Memo

Onderwerp
Managementletter Interim Controle 2017

Datum
9 april 2018

Aan
Gemeenteraad

Van
College/T.J.M. Groot

Doel
Informeren

Geachte leden van de raad,

Deze memo dient als begeleidend schrijven bij de managementletter die de accountant heeft opgeleverd. De managementletter is gebaseerd op de interim-controle van de accountant die in de tweede helft van 2017 is uitgevoerd.

De interim controle van de accountant is onderdeel van de jaarrekeningcontrole 2017. Tijdens de interim-controle gaat de accountant na in hoeverre hij op de interne organisatie rondom bedrijfsvoering en relevante bedrijfsprocessen kan steunen. In dat verband heeft de accountant de opzet en het bestaan van de administratieve organisatie op een aantal punten onderzocht.

In het dashboard op pagina 4 van bijgaande managementletter zijn de belangrijkste bevindingen opgenomen. Wij herkennen deze bevindingen en zien hierin grond voor de verdere doorontwikkeling van onze organisatie.

Omdat bevindingen van accountant naar hun aard kritisch zijn menen wij deze memo als oplegger te moeten meegeven ter nuancering.

Belangrijke constatering van de accountant is dat zij kan steunen op de Verbijzonderde Interne Controle (VIC) zoals deze in Hollands Kroon is georganiseerd. Dit is met name relevant omdat met de VIC, zoals deze georganiseerd is in een organisatie met zelfsturende teams, de accountant haar controlewerkzaamheden kan uitvoeren. De accountant constateert wel dat de effectiviteit van een aantal processen minder is ten opzichte van 2016 (minder vastlegging en daarmee minder transparant). Het betreft de processen Planning en Control, Betalingen en Lonen en Salarissen. Vanuit deze bevindingen zijn aanvullende controles nodig geweest.

De kwalificatie van de processen dient te worden gelezen als schaal die bepalend is voor de intensiteit van de controlewerkzaamheden van de accountant. Niet als diskwalificatie van een proces.

Memo

De accountant geeft een aantal belangrijke ontwikkelingen aan waar gemeenten mee te maken krijgen en waarop wij ons dienen voor te bereiden e/o te organiseren. Het blijkt dat informatietechnologie een steeds belangrijkere factor wordt voor gemeenten. Niet enkel slechts een productiefactor maar ook een factor van strategische betekenis met een steeds groter afbreukrisico voor de gemeente (met zowel financiële, juridische als bestuurlijke risico's). Deze ontwikkelingen zijn bij ons bekend.

Managementletter 2017

Gemeente Hollands Kroon



28 februari 2018

Managementletter 2017

Aan het college van burgemeester en wethouders
van de gemeente Hollands Kroon
Postbus 8
1760 AA ANNA PAULOWNA

Amstelveen, 28 februari 2018
Kenmerk: RB/SS/GvD/DR/AA18-0353

Geacht College,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2017 van de gemeente Hollands Kroon brengen wij u hiermee verslag uit over onze bevindingen naar aanleiding van onze interim-controle.

Voor een nadere omschrijving van onze opdracht, de reikwijdte en aanpak van onze controle en overige afspraken verwijzen wij naar onze opdrachtbevestiging d.d. 29 september 2017. 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. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelfcontrolerend vermogen van uw organisatie.

Het concept van deze managementletter hebben wij ambtelijk afgestemd en op 21 december 2017 met de verantwoordelijke portefeuillehouder. Wij vertrouwen erop u met deze managementletter naar aanleiding van onze interim-controle 2017 van dienst te zijn. Wij willen de organisatie bedanken voor de prettige samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,
BDO Audit & Assurance B.V.

w.g.
H.C.J. Bot RA

Inhoudsopgave

1. Dashboard interim-controle

2. Waarnemingen vanuit onze natuurlijke advies rol

3. Interne beheersing op organisatieniveau

4. Bevindingen significante processen

5. Informatiebeveiliging

Bijlage

1. Dashboard interim-controle

Belangrijkste bevindingen

- Het niveau van de ‘hard controls’ binnen de gemeente is net als voorgaande jaren laag. Veel controls worden niet zichtbaar vastgelegd. Dit is inherent aan de gekozen inrichting van de organisatie. De organisatie heeft de filosofie gebruik te maken van Soft controls, de ‘Soft controls’ dienen nog verder te worden uitgewerkt.
- Wij kunnen de controle niet systeemgericht uitvoeren en daarom voeren wij deze gegevensgericht uit.
- Door het “in huis halen” van de BUIG is de beheersing/monitoring van het proces Sociaal Domein versterkt.
- Het proces P&C is lager dan vorig jaar als gevolg van met name aanpassing van de begroting, het beperkt aantal formele rapportage-momenten en enkele budgetoverschrijdingen.
- Bij de processen Lonen en Salarissen en Betalingen hebben wij een aantal aanvullende bevindingen geconstateerd ten opzichte van voorgaand jaar. M.b.t. het proces Belastingen hebben wij verbeteringen t.o.v. voorgaand jaar onderkend.
- Meerdere bevindingen m.b.t. de automatiseringsomgeving (zie opmerkingen middenonder).
- Gedurende 2017 is de organisatie gestart met het opstellen van verbeterplannen. Deze zullen in 2018 verder worden uitgewerkt.

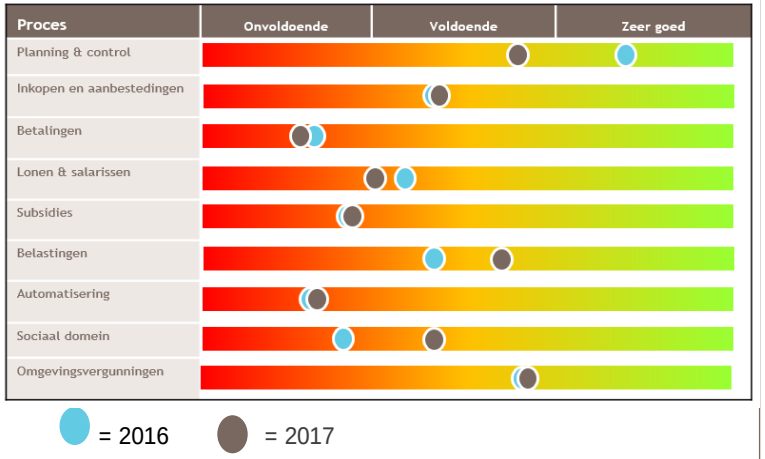
Ontwikkelingen

Vanuit onze natuurlijke adviesfunctie onderkennen wij de volgende ontwikkelingen met betrekking tot de controle van de jaarrekening:

- Herinrichting administratie naar taakvelden
- ENSIA
- WNT
- Wet Normalisering rechtspositie ambtenaren
- Privacybescherming
- Nieuwe omgevingswet

Interne ontwikkelingen: invoering STIP, uitkeringsadministratie per 1-4-2017 zelf gevoerd en Balans 2018 (zie elders op deze pagina).

Effectiviteit processen



Bedrijfsvoering

- Vertrek sleutelfunctionarissen.
- De ‘Soft controls’ dienen nog verder te worden uitgewerkt en een wijze van tussentijdse monitoring op deze controls dient te worden geïmplementeerd.
- KPI’s Incluzio (Wmo en Jeugdzorg) tot en met Q2 2017 nog niet behaald.
- Wij kunnen steunen op de verbijzonderde interne controle (COS 610).
- Er is geïnvesteerd in de VIC die achteraf een grote omvang van gegevensgerichte werkzaamheden uitvoert. Dit mitigeert voor een deel de tekortkomingen in de processen.
- Er is een concept VIC rapportage 1e halfjaar 2017 beschikbaar. Deze rapportage is laat in het jaar beschikbaar gekomen.
- VIC werkzaamheden inzake Wmo en Jeugdzorg nog uit te voeren.
- Het normenkader voor de rechtmatigheid 2017 moet nog worden vastgesteld voor aanvang van de jaarrekeningcontrole.

Bevindingen IT

Logische toegangsbeveiliging

- Authenticatieprocedures (w.o. wachtwoorden) in de applicatie Key2 zijn niet toereikend.
- Vastlegging opzet van vereiste autorisaties en periodieke review op de autorisaties ontbreken.
- Meerdere algemene accounts in gebruik zonder monitoring hierop.

Wijzigingenbeheer

- Geformaliseerde procedures voor wijzigingenbeheer en autorisaties ontbreken.

Continuïteitsmaatregelen

- Back-up procedures vinden plaats en uitwijkmogelijkheden worden getest.

Wij adviseren tevens de bevindingen inzake de automatiseringsomgeving mee te nemen in het verbeterplan ‘’Balans 2018’’.

Plan van aanpak Balans 2018

- Er is een verbeterplan ‘’Balans 2018’’ opgesteld.
- Vier pijlers in plan van aanpak balans 2018
  - het verbeteren van de beleidscyclus (planning & control cyclus);
  - het versterken van regie op projectmatig en programmatisch werken;
  - het verbeteren van onze externe dienstverlening;
  - slimmer inrichten van de interne beheersing.
- Balans 2018 betreft een overkoepelend plan waarin per activiteit afspraken zijn opgenomen en/of waarvoor nadere plannen worden uitgewerkt.
- De eerste aanzet hiertoe is in 2017 gestart en gedurende 2018 zal verdere invulling worden gegeven.

2. Waarnemingen vanuit onze natuurlijke advies rol



2.1 Actuele ontwikkelingen



2.2 Interne ontwikkelingen

2.1 Actuele ontwikkelingen

Inleiding, Taakvelden BBV en ENSIA

Wij signaleren een aantal ontwikkelingen

Inleiding ontwikkelingen en onze natuurlijk adviesrol

De overheidssector is altijd volop in beweging en ook voor gemeenten spelen vele actuele ontwikkelingen. Vanuit onze natuurlijk adviesrol en kennis van de branche signaleren wij een aantal ontwikkelingen die gerelateerd zijn aan ons vakgebied en uw interne beheersing. Het voert te ver om in deze managementletter alle ontwikkelingen uitgebreid te beschrijven en te beoordelen op welke wijze uw gemeente hier invulling aan geeft. Alleen indien deze ontwikkelingen impact hebben op de jaarrekening en onze controle hiervan, zullen wij dat nadrukkelijk benoemen. Wij signaleren een aantal ontwikkelingen in uw branche die wij in dit hoofdstuk verder beschrijven.

O.b.v. BBV nieuwe bijlage met taakvelden in jaarrekening 2017

Taakvelden conform BBV in de jaarrekening 2017

Met ingang van het begrotingsjaar 2017 dient de gemeente of provincie in de financiële begroting én de jaarrekening een bijlage op te nemen met de baten en lasten per taakveld. De doelstelling van deze bijlage is om de vergelijkbaarheid van gemeenten respectievelijk provincies te vergroten. Op grond van artikel 24 lid 3d BBV is de bijlage met de taakvelden formeel onderdeel van de jaarrekening en daarmee een onderdeel van de jaarlijkse controle op de getrouwheid en de rechtmatigheid van de jaarrekening. Wij hebben vastgesteld dat de gemeente de inrichting van de administratie tijdig heeft gedaan. De begroting 2017 is opgesteld op basis van de taakvelden. De begroting is vastgesteld door de raad. Tijdens de jaarrekening controle zullen wij tevens aandacht besteden aan de juiste inrichting van de taakvelden. Over de uitkomsten van onze werkzaamheden rapporteren wij in ons accountantsverslag.

ENSIA vereenvoudiging audits t.a.v. informatieveiligheid

Eenduidige Normatiek Single Information Audit (ENSIA)

De sterk toegenomen en nog steeds toenemende digitalisering van gemeenten vraagt veel aandacht voor de kwaliteit van informatieveiligheid. Gemeenten beheren in toenemende mate veel persoonsgegevens. Elk jaar moeten gemeenten zich dan ook verantwoorden over de kwaliteit van informatieveiligheid en/of de hierbij gebruikte informatiesystemen / -platformen. Tot nu toe bestonden hiervoor diverse aparte audits; een tijdrovende aangelegenheid voor gemeenten. Het project ENSIA (Eenduidige Normatiek Single Information Audit) heeft als hoofddoel de verantwoording voor gemeenten te vereenvoudigen door deze zo effectief en efficiënt mogelijk in te richten, gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De gemeente Hollands Kroon zal in het voorjaar een afzonderlijke audit uit laten voeren.

Zelfevaluatie en audit in 2018

In 2017 dient elke gemeente een zelfevaluatie op te stellen en uit te voeren door middel van het invullen van een vragenlijst. Op basis van de uitkomsten van de zelfevaluatie wordt een collegeverklaring opgesteld waarop een audit plaats zal vinden. De scope van de audit voor 2017 betreft Suwinet en DigiD. Zo wordt ‘horizontaal’ de collegeverklaring (waarin de gemeente de algehele status van informatiebeveiliging verantwoordt) in het jaarverslag verwerkt, om deze vervolgens als integraal rapport aan te bieden aan het ministerie van Binnenlandse Zaken. ‘Verticaal’ wordt de specifieke status per auditonderdeel (voor 2017 Suwinet en DigiD) verantwoord richting de betreffende toezichthouder (bijv. Logius voor DigiD). De rapportagedeadline hiervoor is 1 mei 2018. Omdat de verantwoording plaats vindt via het college en het jaarverslag is ENSIA geen direct onderdeel van onze controle. Eventuele bevindingen en risico’s uit de audit zouden dit mogelijk wel kunnen hebben. Wij blijven graag op de hoogte van de uitkomsten van de zelfevaluatie en de audit.

Vooralsnog geen impact op jaarrekening 2017

2.1 Actuele ontwikkelingen

Gevolgen Evaluatiewet WNT

WNT op enkele onderdelen vereenvoudigd en verbeterd	Wet Normering Topinkomens (WNT) Per 1 juli 2017 is de Evaluatiewet WNT in werking getreden. Hiermee is de WNT op enkele onderdelen vereenvoudigd en verbeterd en worden de administratieve lasten voor WNT-instellingen verminderd. Ook scherpt de Evaluatiewet WNT de normering aan om wetsontwijking tegen te gaan. Voor de bepalingen van de Evaluatiewet WNT geldt dat zij op verschillende momenten in werking treden, deels ook met terugwerkende kracht. De belangrijkste wijzigingen betreffen: *Vervallen algeheel verbod variabele beloning (terugwerkende kracht miv. 1 januari 2017)* Het verbod op het verstrekken van winstdelingen, bonussen of andere vormen van variabele beloning aan topfunctionarissen vervalt. Variabele beloning is vanaf kalenderjaar 2017 toegestaan zolang de totale bezoldiging onder het toepasselijke bezoldigingsmaximum blijft. *Ontslaguitkeringen op grond van cao's en andere collectieve regelingen (terugwerkende kracht miv. 1 januari 2017)* Niet alleen uitkeringen die rechtstreeks, dwingend en eenduidig voortvloeien uit een algemeen verbindend verklaarde cao of een wettelijk voorschrift zijn uitgezonderd van de normering van de ontslaguitkering, maar ook uitkeringen die voortvloeien uit niet algemeen verbindend verklaarde cao's of andere collectieve regelingen. Het moet daarbij gaan om regelingen met een collectief karakter waarop de individuele topfunctionaris geen invloed heeft (o.a. sociaal plan). *Bezoldiging betaald gedurende een van-werk-naar-werk-traject (terugwerkende kracht miv. 1 januari 2017)* De regel dat bezoldiging betaald tijdens een van-werk-naar-werk-traject niet als uitkering wegens beëindiging van het dienstverband maar als bezoldiging wordt aangemerkt, als dat traject rechtstreeks, dwingend en eenduidig voortvloeit uit een algemeen verbindend verklaarde cao of wettelijk voorschrift, is niet langer in de Beleidsregels WNT geregeld, maar bij wet geregeld. *Aanscherping van de personele reikwijdte van de wnt (miv 1 januari 2018)* Een topfunctionaris die tenminste twaalf maanden een topfunctie heeft vervuld en vervolgens een niet-topfunctie gaat vervullen bij dezelfde instelling blijft nog vier jaar aangemerkt als topfunctionaris. Het begrip 'gewezen topfunctionaris' vervalt. WNT-instellingen vermelden gewezen topfunctionarissen voor het laatst in de WNT-verantwoording over kalenderjaar 2017. *Anticumulatiebepaling (miv 1 januari 2018)* De WNT maximeert de totale bezoldiging uit functies als leidinggevende topfunctionaris bij verschillende WNT-instellingen tot het algemeen bezoldigingsmaximum. Daarnaast zijn er een wijzigingen tav de digitale melding van wnt-en publicatieplicht (miv 1 januari 2018). Tevens is het bezoldigingsmaximum miv 1 januari 2018 aangepast. Met ingang van 1 januari 2018 bedraagt het algemene WNT-maximum voor een fulltime topfunctionaris € 186.000. (2017: € 181.000).
Ontwikkeling WNT bij de gemeente Hollands Kroon	WNT ontwikkelingen bij de gemeente Hollands Kroon Bij gemeenten worden conform de Wet Normering Topinkomens de gemeentesecretaris en griffier van de gemeente aangemerkt als topfunctionaris. Gedurende 2017 heeft bij de gemeente Hollands Kroon een wijziging plaatsgevonden van zowel de gemeentesecretaris als de griffier. Bij het opstellen van de jaarrekening dient met deze wijziging van de topfunctionarissen rekening gehouden te worden.

2.1 Actuele ontwikkelingen

WNRA

WNRA ingevoerd vanaf 2020	Wet Normalisering Rechtspositie Ambtenaren (WNRA) Vanaf 1 januari 2020 wordt de Wet Normalisering Rechtspositie Ambtenaren (WNRA) ingevoerd. Het traject dat voor u ligt, vraagt nu al om gerichte acties. Ook omdat u in veel gevallen afhankelijk bent van andere partijen. Dankzij deze drie must do's voor komend jaar bent u beter voorbereid op de invoering van de WNRA.
3 actiepunten voor komend jaar	1. Inventariseren van alle arbeidsvoorwaarden Voordat de WNRA ingaat, is het voor gemeenten belangrijk een nulpunt vast te stellen. Daar zijn drie redenen voor. Ten eerste vanwege de grote kans dat de individuele arbeidsvoorwaarden behoorlijk wat afwijkingen vertonen. Bijvoorbeeld door detachering, individuele onkostenvergoedingen, bonusregelingen, leaseauto's, vaste of parttimedagen. Weet u welke arbeidsvoorwaarden binnen de gemeente gelden, dan kunt die ook vastleggen in een eventuele arbeidsovereenkomst, zodat er later geen discussie ontstaat over welke arbeidsvoorwaarden gelden. Tweede reden om te inventariseren is om straks te kunnen vaststellen welke regelingen u nog in het personeelsreglement moet opnemen. De kans is namelijk groot dat onder andere het verzuimbeleid en regels over het opnemen van verlof in een apart personeelsreglement moeten worden opgenomen. Door de arbeidsvoorwaarden te inventariseren, kunt u straks vaststellen om welke regelingen het precies gaat. Derde reden is dat er in de toekomst wellicht meerdere arbeidsvoorwaarden van toepassing zijn, zoals de cao sociale werkvoorziening (WSW), waardoor er mogelijk conflictsituaties ontstaan. 2. Scholing P&O-medewerkers en OR-leden Dit is belangrijk omdat het hele ontslagrecht gaat veranderen. De bezwaar- en beroepsprocedures komen te vervallen en het civiele ontslagrecht wordt van toepassing. Het spreekt voor zich dat het team P&O tot in detail op de hoogte is. Ook belangrijk is dat de ondernemingsraad (OR) geschoold is, want die krijgt grotere en uitgebreidere bevoegdheden. Zo wordt hun instemmingsrecht belangrijker. Wat betekent dat de OR een grotere rol krijgt bij de invoering van de normalisering, omdat bijvoorbeeld het aanstellingsbeleid gaat wijzigen. En daar is instemming van de OR voor nodig. Het is dus zaak de OR al in het voorstadium van de invoering de kans te geven zich goed te laten scholen. 3. Keuze voor cao Gaat u een eigen cao afsluiten, of sluit u zich aan bij een collectieve cao, zoals van VNG? Het is belangrijk hier nu over na te denken, want cao-trajecten gaan tenslotte niet over een nacht ijs. De vraag is: met wie wilt u die cao afsluiten en wie nodigt u daarvoor uit? Daar heeft u nu een grotere keuzevrijheid in. Overweging is aansluiten bij het nieuw af te sluiten cao van de VNG. Andere optie is een cao afsluiten met andere gemeenten, met oog op een gunstigere concurrentiepositie. Of met andere publieke organisaties, in de regio of naar schaalgrootte. Daar moet u nu over nadenken. Voorbereid zijn op de invoering van WNRA zal veel tijd in beslag nemen. De stappen die nu al mogelijk zijn, moet u vooral gaan zetten. Voor gemeentes is het dan ook handig en verstandig om deze drie must do's zo snel mogelijk te realiseren.

2.1 Actuele ontwikkelingen

Privacybescherming

AVG in 2018	Privacybescherming De bescherming van databestanden en privacygegevens is in de huidige tijd erg belangrijk. Onvoldoende beveiliging kan leiden tot verlies en diefstal van persoonsgegevens en vervolgens tot misbruik ervan, zoals identiteitsfraude. Privacybescherming staat zowel in Nederland als internationaal in de vernieuwde belangstelling, door continue en toenemende incidenten bij zowel bedrijven als overheden. Er zijn momenteel twee wetten die bepalen hoe gemeenten persoonsgegevens mogen gebruiken. Dit zijn de Wet bescherming persoonsgegevens (Wbp/inclusief meldplicht datalekken) en de Wet basisregistratie personen (Wet BRP). De Autoriteit Persoonsgegevens houdt in de gaten of instellingen zich aan deze wetten houden. Bedrijven en overheden die persoonsgegevens verwerken moeten deze volgens de Wet beveiligen en hiervoor passende technische en organisatorische maatregelen nemen. Per 25 mei 2018 wordt de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG zorgt onder meer voor: ▪ Versterking en uitbreiding van privacyrechten. ▪ Meer verantwoordelijkheden voor organisaties. ▪ Dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes (tot € 20 miljoen) op te leggen.
Voorbereiding AVG: 10 belangrijkste stappen	De nadruk bij de AVG ligt - meer dan nu bij de Wpb - op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden. Dat vergt een gedegen voorbereiding. De Autoriteit Persoonsgegevens heeft de 10 belangrijkste stappen op een rijtje gezet: 1. Bewustwording 2. Rechten van betrokkenen 3. Overzicht verwerkingen 4. Data protection impact assesment (DPIA) 5. Privacy by design & privacy by default 6. Functionaris voor de gegevensbescherming 7. Meldplicht datalekken 8. Bewerkersovereenkomsten 9. Leidende toezichthouder 10. Toestemming De gemeente Hollands Kroon heeft systemen en procedures ingericht voor het controleren en signaleren van cyberaanvallen, virussen en datalekken. Gesignaleerde mogelijke datalekken worden vastgelegd, beoordeeld door de privacy beheerder waarbij wordt nagegaan of er sprake is van een datalek volgens de wet en of dit gemeld dient te worden aan de Autoriteit Persoonsgegevens. Dit is uitgewerkt in het beleid en het proces. De leidende toezichthouder is niet van toepassing bij gemeenten. Nieuw is dat de organisatie moet kunnen aantonen dat zij geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

2.1 Actuele ontwikkelingen

Omgevingswet

Nieuwe Omgevingswet per 2021	Omgevingswet Met de Omgevingswet bundelt de overheid de regels voor ruimtelijke projecten. De Omgevingswet gaat in 2021 in. De komst van de Omgevingswet betekent dat er veel verandert. De wet bundelt bijvoorbeeld 26 bestaande wetten voor onder meer bouwen, milieu, water, ruimtelijke ordening en natuur. Het is belangrijk dat de gemeenten nu al beginnen met de voorbereidingen. Wat levert de Omgevingswet de Nederlander op? Een aantal feiten op een rij: ➢ Van 26 wetten naar 1 wet. ➢ Van 5000 wetsartikelen naar 350 artikelen. ➢ Van 120 ministeriële regelingen naar 10 regelingen. ➢ Van 120 algemene maatregelen van bestuur naar 4 maatregelen. ➢ 1 wet voor de hele leefomgeving. ➢ De wet maakt het mogelijk om lokale problemen ook lokaal op te lossen. ➢ Van meerdere bestemmingsplannen naar 1 omgevingsplan.
Omgevingsvisie moeten worden opgesteld	De Omgevingswet verplicht het Rijk, de provincie en gemeente een omgevingsvisie te maken. In de omgevingsvisie moeten zij rekening houden met de verschillende belangen in een gebied.

2.2 Interne ontwikkelingen

STIP **Zelfsturende teams**	STIP In 2015 is begonnen met een ingrijpende organisatieverandering als gevolg van de verdere uitwerking van STIP 2018. In de filosofie van de gemeente krijgen zelfsturende teams de vrijheid en het vertrouwen om hun werkzaamheden op hun eigen manier uit te voeren, binnen de gestelde kaders. In 2018 zal de organisatie geheel uit zelfsturende teams bestaan zonder afdelingsmanagers of leidinggevenden. Gedurende 2017 heeft de afronding van de vorming van de zelfsturende teams plaatsgevonden. De zelfsturende teams zijn allemaal bevestigd. Alle 35 zelfsturende teams zijn in 2017 reeds van start gegaan met hun werkzaamheden. De nieuwe organisatiestructuur vraagt om een andere wijze van aansturen. De 'hard' controls zullen niet volledig worden losgelaten, maar wel gedeeltelijk. Hiervoor in de plaats kunnen soft controls worden opgenomen. Het management heeft momenteel in onderzoek in welke vorm dit ingevoerd kan worden. In 2017 is nog geen sprake geweest van soft controls. Door de vermindering van de hard controls kunnen wij geen systeemgerichte controle uitvoeren. Wij zullen de controle daarom gegevensgericht uitvoeren. Daarbij zullen wij ook gebruik maken van de VIC.
Uitkeringsadministratie en sociaal domein	Uitkeringsadministratie en sociaal domein De gemeente Hollands Kroon had het proces met betrekking tot de uitkeringen (BUIG) tot en met 2014 ondergebracht bij de Intergemeentelijke Sociale Dienst Kop van Noord-Holland. Vanaf 2015 heeft de gemeente Hollands Kroon het proces ondergebracht bij het COWWI dat onder de gemeente Schagen valt. Er is besloten om vanaf 1 april 2017 de uitvoering weer zelfstandig uit te voeren bij de gemeente Hollands Kroon. De uitvoering van de cliëntadministratie en de factuurverwerking m.b.t. de Wmo en Jeugdzorg is in 2015 ook verricht door het COWWI. Vanaf 1 juli 2016 heeft de gemeente Hollands Kroon één overkoepelend contract afgesloten met één partij voor de uitvoering van de Wmo en Jeugdzorg. De cliëntadministratie en de factuurcontrole zullen in 2017 ook door de gemeente Hollands Kroon zelf uitgevoerd worden. Het zelfstandig uitvoeren van de uitkeringsadministratie, Wmo en Jeugdzorg kent een andere wijze van beheersing dan wanneer deze is uitbesteed, zeker gezien de specifieke kenmerken van deze processen.
Balans 2018	Balans 2018 In de tweede helft van 2017 is het Plan van aanpak Balans 2018 opgesteld door de gemeente. De gemeente heeft dit verbeterplan opgesteld om een noodzakelijk geachte kwaliteitssprong binnen de organisatie te realiseren. Het plan van aanpak kent vier pijlers: • het verbeteren van de beleidscyclus (planning & control cyclus); • het versterken van regie op projectmatig en programmatisch werken; • het verbeteren van onze externe dienstverlening; • slimmer inrichten van de interne beheersing. Balans 2018 betreft een overkoepelend plan waarin per activiteit afspraken zijn opgenomen en/of waarvoor nadere plannen worden uitgewerkt. De eerste aanzet hiertoe is in 2017 gestart en gedurende 2018 zal verdere invulling worden gegeven. Wij adviseren per proces de verbeteracties concreter te benoemen en uit te werken. Een belangrijk aandachtspunt dat meegenomen dient te worden betreft ook de IT in de processen.

3. Interne beheersing op organisatieniveau



3.1 Planning & Control cyclus



3.3 Frauderisico-analyse



3.2 Verbijzonderde interne controle

3.1 Planning en control cyclus

Indien mogelijk gebruik maken van overkoepelende beheersingsmaatregelen

Planning en control

In het kader van onze controle hebben wij aandacht besteed aan de Planning & Control cyclus. De Planning & Control cyclus omvat overkoepelende beheersingsmaatregelen, ook wel 'entity level controls' genoemd (afgekort ELC's). Bij de gemeente Hollands Kroon wordt dit de Beleid cyclus genoemd. Indien deze interne beheersing in opzet, bestaan en werking toereikend en aantoonbaar is, kunnen wij als accountant hiervan gebruik maken in onze controle.

Middels een gesprek en door het opvragen van onderliggende documenten hebben wij de volgende onderdelen beoordeeld:

1. Inrichting organisatie ten aanzien van financiën en control
2. Totstandkoming en autorisatie begroting (-wijzigingen)
3. Totstandkoming tussentijdse rapportages
4. Extern (provinciaal) toezicht
5. Systeem van risicomanagement
6. Het proces van de totstandkoming van de jaarrekening

In het algemeen constateren wij dat de gemeente Hollands Kroon een uitgebreid systeem van interne beheersing heeft binnen de Planning & Control cyclus. Niet alle onderdelen in het proces zijn achteraf zichtbaar. Naar aanleiding van onze werkzaamheden hebben wij de volgende bevindingen en aanbevelingen:

- De organisatievisie van de gemeente Hollands Kroon gaat uit van eigen verantwoordelijkheid van de zelfsturende teams. Iedere budgetbeheerder heeft de mogelijkheid de bestedingen op zijn budget ten opzichte van de begroting te bekijken. Wij hebben geconstateerd dat de er geen formele rapportages aan budgethouders plaatsvinden (wel informeel, maar niet voor ons waarneembaar). Gedurende 2017 is het team Consult gestart (financiële consulenten bij afdelingen). Dit team is onder andere verantwoordelijk voor het monitoren van de planning en control cyclus.
- De begroting wordt bottum-up opgesteld. Hiervoor is een gedetailleerde planning, mede op basis van de kadernota, bestuursrapportage, etc. De programmabegroting 2017 bestaat uit vier programma's: Bedrijvigheid, Leefbaarheid, Vitaliteit en Bedrijfsvoering. De programmabegroting is hierdoor in grote mate op hoofdlijnen. Wij hebben begrepen dat dit proces niet beschreven is. Wij adviseren u dit proces te beschrijven, inclusief de interne controlemaatregelen ten aanzien van de totstandkoming van de begroting, vanwege het belang van de begroting als sturingsinstrument. Hetzelfde geldt ook voor het proces ten aanzien van de begrotingswijzigingen.
- De bestuursrapportages komen tot stand mede op basis van de voortgang- en realisatiegesprekken met de verantwoordelijke budget beheerders en betrokkenheid van team consult. De budget beheerders zijn verantwoordelijk voor de subadministratie en verklaren eventuele afwijkingen tussen budget en realisatie. Wij hebben tijdens onze interim-controle vastgesteld dat voorafgaand aan het opstellen van de bestuursrapportages een structureel proces wordt doorlopen.
- Ten aanzien van het risicomanagement en extern (provinciaal) toezicht hebben wij geen tekortkomingen gesignaleerd.
- Over het proces van de totstandkoming van de jaarrekening rapporteren wij in het accountantsverslag.

Wij adviseren u het financieel afsluitproces te formaliseren en de verschillende stappen binnen het proces zichtbaar te maken aan de hand van documentatie. Ten aanzien van de begrotingswijzigingen zal de verbijzonderde interne controle nog verbijzonderde interne controle werkzaamheden uitvoeren waarbij wordt gekeken naar juiste en rechtmatige verwerking.

3.2 Verbijzonderde interne controle

Verbijzonderde interne als sluitstuk interne beheersing

Beoordeling VIC

Positie VIC in de organisatie voldoende onafhankelijk

VIC is voldoende deskundig

Inleiding

De verbijzonderde interne controle (VIC) vormt binnen uw gemeente als het ware het sluitstuk van het systeem van interne beheersing. Bij de uitvoering van onze controlewerkzaamheden maken wij waar mogelijk gebruik van de door de Verbijzonderde Interne Controle uitgevoerde werkzaamheden. De verbijzondere interne controles worden bij de gemeente Hollands Kroon uitgevoerd door het team Effect.

Bij het beoordelen van de organisatie van de verbijzonderde interne controle van uw gemeente onderscheiden wij een aantal belangrijke aandachtspunten, te weten:

- Positionering van de VIC binnen de organisatie
- De rol, omvang en kwaliteit van de VIC-functie in uw gemeente
- Het binnen uw organisatie opgestelde risico-analyse en interne controleplan
- De planning, uitvoering en evaluatie van de interne controle werkzaamheden, waaronder:
    - De jaarlijkse planning van de uit te voeren VIC-werkzaamheden
    - De werkprogramma's/checklists die worden gehanteerd door de VIC
    - Het bepalen van het aantal te verrichten deelwaarnemingen
    - De daadwerkelijke uitvoering van de VIC-werkzaamheden
    - Het evalueren van en rapporteren over de bevindingen

Jaarlijks worden steeds hogere eisen gesteld aan de onafhankelijkheid en kwaliteit van de VIC, voordat wij als accountant hierop kunnen steunen.

Net als voorgaand jaar concluderen wij dat wij kunnen steunen op de VIC bij de gemeente Hollands Kroon. Het team Effect voldoet in voldoende mate aan de eisen zoals deze zijn gesteld aan COS 610. De positie van het team Effect binnen de organisatie is onafhankelijk. De coördinatie en kwaliteitsbewaking vindt plaats door een Qualified Controller en het team heeft voldoende ervaring en kennis is opgebouwd de afgelopen jaren.

De uitvoering van de interne controlewerkzaamheden vinden gedurende het gehele jaar plaats waardoor tijdige bijsturing in het proces kan plaatsvinden.

Bij de gemeente Hollands Kroon zijn er beleid en procedures omtrent de plaats van de VIC in de organisatie, de deskundigheid van de medewerkers en review van werkzaamheden. Deze zijn echter niet geformaliseerd in het interne Controleplan en rapportage. Wij adviseren u dit wel explicieter op te nemen. Daarnaast hebben wij geconstateerd dat uitgevoerde werkzaamheden worden gereviewd. De zichtbaarheid hiervan betreft echter nog een aandachtspunt.

Voor het boekjaar 2017 is een nieuw intern controleplan vastgesteld. De VIC heeft gezien de omstandigheden bij de gemeente gedurende 2017 nog geen tussentijds verslag gedaan van de bevindingen. De eerste rapportage zal derhalve nog moeten worden uitgebracht. Tijdigheid van de rapportage betreft een aandachtspunt wat wij reeds meerdere jaren in de managementletter hebben vermeld.

3.3 Frauderisico-analyse

Jaarlijks frauderisico's herbeoordelen

Advies: opstellen M&O-beleid

Frauderisico-analyse

Jaarlijks verricht de gemeente Hollands Kroon verschillende risico-analyses. Deze risico-analyses zijn met name gericht op de operationele activiteiten en in mindere mate op het fraude-aspect binnen processen. Bij de opzet van de interne beheersingsmaatregelen dient rekening te worden gehouden met fraude-risico's in de processen (beschrijvingen). Het verdient de aanbeveling de frauderisico's jaarlijks zichtbaar te evalueren.

Daarnaast adviseren wij ook een M&O-beleid op te stellen ten behoeve van het voorkomen van misbruik en oneigenlijk gebruik. In het Bado wordt onder het rechtmatigheidsbegrip namelijk ook het Misbruik en Oneigenlijk gebruik (M&O) criterium genoemd. De rechtmatigheidseis betreft ook de toetsing op juistheid en volledigheid van de gegevens, die door de belanghebbenden zijn verstrekt om het voldoen aan voorwaarden aan te tonen. Dit ter voorkoming en bestrijding van misbruik en oneigenlijk gebruik van wet- en regelgeving (M&O-criterium).

In de Kadernota Rechtmatigheid van de commissie BBV is ook opgenomen dat om misbruik en oneigenlijk gebruik van overheidsgelden te voorkomen de interne en externe controle erop gericht zullen moeten zijn om dat vast te stellen. Het gaat bij het M&O-criterium in het bijzonder om vast te stellen dat in de organisatie effectieve maatregelen zijn getroffen om misbruik te voorkomen, dan wel op te sporen en dat de vigerende wet- en regelgeving duidelijk is, aangepast is aan actuele omstandigheden en te handhaven is. Om dit te bewerkstellingen is een mix van maatregelen nodig.

Het op te stellen M&O-beleid omvat bijvoorbeeld de interne beheersingsactiviteiten die zijn geïmplementeerd in de processen, maar ook de rol van de Verbijzonderde Interne Controle, de omgeving waarin de processen worden uitgevoerd (integriteit medewerkers) en handhaving.

Wij verwijzen verder naar de nota 'Rechtmatigheid: Voorkoming Misbruik & Oneigenlijk Gebruik (M&O)' van de Commissie BBV waarin hier uitgebreid op wordt ingegaan (www.commissiebbv.nl).

Het uitvoeren van een frauderisico-analyse en het opstellen van een M&O-beleid zullen worden opgenomen in het plan 2018 van de verbijzonderde interne controle.

4. Bevindingen significante processen

4.1

Onze controleaanpak transparanter

4.3

Detailbevindingen

4.2

Effectiviteit processen

4.1 Onze controleaanpak transparanter

Toenemende eisen aan kwaliteit en documentatie accountantscontrole

Ontwikkelingen in accountancy

De afgelopen jaren is er veel discussie over de kwaliteit van de accountantscontrole. Recent is een opnieuw een rapport van de AFM uitgekomen waarin de kwaliteit van de accountantscontrole bij Organisaties van Openbaar Belang (OOB's) is onderzocht. Daarin constateert de AFM dat het veranderproces en de kwaliteitsverbeteringen bij accountantskantoren te langzaam gaan. Wij hebben als BDO kennis genomen van dit rapport en werken hard aan de implementatie van een groot scala van verandermaatregelen.

Door de toenemende eisen aan de controle en documentatie, dienen wij ook voor de gemeente Hollands Kroon meer werkzaamheden uit te voeren, meer vragen te stellen en soms uitgebreidere onderbouwingen te verkrijgen. In onze visie is het cruciaal met onze cliënten in gesprek te blijven over de veranderende eisen die worden gesteld aan de accountantscontrole. Wij vinden het van groot belang dat wij inzicht geven in de normen en verwachtingen ten aanzien van onze controle en de vertaling hiervan specifiek voor de gemeente Hollands Kroon. Alleen dan gaat de discussie niet alleen over de kwaliteit van de accountantscontrole, maar ook over de wijze waarop de gemeente hiervan kan profiteren. In deze managementletter hebben wij daarom meer in detail uitgelegd op welke wijze wij de controle hebben ingericht en welke afwegingen wij daarbij maken. Wij doen dat door in deze paragraaf onze risico-inschatting, belangrijkste processen, controleaanpak en afwegingen te beschrijven.

Onderkende significante risico's

Onze inschatting van de risico's en belangrijkste processen

In het kader van de controle van de jaarrekening 2017 en onze aanpak hebben wij een zogenaamde initiële risico-inschatting gemaakt. Wij zien de volgende significante risico's in de controle van de jaarrekening van de gemeente Hollands Kroon:

- ✓ Het risico van management override: dit is het op grond van de controlestandaarden te onderkennen risico dat het management buiten de getroffen interne beheersmaatregelen om invloed zou kunnen of willen uitoefenen op de in de jaarrekening gepresenteerde uitkomsten, bijvoorbeeld door beïnvloeding van schattingsposten (bijvoorbeeld voorzieningen).
- ✓ Het niet naleven van de Europese aanbestedingsregels: dit is een sectorspecifiek risico voor gemeenten vanwege de omvang en complexiteit van de regelgeving met betrekking tot aanbestedingen.
- ✓ De waardering van de grondexploitaties: dit is een specifiek risico voor de gemeente gezien de (relatief) omvangrijke grondexploitatie(s) binnen de gemeente en de waardering daarvan.
- ✓ De rechtmatigheid van de uitgaven en de levering nieuwe taken sociaal domein: dit is een sectorspecifiek risico gezien deze taken relatief nieuw zijn en de ontwikkelingen hierin.
- ✓ De gevolgen van ongeautoriseerde handelingen in de IT systemen (autorisaties): dit risico is opgenomen n.a.v. de bevindingen in de IT-omgeving.

Per proces toetsen:
- **AO/IB**
- **ICT**
- **VIC**

In onze aanpak steunen wij op de interne beheersing in de significante processen van de gemeente Hollands Kroon (een zogenaamde systeemgerichte aanpak). Zoals hiervoor beschreven maken wij voor een deel gebruik van de verbijzonderde interne controle (VIC). In onze aanpak hebben wij een aantal processen beoordeeld. Voor elk proces beoordelen wij de volgende onderdelen:

- AO/IB : Is sprake van een actueel en toereikend procesbeschrijving met voldoende beheersmaatregelen?
- IT maatregelen : Zijn in en rondom het systeem voldoende waarborgen getroffen ten aanzien van de betrouwbaarheid van de gegevensverwerking?
- VIC : Heeft de VIC de interne beheersmaatregelen getoetst en kunnen wij daar gebruik van maken?

Indien bovenstaande vragen positief kunnen worden beantwoord, kunnen wij optimaal gebruik maken van uw eigen interne beheersing en kunnen de gegevensgerichte werkzaamheden beperkt blijven tot een minimum.

4.2 Effectiviteit processen

Inschatting processen

Om u inzicht te verschaffen in de kwaliteit van de administratieve organisatie van de gemeente Hollands Kroon hebben wij de belangrijkste voor onze controle significante processen van de gemeente Hollands Kroon aan de hand van een aantal criteria beoordeeld en vergeleken met de norm. Wij hebben hiervoor o.a. de volgende criteria gehanteerd:

- Is het proces toereikend beschreven?
- Is de opzet van het proces toereikend?
- Bestaat en werkt het proces ook daadwerkelijk conform de beschreven opzet?
- Is het proces onderdeel van (verbijzonderde) interne controle?
- Is de (verbijzonderde) interne controle voldoende met betrekking tot getrouwheid en rechtmatigheid?
- Hebben wij vanuit de externe controle bevindingen rondom dit proces?
- Zijn voldoende beheersmaatregelen genomen in de applicaties waarvan het proces gebruik maakt?

Afgezien van bovenstaande criteria blijft altijd sprake van een inschatting (professional judgement) en moet dit vooral worden gebruikt om, samen met uw gemeente, te bespreken op welke aspecten nog verbeteringen mogelijk zijn.

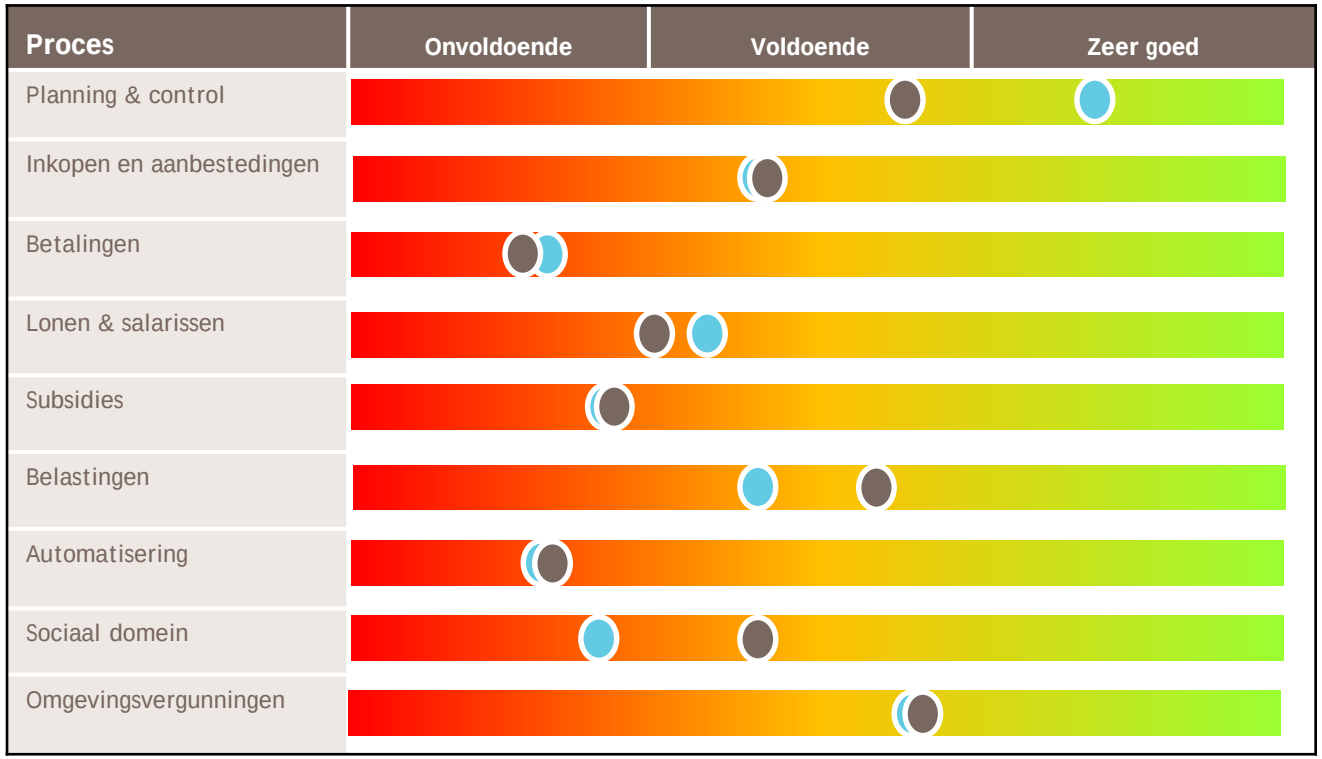
Ons beeld van de processen

Om u in één oogopslag inzicht te verschaffen in de kwaliteit van de (administratieve) processen van gemeente Hollands Kroon hebben wij in het figuur op de volgende pagina de door ons getoetste processen weergegeven. Daarbij zijn wij bij de beoordeling uitgegaan van de kwaliteit van de processen, rekening houdend met de ons bekende aanvullende gegevensgerichte maatregelen die de gemeente reeds uitvoert (VIC). Indien wij alleen de beheersmaatregelen in het proces en de hieraan gerelateerde IT- aspecten als norm zouden nemen en beoordelen, zouden de scores minder positief zijn. Wij zijn echter van mening dat een mix van systeem- en gegevensgerichte controles leiden tot een goede interne beheersing.

In het figuur zijn onze beoordelingen over het boekjaar 2016 en over het boekjaar 2017 opgenomen.

4.2 Effectiviteit processen

De beheersorganisatie scoort voldoende, rekening houdend met de nog uit te voeren gegevensgerichte werkzaamheden



Legenda:

Beoordeling per/over

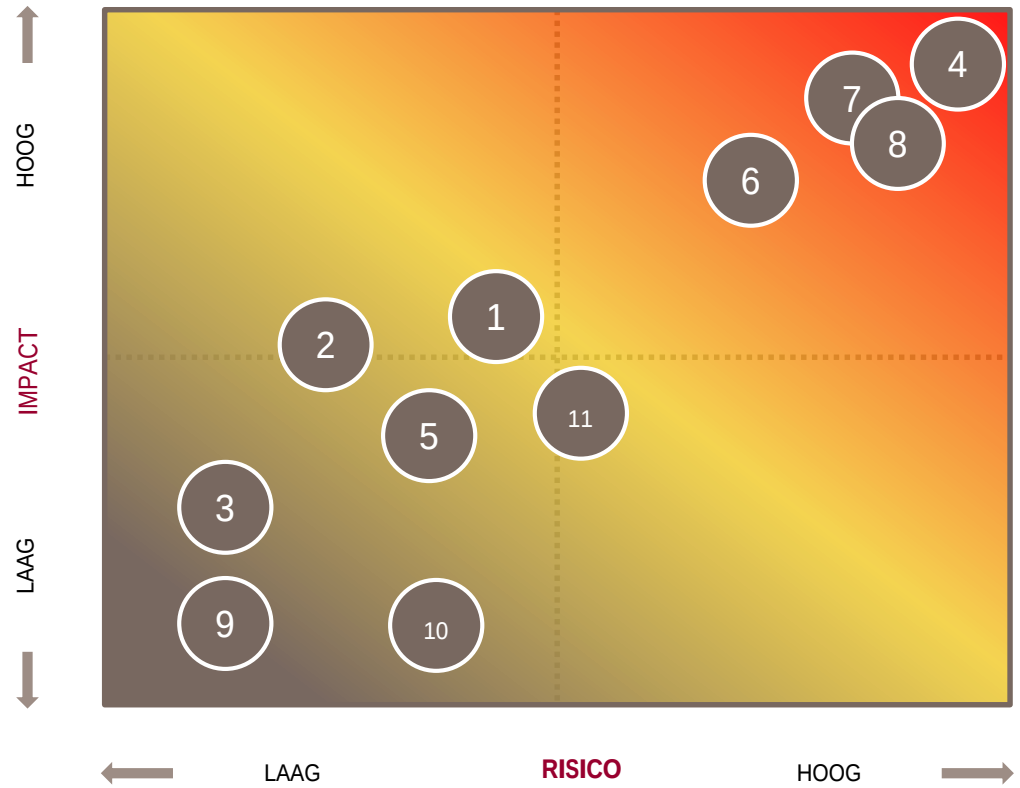
= 2016

= 2017

4.2 Effectiviteit processen

Kwaliteit van de materiële processen varieert	Effectiviteit processen Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat kwaliteit van de significante processen uitgaande Subsidies, Betalingen en de automatiseringsomgeving niet van een voldoende niveau zijn. De effectiviteit van de interne beheersingsmaatregelen in de processen is voor een groot deel gelijk aan voorgaand jaar. Bij de processen Planning & Control, Betalingen en Lonen en salarissen is sprake van een afname van de effectiviteit van de interne beheersing ten opzichte van voorgaand jaar. Bij deze processen hebben wij gedurende de interim-controle meerdere bevindingen geconstateerd, waaronder een aantal nieuwe bevindingen. Binnen het sociaal domein is sprake van een verbetering welke volgt uit het “in huis nemen” van de BUIG. Dit is per 1-4-2017 geeffectueerd en kent derhalve vanaf 2018 haar volle werking. Het proces inzake Planning & Control is lager ten opzichte van voorgaand jaar. Deze afname hangt samen met de aanpassing van de begroting – en daarmee de monitoring en sturing – naar 4 programma’s (high level), de bevinding dat er geen formele rapportages aan budgethouders plaatsvinden (wel informeel, maar niet voor ons waarneembaar) en gezien een aantal budgetoverschrijdingen in 2017. Daarentegen is in 2017 het team Consult gestart (financiële consulenten bij afdelingen). Het proces inzake Betalingen scoort lager ten opzichte van vanwege het feit dat er weliswaar functiescheiding aanwezig is in de betaalapplicatie, maar dat er geen feitelijk geen controles worden uitgevoerd (slechts steekproefsgewijs). Het proces Lonen en salarissen kent een lagere score ten opzichte van voorgaand jaar doordat de controle die plaats vindt op de mutatieverslagen die worden aangeleverd door de serviceorganisatie niet zichtbaar plaatsvindt en door bevindingen die vanuit de VIC zijn geconstateerd gedurende 2017. Het subsidieproces is als onvoldoende aangemerkt vanwege het ontbreken van functiescheiding in het proces en vanwege het feit dat wij hebben geconstateerd dat meerdere subsidieaanvragen niet voldoen aan alle elementen zoals opgenomen in de Algemene subsidieverordening, waarbij in sommige gevallen wel een beroep wordt gedaan op de hardheidsclausule. Het proces Informatiebeveiliging/automatiseringsomgeving hebben wij op onvoldoende beoordeeld. Hiervoor verwijzen wij naar hoofdstuk 5 van deze managementletter. Wij hebben geconstateerd dat een groot aantal van onze aanbevelingen uit voorgaande jaren gedurende 2017 (nog) niet zijn opgevolgd. Wij hebben geconstateerd dat een groot aantal processen niet zijn vastgelegd in procesbeschrijvingen. Wij adviseren de gemeente dit wel te doen, omdat dit waarborgen kan bieden voor de kwaliteit van de processen en als basis kan dienen voor risicoanalyse en overdracht. Bij de bovenstaande beoordeling van de effectiviteit van de processen hebben wij niet de processen inzake Treasury en Grondexploitaties opgenomen. Treasury en grondexploitaties controleren wij in maart 2018. Indien noodzakelijk rapporteren wij hier afzonderlijk over in ons accountantsverslag.

4.3 Detailbevindingen



Korte toelichting detailbevindingen	
1	P&C: Controle memoriaalboekingen met brondocumentatie ontbreekt
2	P&C: Monitoring tussentijdse interne rapportage budgethouders
3	P&C: Actualiseren/ ontbreken procesbeschrijvingen
4	IT: Bevindingen automatiseringsomgeving (logische toegangsbeveiliging, wijzigingenbeheer en continuïteit)
5	Treasury: ontbreken actueel treasurystatuut
6	I&A: Contractregister
7	I&A: Inkopen: geen zichtbare controle op prestatielevering
8	I&A: Betaalbevoegdheden
9	L&S: Bevindingen lonen en salarissen
10	Uitkeringen: bevindingen uitkeringen
11	Subsidies: bevindingen subsidies

5. Informatiebeveiliging

5.1

Inleiding Informatiebeveiliging

5.2

Logische toegangbeveiliging

5.3

Wijzigingenbeheer

5.3

Continuïteitsbeheer

5.1 Inleiding informatiebeveiliging

Audit werkzaamheden op ICT systemen 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 is gericht 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 werkzaamheden gericht op de kritieke ICT systemen en beheersmaatregelen daar omheen zijn geïntegreerd binnen de controle van de jaarrekening.

Het inzicht in de betrouwbare werking van ICT systemen 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 onbeheerste wijzigingen, ongeautoriseerde handelingen en het optreden van verstoringen met impact op de gegevensverwerking.

1. Om te beoordelen of wij kunnen steunen op de IT- beheersmaatregelen hebben wij op de volgende drie aspecten de interne beheersmaatregelen beoordeeld:
   Het *wijzigingenbeheer* moet zorgdragen voor het beheerst en controleerbaar doorvoeren van wijzigingen in de automatiseringsomgeving. Het proces van wijzigingenbeheer dient te waarborgen dat slechts door gebruikers geteste en akkoord bevonden wijzigingen aan de programmatuur worden aangebracht. Dit vormt voor het management en voor BDO de basis om vast te kunnen stellen of kritieke controlemaatregelen en rapportages gedurende het jaar hebben gewerkt en/of zijn gewijzigd.
2. De *logische toegangsbeveiliging* en adequate functiescheiding in het geautomatiseerde systeem zijn belangrijke onderdelen van de interne beheersing. Deze controlemaatregelen moeten de controle technische functiescheiding in de IT systemen waarborgen.
3. De *continuïteitsmaatregelen* beperken het risico dat bij uitval van het geautomatiseerde systeem de bedrijfsprocessen stilvallen. De getroffen maatregelen dienen in balans te zijn met het afbreukrisico van de uitval van het geautomatiseerde systeem. Te allen tijde dient voorkomen te worden dat (kritieke) bedrijfsgegevens niet meer terug te halen zijn na een verstoring.

De bevindingen zoals gerapporteerd in deze managementletter zijn gericht geweest op het beoordelen van de opzet en het vaststellen van het bestaan van algemene IT beheersmaatregelen. Op het moment dat intern niet voldoende maatregelen in het beheer van de systemen aanwezig zijn, zullen aanvullende (gegevensgerichte) werkzaamheden moeten worden uitgevoerd om aan te tonen dat er zich geen risico's of fouten hebben voorgedaan.

Voor 2017 zijn Key2Finance (financieel-administratief pakket), GISVG (Belastingen), ADP (Personeel) en Suites voor het Sociaal Domein (S4SD, voorheen GWS) in scope. De applicatie S4SD betreft een nieuwe applicatie in 2017. De beoordeling van deze applicatie is nog onder handen en wij zullen hierover op een later moment rapporteren.

5.2 Logische toegangsbeveiliging

	Bevindingen logische toegangsbeveiliging Toegangsbeveiliging en adequate functiescheiding in het geautomatiseerde systeem zijn belangrijke onderdelen van de interne beheersing van de gemeenten. Deze controlemaatregelen moeten waarborgen dat de controle technische functiescheiding ook in de IT-systemen wordt gewaarborgd. Uit onze controlewerkzaamheden zijn de volgende bevindingen naar voren gekomen:
Procedure autorisatiebeheer ontbreekt	- Procedures rond het gebruikersbeheer (in dienst komen en uit dienst gaan) zijn nog niet beschikbaar. - Door het ontbreken van voldoende vastleggingen in het proces van het verwerken van indiensttredingen en uit dienst gaan van medewerkers is het praktische proces niet controleerbaar. Hierdoor bestaat het risico dat de gebruikers in het systeem niet allen geautoriseerde medewerkers van de gemeente zijn. De personele bezetting van medewerkers die gebruik maken van GISVG is gedurende het jaar niet gewijzigd. - Een vastgelegde opzet van de vereiste autorisatie inrichting om de minimale controle technische functiescheidingen te kunnen waarborgen ontbreekt en vervult daarom ook geen rol in het autorisatiebeheer. Het risico bestaat dat gebruikers functie overschrijdende rechten in het systeem hebben waardoor controle technische functiescheidingen zouden kunnen worden doorbroken. - Een periodieke review op de actualiteit van gebruikersaccounts en de juistheid van hieraan toegekende rechten vindt niet plaats. Het uitvoeren van een periodieke review zou een compenserende maatregel kunnen zijn voor de eerder genoemde tekortkomingen in het gebruikers-en autorisatiebeheer.
Beheerrechten te ruim toegekend	- In GISVG en Key2Financiën zijn beheerrechten ruim toegekend. Hierdoor bestaat het risico dat onbewust of bewust wijzigingen aan de applicatie worden gemaakt waardoor fouten kunnen ontstaan in de administratie. - In principe krijgen gebruikers persoonsgebonden gebruikersaccounts. Er komen een aantal algemene gebruikersaccounts voor, waarvan enkel met kritieke rechten. De noodzaak van deze algemene gebruikersaccounts is niet in alle gevallen aangetoond.
Te veel unieke accounts **Authenticatiemaatregelen ontoereikend**	- Authenticatiemaatregelen die moeten waarborgen dat de gebruiker ook degene is die bij de gebruikersaccount hoort zijn niet in alle systemen voldoende aanwezig. Voor Key2Finance geldt dat wachtwoorden worden uitgegeven door de (functioneel) applicatiebeheerder, dit betreft een standaard wachtwoord. Gebruikers worden niet verplicht het wachtwoord bij eerste gebruik te wijzigen waardoor de mogelijkheid bestaat dat gebruikers onder een ander account inloggen. - Toegang tot ADP wordt door beheerders verkregen op basis van 2-factor authenticatie. Gebruikers moeten naast een gebruikersnaam/wachtwoordcombinatie tevens een unieke code invoeren op basis van een volgnummer welke account gebonden is. Voor reguliere gebruikers geldt dat het wachtwoord complexe tekens moet bevatten (hoofd- en kleine letters, getallen en symbolen) en periodiek gewijzigd dient te worden.
	De logische toegangsbeveiliging tot de systemen en de inrichting van de systemen laten tekortkomingen zien. In het bijzonder hebben die effect op de waarborgen voor controle technische functiescheidingen en de controleerbaarheid van de handelingen van gebruikers in de systemen. Wij stellen voor de uitkomsten voortkomend uit de IT-Audit in detail met u te bespreken zodat een concreet verbeterplan kan worden opgesteld. wij stellen voor concrete verbeteracties te benoemen m.b.t. de logische toegangsbeveiliging in het verbeterplan Balans 2018. Wij zullen dan aanvullende afspraken maken over het volgen van de verbeterstappen.

5.3 Wijzigingen- en continuïteitsbeheer

GISVG / Key2Financiën	Bevindingen wijzigingenbeheer Voor de kritieke systemen bij de gemeenten is sprake van standaardprogrammatuur met specifieke instellingen voor de gemeenten. Updates zijn standaard en worden door leveranciers aangeleverd. Het aantal updates is beperkt. • Formele procedurebeschrijvingen rond het beheer van wijzigingen ontbreken. • Er is geen formele procedure voor het plannen, uitvoeren en vastleggen van uitgevoerde testen. • De controleerbaarheid van het proces van wijzigingenbeheer is beperkt. • Er is wel een testomgeving aanwezig en wijzigingen worden (niet structureel) opgenomen in Topdesk. • Inzicht in wijzigingen enkel aan de hand van (technische) release notes, impactanalyses hierop door de gebruikersorganisaties zijn niet aantoonbaar. • Wijzigingen worden getest en geaccepteerd door de gebruikersorganisatie maar dit is niet aantoonbaar. • Autorisatie door de gebruikers voor de verplaatsing van test naar productie na acceptatie in niet volledig aantoonbaar.
ADP	Het beheer van wijzigingen laat tekortkomingen zien. De wijzigingen zijn standaard updates en beperkt in aantal. Daarentegen zijn de beheersingsmaatregelen zoals het testen van wijzigingen nog niet geborgd door uitgewerkte procedures en aantoonbare vastleggingen. Wij adviseren u deze processen meer te standaardiseren en zorg te dragen voor controleerbare vastleggingen. Het proces rondom wijzigingen aan ADP is uitbesteed aan deze partij, derhalve zal inzicht moeten worden verkregen in de beheersmaatregelen welke zij treft rondom het wijzigingsbeheer. ADP beschikt hiervoor over een assuranceverklaring waarin door een onafhankelijke partij de beheersmaatregelen in dit proces zijn getoetst.
Continuïteit	Bevindingen inzake continuïteit van de automatiseringsomgeving Continuïteitsmaatregelen beperken het risico dat bij uitval van het geautomatiseerde systeem de bedrijfsprocessen stilvallen. De getroffen maatregelen dienen in balans te zijn met het afbreukrisico van de uitval van het geautomatiseerde systeem. Te allen tijde dient voorkomen te worden dat (kritische) bedrijfsgegevens niet meer terug te halen zijn na een verstoring.
Verstoringen niet plaatsgevonden	Op basis van interviews met diverse applicatie-en technische beheerders hebben wij vastgesteld dat zich geen verstoringen met impact op de financieel-administratieve gegevensverwerking hebben voorgedaan. Gegevens en programmatuur worden via een cyclische back-up veilig gesteld. Afgelopen boekjaar is geen uitwijktest en restoretest uitgevoerd.

Bijlagen



Bijlage A: Reikwijdte en controleaanpak

BIJLAGE A: REIKWIJDTE EN CONTROLEAANPAK

REIKWIJDTE WERKZAAMHEDEN

In het kader van de door de raad aan ons verstrekte opdracht tot controle van de jaarrekening 2017 van de gemeente Hollands Kroon brengen wij u hierbij verslag uit van de belangrijkste bevindingen en aanbevelingen naar aanleiding van de tussentijdse controlewerkzaamheden die wij onlangs hebben uitgevoerd. De opdrachtvoorwaarden hebben wij met u afgestemd en vastgelegd in de opdrachtbevestiging d.d. 29 september 2017 met kenmerk “RB/SS/DR/AA17-1760”.

Bij de jaarrekeningcontrole maken wij mede gebruik van de administratieve organisatie en het daarvan deel uitmakende systeem van interne controle van uw gemeente. In dit verband hebben wij de opzet en bestaan van de administratieve organisatie op een aantal door ons noodzakelijk geachte punten onderzocht. Wij wijzen u erop dat onze controle niet was gericht op het vormen van een oordeel over de administratieve organisatie als zodanig. De in deze managementletter opgenomen bevindingen kunnen dan ook niet als limitatief worden beschouwd.

Onze werkzaamheden zijn erop gericht een oordeel te kunnen geven over de jaarrekening 2017 van de gemeente Hollands Kroon. Ze zijn niet primair gericht op het opsporen van fraudes of onregelmatigheden in uw organisatie. De bevindingen in deze brief zijn daarom beperkt tot de punten die voortvloeien uit de door ons uitgevoerde werkzaamheden. Indien onze werkzaamheden aanwijzingen hebben opgeleverd voor opgetreden fraudes of onregelmatigheden, dan hebben wij u daarover onmiddellijk gerapporteerd.

Bij onze controlewerkzaamheden hebben wij als uitgangspunt de door de raad vastgestelde toleranties gehanteerd. De raad heeft ons daarbij opgedragen om bij onze oordeelsvorming en rapportering uit te gaan van de hierna vermelde goedkeurings- en rapporteringstolerantie.

Goedkeuringstolerantie	Goedkeurend	Beperking	Oordeelsonthouding	Afkeurend
Fouten in de jaarrekening (% lasten)	≤ 1%	> 1% < 3%	-	≥ 3%
Onzekerheden in de controle (% lasten	≤ 3%	> 3% < 10%	≥ 10%	-

Op basis van de begroting 2017 van de gemeente Hollands Kroon betekenen bovengenoemde percentages dat een totaalbedrag aan fouten in de jaarrekening van € 950.000 en een totaal van onzekerheden van € 2,8 miljoen de goedkeurende strekking van de controleverklaring niet zullen aantasten. De rapporteringstolerantie is, zoals met u overeengekomen, gesteld op € 100.000. Onze controle richt zich tevens op de getrouwheid en rechtmatigheid van de informatie in de SiSa-bijlage van de jaarrekening. Voor SiSa gelden specifiek voorgeschreven rapporterings-toleranties die veelal lager zijn dan uw rapporteringstolerantie. Wij passen deze voorgeschreven SiSa-toleranties eveneens op correcte wijze toe.

bdo.nl

Nieuwe perspectieven

In de nieuwe economie doen kansen zich sneller voor dan ooit. Nieuwe spelregels geven een boost aan zakelijk werken. En een nieuwe generatie staat klaar om het anders te doen. Beter, slimmer, innovatiever. Wie succesvol wil ondernemen, moet zelf ook vernieuwen. Open staan voor verandering. En met open vizier kijken naar de mogelijkheden die voor ons liggen.

Nieuwe perspectieven, dát is wat BDO u wil bieden. En kan bieden, dankzij onze unieke combinatie van lokale marktkennis en een internationaal netwerk. Persoonlijke dienstverlening en een professionele aanpak. BDO helpt u graag om vanuit een andere invalshoek naar uw business te kijken. Zodat u de juiste beslissingen neemt om uw organisatie sterker, wendbaarder en succesvoller te maken. Of u nu een mkb-bedrijf, familiebedrijf, publieke organisatie of internationale onderneming bent.

BDO kijkt graag met u vooruit. Samen komen we tot nieuwe inzichten en nieuwe kansen in uw markt. Samen creëren we nieuwe perspectieven.

BDO Accountants & Adviseurs verleent vanuit 28 vestigingen in heel Nederland en met ruim 2.150 professionals diensten op het gebied van accountancy, belastingadvies en consultancy.
BDO adviseert ondernemingen in tal van branches en is sterk in de advisering aan het Nederlandse middenbedrijf, (semi-) overheidsinstellingen en familiebedrijven. Of het nu gaat om een controle van uw jaarrekening, de begeleiding van een ingewikkelde overname of een fiscaal advies op maat. In alle gevallen heeft u te maken met professionals. Zowel lokaal, regionaal, landelijk als internationaal. BDO maakt deel uit van het internationale BDO-netwerk (actief in 158 landen, meer dan 67.000 medewerkers wereldwijd) dat bestaat uit zelfstandige en onafhankelijke organisaties, die over de hele wereld onder de merknaam BDO actief zijn op het gebied van de zakelijke dienstverlening. Dat maakt ons in alle opzichten bijzonder betrokken. Kijk voor meer informatie op **www.bdo.nl**

All rights reserved 2017