan te maken voor aanbestedingstrajecten. De gemeente heeft met presentaties over het aanbestedingsbeleid aan budgethouders bewustwording bij hen gecreëerd. Gedurende het begrotingsjaar kunnen inkopen worden gedaan die niet zijn opgenomen in het inkoopplan. Middels het bijhouden van een contractenregister heeft Stichting Rijk preventief inzichtelijk welke aanbestedingstrajecten in de toekomst gaan lopen.

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
		<p><i>Naar aanleiding van de eindrapportage Interne Controle 2018, waarbij bevindingen door de Verbijzonderde Interne Controle zijn geconstateerd bij de toetsing van aanbestedingen, die op 27 februari 2019 is besproken in het DO (Directieoverleg) wordt in maart/april 2019 voor de leidinggevenden opnieuw een bijeenkomst inkopen & aanbesteden georganiseerd in samenwerking met het inkoopbureau Stichting RIJK. Inkopen & aanbesteden blijft een onderwerp dat continue aandacht verdient.</i></p>		
<p>Audit commissie Vraag 2 Inkopen: prestatielevering (2018)</p> <p><i>Heeft de gemeente voldoende waarborgen getroffen ter afdekking van het risico op betaling en verwerking van valse facturen?</i></p>	<p>Wij adviseren om een risicoscan uit te voeren op welke kosten en investeringen prestatielevering een issue is c.q. kan zijn. Juist ten aanzien van deze posten is het risico op verwerking / betaling van valse facturen groter.”</p>	<p><i>In de verordening is aangegeven dat de budgethouder en (deel)budgetbeheerder op basis van een mandaat binnen de Regeling budgetbeheer verantwoording is verschuldigd aan het College van Burgemeester en Wethouders voor alle verplichtingen die samenhangen met en/of voortvloeien uit het beheer van de budgetten die onder zijn/haar verantwoording vallen conform het organogram. Hieronder vallen zowel kwalitatieve (doelstellingen, prestaties etc.) als de kwantitatieve gegevens (middelen, dekkingspercentages, kengetallen etc.).</i></p>		<p>Gereed</p> <p>De controle op prestatielevering wordt in overeenstemming met de regeling budgetbeheer uitgevoerd door de budgetbeheerders.</p>

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
Bevinding 7 (2017)	De accountant adviseert om de functiescheiding in Civision Samenleving zoals buiten de applicatie ook binnen de applicatie in te richten zodat een juiste verwerking van mutaties is gewaarborgd.	<p><i>De constatering dat aan functionarissen meerdere rollen zijn toegewezen wordt onderkend. Dit betekent echter nog niet altijd dat daarmee de functiescheiding wordt doorbroken. Daar waar dat wel het geval is zullen wij in 2018 op de kritieke processen (crediteuren stamgegevens/betalingen) maatregelen doorvoeren die de functiescheiding waarborgen.</i></p> <p><i>Reactie 2019</i></p> <p><i>De functiescheiding is doorgevoerd in Civision. Vanaf heden gebruiken wij de nieuwe indeling van bevoegdheden.</i></p>	Midden	Gereed. Per functie zijn de rollen en bevoegdheden gedefinieerd. De aanpassingen zijn in Civision verwerkt.
Bevinding IT 3 (2017)	De accountant adviseert: <ul style="list-style-type: none"> a) De aanvragen tot toekennen en intrekken van rechten in applicaties te registreren (bv via Topdesk); b) Een normpositie met gewenste functiescheiding en rechten op functieniveau per applicatie op te stellen; c) Het aantal applicatiebeheerders per applicatie te herzien en te beperken tot zo weinig mogelijk gebruikers die deze rechten hebben en buiten het primaire proces vallen. d) Het aantal generieke accountants te minimaliseren; e) Het wachtwoordbeleid van het financieel systeem (Key2Financiën) te versterken; f) Een periodieke controle (minimaal jaarlijks) van de gebruikers en de autorisaties uit te voeren. 	<p><i>Wij onderschrijven het belang van de door de accountant genoemde punten en daarmee het belang het functioneel applicatiebeheer in onze organisatie verder te professionaliseren. Een concrete maatregel is dat begin 2018 de werving start voor de invulling van een (nieuwe) functie voor functioneel applicatiebeheer van het financieel systeem. In de begroting zijn hiervoor gelden gereserveerd. Conform de uitgangspunten van de accountant wordt periodiek gerapporteerd over de follow-up van de genoemde bevindingen.</i></p>		Gereed <ul style="list-style-type: none"> a) Applicatiebeheerders zijn toegevoegd aan Topdesk en ontvangen bericht van personeelswijzigingen (<u>gereed</u>). b) De gemeente heeft een normpositie gedefinieerd voor de betreffende functiescheiding in de applicaties Key Financiën en Beaufort (<u>gereed</u>). c) Het aantal applicatiebeheerders heeft de gemeente beperkt tot 1 à 2 (<u>gereed</u>). d) Er is geen sprake van generieke gebruikers, omdat in de applicaties rollen zijn toegekend aan de gebruikers (<u>gereed</u>). e) Het wachtwoordbeleid steunt met name op het wachtwoordbeleid voor toegang tot het netwerk. Dit wachtwoordbeleid biedt voldoende beveiliging (<u>gereed</u>). f) Vier keer per jaar vindt een controle plaats op de gebruikers die toegang hebben tot de applicaties (<u>gereed</u>).

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
Bevinding IT 4	<p>De accountant adviseert:</p> <p>a) De wijzigingen en updates van applicaties in de toekomst in Topdesk te registreren. Hierbij dienen de stappen van testen, ontwikkeling, acceptatie en tussenliggende activiteiten zichtbaar, volgens standaardprotocol en traceerbaar te zijn;</p> <p>b) Voor de toekomst het advies om wijzigingen en updates van de diverse applicaties middels Topdesk zichtbaar af te wikkelen. Dit uit te voeren door de CISO (Chief Information Security Officer/manager informatiebeveiliging).</p>	<p><i>Sinds 2018 is wijzigingsmanagement ingevoerd binnen GRIT. In eerste instantie heeft GRIT wijzigingsmanagement toegepast met betrekking tot alle IT-infrastructurele wijzigingen. Doelstelling is dat dit proces organisatiebreed wordt toegepast. Om dit te concretiseren is er een Request For Change (RFC) formulier gemaakt zodat wijzigingen vanuit de organisatie goed worden gedocumenteerd. Er zal tevens een Change Advisory Board (CAB) worden samengesteld. Het CAB zal verantwoordelijk zijn voor het prioriteren van alle binnengekomen wijzigingsverzoeken (RFC's). Tevens zal het CAB een advies geven ten aanzien van haalbaarheid van de RFC's. De implementatie van het Change proces zal geleidelijk worden ingevoerd binnen de gemeente Heemstede en Bloemendaal en zal uiterlijk 1 april 2019 volledig operationeel moeten zijn. Het Change proces zal volledig via Topdesk lopen.</i></p>		<p>Gereed Wijzigingen en updates in applicaties worden geregistreerd in Topdesk. De applicaties hebben een test- en productieomgeving waarin de functioneel beheerders de wijzigingen kunnen testen.</p>

Verwijzing managementletter	Advies	Reactie college	Prioriteit	Status
Bevinding IT 5	<p>De accountant adviseert:</p> <p>a) Testprotocollen te ontwikkelen en uitkomsten hiervan te documenteren en zichtbaar opvolging te geven aan bevindingen. Dit kan eveneens zichtbaar middels Topdesk (bijvoorbeeld afwikkeling van errors);</p> <p>b) Het opstellen en implementeren van een noodplan bij calamiteiten en betrokken medewerkers hierover te informeren.</p>	<p><i>Het proces van een Disaster & Recovery test (DR) is nog niet gedocumenteerd. Het proces beschrijft de handelingen die nodig zijn om bij calamiteiten de bedrijfscontinuïteit te kunnen borgen. In april 2018 zijn de laatste stappen uitgevoerd om het netwerk van de gemeente Bloemendaal en Heemstede te migreren naar het GRIT netwerk. Bij deze migratie is er rekening gehouden met een mogelijkheid om bij eventuele calamiteiten de primaire processen te kunnen blijven uitvoeren. Tijdens de migratie is dit getest. De DR-test beschrijving zal in januari 2019 worden opgeleverd.</i></p>		<p>Gereed Het proces van Disaster & Recovery is en gedocumenteerd.</p>