

KOPIE



bakertilly

Managementletter

Hoogheemraadschap Hollands
Noorderkwartier
Boekjaar 2019

© Baker Tilly, 31 januari 2020

INGEKOMEN 03 FEB. 2020

Aan de directie van
Hoogheemraadschap Hollands Noorderkwartier
Postbus 250
1700 AG HEERHUGOWAARD

Breda, 31 januari 2020

Geachte directie,

Als onderdeel van de controle van de jaarrekening 2019 van het Hoogheemraadschap Hollands Noorderkwartier hebben wij de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing beoordeeld.

De opzet, het bestaan en de werking van de interne beheersingsmaatregelen van het personeelsproces, het betaalproces en het inkoopproces, in uw organisatie zijn beoordeeld en getoetst, zodat we een terugkoppeling kunnen geven over de betrouwbaarheid van de interne informatievoorziening en de jaarrekening.

Voor de overige processen ('aanbestedingen', 'belastingopbrengsten' en 'monitoring') geldt dat wij met name de opzet van de interne beheersing hebben beoordeeld en het bestaan hebben vastgesteld. In onze controleaanpak is het efficiënter om de transacties in deze processen grotendeels door gegevensgerichte werkzaamheden te controleren in plaats van door systeemgerichte werkzaamheden. Gedeeltelijk hebben we deze werkzaamheden reeds uitgevoerd tijdens de interim-controle.

De aanbevelingen met betrekking tot de inrichting van de digitale beheer omgeving van de applicaties en het netwerk zijn opgenomen in de bijlage bij deze rapportage.

Onze bevindingen zijn gebaseerd op de normale werkzaamheden in het kader van de jaarrekeningcontrole. Deze brief bevat daardoor niet alle onvolkomenheden in uw hoogheemraadschap, die bij een eventueel uitgebreid en hierop specifiek gericht onderzoek naar voren zouden kunnen komen.

Zoals u zult begrijpen, is de managementletter van nature kritisch. Wij rapporteren over de eventuele leemtes of mogelijkheden ter verbetering van de financiële en administratieve processen, de administratieve organisatie daarvan en de daarin opgenomen maatregelen van interne beheersing.

Op uw verzoek geven wij in deze managementletter aan op welke wijze verbeteringen van de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing kunnen worden gerealiseerd. De aanbevelingen en oplossingsrichtingen zoals beschreven in deze managementletter bieden u handvatten voor deze uitwerking.

Deze managementletter is door ons opgesteld voor uw informatie en mag niet zonder onze uitdrukkelijke toestemming geheel of gedeeltelijk aan derden ter beschikking worden gesteld.

Wij danken u en uw medewerkers voor de samenwerking en zijn graag bereid tot het verstrekken van nadere toelichting.

Hoogachtend,
Baker Tilly (Netherlands) N.V.

V.B. Damen RA

Inhouds- opgave

1. Management samenvatting	4
2. Attentiepunten jaareinde controle en overige aandachtspunten	9
3. Overige onderwerpen	12
 Bijlage	
Detailbevindingen	16

Management samenvatting

1. Management samenvatting

1.1 Inleiding



Deze managementletter bevat onze bevindingen in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2019. Ten behoeve van de jaarrekeningcontrole 2019 hebben wij in november 2019 kennis genomen van de opzet en het bestaan van de processen die ons inziens van belang zijn voor de jaarrekeningcontrole. Daarnaast hebben wij ook de werking van de maatregelen waar wij op willen steunen getoetst bij het proces personeel, inkopen en betalingen. In deze managementletter geven wij een terugkoppeling van onze bevindingen die wij tijdens deze controle geconstateerd hebben. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw hoogheemraadschap als geheel noch over het geven van een oordeel over de kwaliteit van de jaarrekening.

Wij wijzen u erop dat een managementletter van nature kritisch van aard is, omdat deze zich richt op te verbeteren aspecten binnen uw organisatie.

Administratieve Organisatie en Interne Beheersing

Voorgaande jaren hebben wij tijdens onze besprekingen met u diverse aanbevelingen benoemd ter verdere optimalisering van de bestaande administratieve organisatie. In deze managementletter geven wij u een schriftelijke update van onze bevindingen omtrent de interne beheersing.

Deze rapportage bevat de (significante) bevindingen en opmerkingen met betrekking tot de administratieve organisatie en interne beheersing.

Tijdens de interim-controle is aandacht besteed aan de volgende processen:

- Inkopen en aanbestedingen
- Betalingen
- Personeel
- Belastingen
- Monitoring

Van deze processen is de opzet beoordeeld en het bestaan vastgesteld. Daarnaast is de werking van de interne beheersingmaatregelen getest voor de inkopen, betalingen en personeel.

Bevindingen

In onderstaande tabel is een totaal overzicht opgenomen van het totaal aantal bevindingen:

	Bevindingen met prioriteit hoog	Overige Bevindingen
Aantal aanbevelingen uit voorgaande jaren	0	2
Waarvan opgelost in 2019	0	1
<i>Resterende aanbevelingen uit voorgaande jaren</i>	<i>0</i>	<i>1</i>
<i>Aantal nieuwe aanbevelingen</i>	<i>0</i>	<i>1</i>
Aantal openstaande aanbevelingen	0	2

De bevindingen en onze aanbevelingen worden in de bijlage bij deze managementletter in detail toegelicht.

1. Management samenvatting

1.2 Bevindingen interne beheersing



In onderstaand overzicht hebben wij onze bevindingen ten aanzien van de interne beheersing van de bedrijfsprocessen uiteengezet met daarbij de prioriteitstelling.

Nr.	Proces	Bevinding	Status	Prioriteit 2019	Prioriteit 2018
1	Personeel	Interne controle P&O		Laag	Laag
2	Automatisering	Wijzigingsbeheer en logische toegangsbeveiliging		Midden	Midden
3	Monitoring	Frauderisicoanalyse		Midden	

Legenda status:

-  = opgelost
-  = actie ondernomen, maar nog niet afgerond
-  = geen actie ondernomen
-  = Nieuwe bevinding

Toelichting prioriteit

- Prioriteit hoog: Bevinding op te lossen voor de jaarrekeningcontrole 2019
- Prioriteit midden: Bevinding op te lossen voor de jaarrekeningcontrole 2020
- Prioriteit laag: Bevinding op te lossen op lange termijn

1. Management samenvatting

1.3 Bevindingen op hoofdlijnen



Inkopen en aanbesteding

Vooruitlopend op de jaareinde controle hebben wij reeds een controle verricht op basis van de door u aangeleverde spendanalyse. De door ons gecontroleerde posten hebben niet geleid tot bevindingen die gerapporteerd zouden moeten worden in het kader van rechtmatigheid.

Betalingen

Tijdens de controle hebben wij vastgesteld dat de noodzakelijke functiescheidingen binnen het betaalproces toereikend aanwezig zijn.

Personeel en belastingen

Bij de controle van het personeelsproces en de belastingen hebben wij geen significatie bevindingen geconstateerd. Voor de overige bevindingen verwijzen wij naar de 'detailbevindingen interim-controle'.

Automatisering

De IT-audit activiteiten zijn in scope beperkt tot de applicatie Baseware en de onderliggende infrastructuur. Voor de applicaties CMS, Timeconnect en FIS2000 geldt dat deze op dit moment worden vervangen, derhalve zijn er geen wijzigingen in de interne beheersing ten opzichte van de situatie 2018 te melden. Wij hebben deze applicaties met het oog hierop niet meegenomen in deze managementletter.

De applicaties Key2Belastingen en Youforce komen anders dan voorgaand jaar, niet terug in deze managementletter. Wij maken voor de jaarrekeningcontrole geen gebruik van de interne beheersing in die applicaties. Wij hebben daarom, anders dan voorgaand jaar, minder uitgebreid onderzoek gedaan naar de interne beheersing van die applicaties.

Hoogwaterbeschermingsprogramma

Gezien de omvang en complexiteit van het Hoogwaterbeschermingsprogramma heeft u ons verzocht een tussentijdse review uit te voeren voor de projecten Markermeerdijken, Hoogwaterkering Den Oever en Waddenzeedijk Texel. Tijdens de tussentijdse review hebben wij de aangeleverde dossiers van Markermeerdijken, Hoogwaterkering Den Oever en Waddenzeedijk Texel beoordeeld en gesprekken gevoerd met medewerkers van uw organisatie.

Op grond de reeds door ons verrichte werkzaamheden concluderen wij dat de aangeleverde dossiers voldoen ten behoeve van de uitvoering van onze controle. De dossiers voor de jaareinde controle kunnen derhalve op dezelfde manier worden ingericht als bij de tussentijdse review.

Overige subsidiecontroles

Naast de verrichte werkzaamheden in het kader van het Hoogwaterbeschermingsprogramma hebben wij overige subsidies gecontroleerd. Het gaat hierbij met name om de controle van tussentijdse projectdeclaraties in het kader van het Europese subsidieprogramma Interreg. De door ons gecontroleerde en gecertificeerde projectdeclaraties geven geen aanleiding tot opmerkingen.

1. Management samenvatting

1.3 Bevindingen op hoofdlijnen



Frauderisicoanalyse

Vanuit maatschappelijk belang wordt het steeds belangrijker voldoende aandacht te besteden aan de beheersing van frauderisico's. De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude berust bij het College van Dijkgraaf en Hoogheemraden. Deze verantwoordelijkheid betreft ook het onderhouden van een zodanige interne beheersing om het opmaken van de jaarrekening mogelijk te maken zonder dat deze afwijkingen van materieel belang bevat als gevolg van fraude of fouten.

Op basis van onze uitgevoerde interim-controle hebben wij vastgesteld dat het hoogheemraadschap wel aandacht heeft voor frauderisico's en de preventie daarvan, maar niet beschikt over een actuele geformaliseerde frauderisicoanalyse. Wij achten het verstandig om intern een frauderisicoanalyse op te stellen en deze te formaliseren, ook met het oog op de ontwikkelingen rondom de rechtmatigheidsmededeling.

Voor de frauderisicoanalyse kunnen de volgende stappen worden onderkend:

- Uitvoeren van een organisatie-brede frauderisico inventarisatie, zodat een door de hele organisatie gedragen frauderisicoanalyse kan worden opgesteld.
- Voeren van een frauderisico discussie met het College en de Werkgroep Audit & Risk.
- Uitwerken van de getroffen beheersingsmaatregelen ter afdekking van onderkende frauderisico's.
- Identificatie van restrisico's en verbetermaatregelen treffen om waar nodig deze restrisico's af te dekken.

Naast het opstellen van deze analyse adviseren wij u ook om deze vervolgens te delen met de ambtelijke organisatie en de Werkgroep Audit & Risk, om daarmee zichtbaar te maken hoe het College fraude(risico's) heeft geanalyseerd en daarmee omgaat.

Attentiepunten jaareinde controle en overige aandachtspunten

2. Attentiepunten jaareinde controle en overige aandachtspunten



2.1 Planning jaareinde controle

In de weken 7 tot en met 9 van 2020 zal de jaareinde controle van de jaarrekening Hoogheemraadschap Hollands Noorderkwartier plaatsvinden. Belangrijk voor een goed controleproces is een tijdige en volledige oplevering van zowel de (concept) jaarrekening als het digitale balansdossier.

Wij verzoeken u het controledossier conform voorgaande jaren aan te leveren in het portaal van HHNK. Hierbij hebben wij afgesproken dat het mijlpalendossier wordt opgeladen nadat het eerste concept van de jaarrekening door uw organisatie op dit punt is beoordeeld.

2.2 Aanbestedingsrechtmatigheid

Ten behoeve van onze jaarrekeningcontrole hebben wij reeds een gedetailleerde en onderbouwde spendanalyse ontvangen. Wij vragen daarbij expliciet aandacht voor een toereikende analyse op alle uitgaven die gedurende de periode 2016-2019 hoger zijn dan € 221.000 (exclusief btw) en over 2019 hoger zijn dan € 55.250 (exclusief btw). Daarnaast vragen wij u om de inkopen met een lagere waarde die moeten voldoen aan het interne inkoopbeleid te analyseren. De opdrachten die boven het Europese drempelbedrag uitkomen controleren wij integraal. De controle op de naleving van het interne inkoopbeleid zullen wij middels een steekproef uitvoeren.

2. Attentiepunten jaareinde controle en overige aandachtspunten



2.3 WNT verantwoording

Wij verwachten dat u per jaareinde een analyse maakt van de WNT waarbij inzichtelijk wordt gemaakt, welke functionarissen vallen onder de WNT. Voor deze functionarissen dient op basis van het controleprotocol adequaat te worden onderbouwd, welke salariscomponenten (en op welke wijze) verantwoord dienen te worden in de WNT-verantwoording.

Wij vragen hierbij uw aandacht voor de nauwkeurigheid van de bedragen, maar ook voor de volledigheid (bijvoorbeeld inzake declaraties, welke niet via de salarisadministratie geboekt worden).

2.4 Structurele en incidentele baten en lasten

In de herziene notitie structurele en incidentele baten en lasten wordt het onderscheid tussen incidentele en structurele baten en lasten verduidelijkt, zodat de begrippen 'incidenteel' en 'structureel' meer eenduidig toegepast worden. Deze verduidelijking vindt in de notitie plaats door middel van een algemeen kader en diverse uitgewerkte (niet limitatieve) voorbeelden.

Wij vragen u bij het opstellen van de jaarrekening 2019 rekening te houden met de in de notitie opgenomen stellige uitspraken en aanbevelingen:

- Voor de in het overzicht van incidentele baten en lasten opgenomen posten is een nadere toelichting vereist.
- De Commissie BBV adviseert in de 'financiële verordening' (artikel 108 Waterschapswet) een grensbedrag op te nemen vanaf welke omvang incidentele baten en lasten afzonderlijk gespecificeerd worden in het overzicht van incidentele baten en lasten.
- De Commissie BBV adviseert het structureel begrotingssaldo te presenteren conform het voorbeeld in hoofdstuk 4 van de notitie.

Overige onderwerpen

3. Overige onderwerpen

3.1 Rechtmatigheidsverantwoording

Met ingang van boekjaar 2021 dienen gemeenten een rechtmatigheidsverantwoording van het College van burgemeester en wethouders op te nemen in de jaarstukken. Mogelijk gaat deze regelgeving in de toekomst ook gelden voor Waterschappen.

In deze verantwoording zal het College van Dijkgraaf en Hoogheemraden zelf verantwoording af leggen aan het College van Hoofdingelanden over het rechtmatig tot stand komen van de in de jaarrekening verantwoorde baten en lasten alsmede de balansmutaties, dat wil zeggen in overeenstemming met de begroting en met de relevante wet- en regelgeving, waaronder de interne verordeningen.

Deze verantwoording zal mogelijk onderdeel uit gaan maken van de jaarrekening van het hoogheemraadschap en als zodanig object van onderzoek worden voor de accountant in zijn opdracht om een getrouwheidsoordeel bij de jaarrekening af te geven. Het hoogheemraadschap zal de materialiteits- en rapporteringsgrens bepalen, mogelijk wel binnen een bepaalde wettelijke bandbreedte. Naar verwachting zal in het najaar van 2019 door het Ministerie van BZK en de Commissie BBV expliciet worden gecommuniceerd over de specifieke uitwerking voor gemeenten. Wij adviseren u om kennis te nemen van deze uitwerking; omdat dit voor Hoogheemraadschappen in de toekomst mogelijk in vergelijkbare vorm geïntroduceerd zal worden.

Wij kunnen ons voorstellen dat het belangrijk is voor het College van Hoofdingelanden, het College van Dijkgraaf en Hoogheemraden en de ambtelijke organisatie om duidelijkheid te krijgen over de invulling van ieders rol en verantwoordelijkheid en de eisen die (mogelijk) worden gesteld aan de interne beheersing om tot een rechtmatigheidsverantwoording te kunnen komen en met elkaar hierover het goede gesprek te hebben. Niet in de laatste plaats is het voor het College van Dijkgraaf en Hoogheemraden een nieuwe en expliciete verantwoordelijkheid. Daarbij is voor de portefeuillehouder Financiën mogelijk een coördinerende rol logisch, het is echter niet zijn zelfstandige verantwoordelijk, het voltallige College van Dijkgraaf en Hoogheemraden is verantwoordelijk. Op basis van onze visie als Baker Tilly én onze deelname aan landelijke overlegtafels inzake de rechtmatigheidsverantwoording ondersteunen wij uw hoogheemraadschap hier graag bij.

3.2 Verbijzonderde interne controle

De commissie Bedrijfsvoering, Auditing Decentrale Overheden (BADO) heeft begin 2019 een notitie uitgebracht over de verbijzonderde interne controle (VIC), waarbij inzicht wordt geboden in hoe de verbijzonderde interne controle kan worden ingericht en welke gevolgen dit heeft voor de mogelijkheden voor de controlerend accountant om hiervan gebruik te maken.

In de financiële verordeningen wordt een belangrijke rol gegeven aan het College van Dijkgraaf en Hoogheemraden. Het College van Dijkgraaf en Hoogheemraden moet jaarlijks zorgen voor een interne toetsing van de getrouwheid van de informatieverstrekking en de rechtmatigheid van de (financiële) beheers handelingen. Een beheerste bedrijfsvoering staat hierbij voorop en de VIC is daarvoor een instrument. Zo levert de VIC een belangrijke bijdrage aan het planning- en control instrumentarium en aan een betrouwbare informatievoorziening.

3. Overige onderwerpen

Uitgangspunt hierbij is een goed werkende bestuurlijke inrichting, risicomanagement, naleving van afspraken (plan, do, check en act) en toezicht op de invoering van verbetermaatregelen.

De externe accountant kan op vier mogelijke manieren gebruik maken van de VIC, namelijk als:

1. Instrument om de aanlevering van stukken aan de accountant te verbeteren;
2. Onderdeel van het interne beheersingskader om toezicht te houden op de uitvoering van interne beheersingsmaatregelen;
3. Interne beheersingsmaatregelen, waarop hij kan steunen bij zijn organisatiegerichte werkzaamheden;
4. Interne auditfunctie (IAF).

Praktisch gesproken dienen dan keuzes gemaakt te worden met betrekking tot de positionering, de omvang van de personele bezetting, de kwalificatie van de eindverantwoordelijke persoon en het kostenaspect. Dit moet afgewogen worden tegen de baten, in de vorm van een betere beheersing van de bedrijfsprocessen en de risico's. Er moet niet vanuit worden gegaan dat een investering in de VIC een evenredige besparing op zal leveren in de kosten van de controle door de accountant. De intern uitgevoerde controlewerkzaamheden kunnen immers geen volledige vervanging zijn van de eigen waarnemingen door de externe accountant. Daar staan echter ook andersoortige baten tegenover, in de vorm van een betere beheersing van bedrijfsprocessen en risico's.

Bij uw hoogheemraadschap is de VIC al goed ingeregeld levert een belangrijke bijdrage aan de internen beheersing.

3.3 Fraude- en integriteitsissues

Ten tijde van onze controlewerkzaamheden hebben wij vernomen dat naar aanleiding van een aanbestedingsprocedure mogelijke integriteitsissues bij u onder de aandacht zijn gebracht. Wij hebben kennis genomen van de casus, waarnaar u extern onderzoek hebt laten verrichten. Wij hebben begrepen dat de vervolgstappen nog in het proces van afwikkeling zitten.

Bovengenoemde casus geeft ons geen aanleiding voor aanvullende werkzaamheden voor de inkoop- en aanbestedingsprocedure.

3. Overige onderwerpen

3.4 Verduurzaming maatschappelijk vastgoed

Vanwege het klimaatbeleid van overheden en vanwege wettelijke regels moeten overheidsorganisaties verduurzamen. Dat heeft onder andere consequenties voor het maatschappelijk vastgoed dat Waterschappen in bezit hebben. Een voorbeeld van nieuwe regels: per 1 januari 2023 wordt voor elke kantoorruimte groter dan 100 m2 een energielabel van minimaal C verplicht.

Overheidsgebouwen hebben volgens de Europese richtlijn EPBD een voorbeeldfunctie. Daarom moeten nieuwe overheidsgebouwen bij aanvraag van de omgevingsvergunning sinds 1 januari 2019 al aan de BENG-eisen voldoen. BENG staat voor bijna energie neutrale gebouwen. Voor alle overige nieuwbouw (woningbouw en utiliteitsbouw) geldt dat vanaf 1 juli 2020.

De verduurzamingsopgave stelt aanvullende eisen aan de onderhoudsbegroting van gebouwen. Dit vraagt het opstellen van een goed onderbouwd Meerjarenonderhouds-, -investerings- en -duurzaamheidsplan (MJOIDP).

Wij adviseren u naar aanleiding van deze wetgeving extra aandacht te besteden aan het MJOIDP en de mogelijke vorming van een voorziening te heroverwegen.

3.5 Geprognosticeerde balans en EMU-saldo

De nieuwe notitie geprognosticeerde balans en EMU-saldo bevat handreikingen voor het opstellen van de geprognosticeerde (meerjaren)balans en voor de wijze van berekenen van het EMU-saldo. In de notitie wordt onder meer duiding gegeven aan de betekenis voor leden van het College van Hoofdingelanden en andere bestuurders: de bedoeling om meer naar toekomstige ontwikkelingen te kijken en eerder signalen af te geven om daardoor zo nodig bij te sturen. Zo geven de verschillende posten van de geprognosticeerde balans het CHI meer inzicht in de verwachte ontwikkeling van de financiële positie, het risicoprofiel van de financiële positie (risico's van investeringen en schuldportefeuille) en de mate van flexibiliteit van de exploitatie(begroting). Meer investeringen en schulden betekenen immers ook structureel hogere vaste afschrijvings- en rentelasten en meer risico's die samenhangen met de investeringen en schuldportefeuille.

Het EMU-saldo kan gezien worden als een extra financieel kengetal. Het EMU-saldo geeft namelijk in één oogopslag aan of het waterschap via reële transacties netto geld uitgeeft, of dat er netto geld binnenkomt. Het EMU-saldo van één jaar zegt relatief weinig. Het hoogheemraadschap werkt met grote investeringen over de jaren heen. De inkomsten en uitgaven hebben effect op het structurele EMU-saldo. Bij een structureel positief of negatief EMU-saldo is het verstandig de vinger aan de pols te houden en een goede toelichting te geven.

Ondanks dat de notitie geprognosticeerde balans en EMU-saldo niet verplicht is in de BBV-W kan het EMU saldo worden gezien als een extra kengetal. Wij adviseren u om, evenals voorgaande jaren, goed te onderbouwen waarom het EMU-saldo een overschot vertoont.

Bijlage Detailbevindingen

Detailbevindingen interim-controle

Uitleg opbouw management letter



In deze bijlage zijn de detailbevindingen opgenomen. Per bladzijde van deze bijlage is een bevinding opgenomen met daarbij het risico en een aanbeveling. Bij elke bevinding staat het boekjaar van de eerste vermelding aangegeven. Bij de prioriteit staat de mate van belangrijkheid en urgentie (hoog, gemiddeld, laag).

Boekjaar	Prioriteit	De kleur van de het symbool geeft de status van de constatering aan.		
Boekjaar eerste vermelding	Urgentie en belang van de bevinding	● = opgelost	● = actie ondernomen, maar nog niet afgerond	
		● = geen actie ondernomen	● = Nieuwe bevinding	
Bevinding /risico/aanbeveling / commentaar management				
<i>Bevinding</i> In dit blok wordt aangegeven wat gedurende de accountantscontrole is geconstateerd en waarvan wij u graag op de hoogte willen brengen.	<i>Risico</i> Hierbij geven wij aan wat de risico's zijn van de bevinding en wat de gevolgen voor uw onderneming kunnen zijn.	<i>Aanbeveling</i> Hier geven wij u aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.		

Update 2019:

In dit blok wordt een update gegeven van de status van de bevindingen uit voorgaande jaren.

Detailbevindingen interim-controle

Bevinding 1	Interne controle P&O			
Jaar van constatering:	2018 ●	Proces:	Personeel	Prioriteit: Laag

Bevinding

Jaarlijks wordt er door een medewerker P&O een interne controle uitgevoerd op de mutaties die plaatsvinden binnen het personeelsbestand. Tevens vinden geautomatiseerde controles plaats binnen de applicatie Youforce van Raet.

Risico

Het risico dat de controle zowel geautomatiseerd alsook handmatig worden uitgevoerd, waardoor inefficiëntie in het proces ontstaat.

Overigens is bovenstaande voor de accountantscontrole geen risico, omdat wij geen hiaten hebben geconstateerd in de uitgevoerde interne controle.

Aanbeveling en gevolgen jaarrekening

Vorig jaar hebben wij u geadviseerd te onderzoeken of er handmatige controles zijn die ook reeds geautomatiseerd plaatsvinden. Wij hebben u hierbij in overweging gegeven de interne controle door P&O opnieuw in te richten om een efficiëntievoordeel binnen uw organisatie te behalen.

Update 2019

Van de afdeling P&O hebben wij begrepen dat de controles die worden uitgevoerd zijn geëvalueerd en waar nodig opnieuw ingericht. De bevinding van 2018 is opgelost.

Detailbevindingen interim-controle

Bevinding 2	Wijzigingsbeheer en logische toegangsbeveiliging			
Jaar van constatering:	2018	Proces:	ICT	Prioriteit: Laag

Bevinding

Wijzigingsbeheer

Wijzigingen in rechten in de applicatie worden niet gelogd. De inrichting van rollen en rechten in het systeem wordt periodiek beoordeeld. Voor de toewijzing van accounts aan rollen wordt gebruik gemaakt van spreadsheets.

Logische toegangsbeveiliging

Het wachtwoordbeleid van de Windows Active Directory voldoet niet aan de best practices voor het toepassen van een goed wachtwoordbeleid, doordat er geen complexiteit wordt afgedwongen. Wij hebben daarnaast vastgesteld dat er voor een groot aantal accounts, waaronder accounts met hoge rechten, is ingesteld dat het wachtwoord niet verloopt.

Risico

Wijzigingsbeheer

Het risico bestaat dat het de spreadsheets geen juist en volledig beeld geven van de rechten in de applicatie.

Logische toegangsbeveiliging

Het risico bestaat dat wachtwoorden met hoge rechten bekend worden bij andere medewerkers, waarmee ongeautoriseerde wijzigingen worden doorgevoerd.

Aanbeveling en gevolgen jaarrekening

Wijzigingsbeheer

Vorig jaar hebben wij u geadviseerd om voor alle wijzigingen in applicaties een centraal bepaald proces te volgen, waarbij minimaal wordt getest of hoofdcomponenten van de applicatie nog naar behoren werken en dit toetsbaar vast te leggen.

Voor de netwerkomgeving wordt gewerkt aan controles op basis van Identity Access Management (IAM), echter dit is nog niet volledig geïmplementeerd.

Logische toegangsbeveiliging

Wij adviseren wachtwoorden te voorzien van complexiteitseisen en het wijzigingen van wachtwoorden periodiek af te dwingen.

Update 2019

De aanbevelingen m.b.t. wijzigingsbeheer en logische toegangsbeveiliging zijn waar mogelijk opgevolgd. Gedeeltelijk moet dit nog worden geïmplementeerd, omdat HHNK overstapt naar een nieuw systeem.

Detailbevindingen interim-controle

Bevinding 3	Frauderisicoanalyse			
Jaar van constatering:	2019	Proces:	Monitoring	Prioriteit: Midden

Bevinding

Tijdens de controle hebben wij vastgesteld dat recent geen frauderisicoanalyse opgesteld is.

Wel is er een Intern Control Framework (ICF) beschikbaar waarin Risico's zijn gekoppeld aan beheersdoelstellingen, beheersmaatregelen en proceseigenaren. Fraude wordt hierin niet expliciet benoemd. Op basis van interviews hebben we begrepen dat het ICF hiervoor wel wordt gebruikt.

Risico

Mogelijke frauderisico's of gelegenheden tot fraude worden niet tijdig herkend.

Aanbeveling en gevolgen jaarrekening

Wij adviseren u om periodiek de frauderisico's te analyseren en na te gaan of de aanwezige interne beheersmaatregelen voldoende zijn om deze risico's te ondervangen.

Op basis van onze bevindingen bij de interim-controle en onze ervaringen van de controle voorgaand boekjaar zullen wij evalueren of er frauderisico's zijn en hoe deze ondervangen worden.

Contactgegevens

V.B. (Barry) Damen RA

Partner

M: 06 – 55 88 54 32

E: b.damen@bakertilly.nl

L.J. (Louw-Jan) Feitsma RA

Manager

M: 06 – 10 14 34 14

E: l.feitsma@bakertilly.nl

Kantoorgegevens:

Baker Tilly (Netherlands) N.V.

Bijster 39

Postbus 3814

4800 DV BREDA

T: 076 – 525 00 00





Bijlage 1 - Bevindingen IT-beheersing

Algemeen

Voor u ligt het onderdeel van de managementletter dat gebaseerd is op de IT-auditwerkzaamheden die in het kader van de jaarrekeningcontrole over het boekjaar 2019 zijn uitgevoerd. In dit onderdeel van de managementletter staat welke IT-audit activiteiten door ons zijn uitgevoerd en wat onze bevindingen zijn voor de controle.

De IT-audit activiteiten zijn in scope beperkt tot de applicatie Basware en de onderliggende infrastructuur. Voor de applicaties CMS, Timeconnect en FIS2000 geldt dat deze op dit moment worden vervangen, derhalve zijn er geen wijzigingen in de interne beheersing ten opzichte van de situatie in 2018 te melden. Wij hebben deze applicaties met het oog hierop niet meegenomen in deze managementletter.

De applicaties Key2Belastingen en Youforce komen, anders dan vorig jaar, niet terug in deze managementletter. Wij maken voor de jaarrekeningcontrole geen gebruik van de interne beheersing in die applicaties. Wij hebben daarom, anders dan vorig jaar, minder uitgebreid onderzoek gedaan naar de interne beheersing van die applicaties.

IT General Controls

Veel handelingen die binnen organisaties plaatsvinden, worden geregistreerd door middel van automatisering. Daarbij zijn diverse interne beheersingsmaatregelen steeds vaker geautomatiseerd in softwarepakketten. Wij onderzoeken daarom de algemene onderwerpen rondom de beheersing van uw IT-omgeving en rapporteren daarover in de navolgende pagina's.

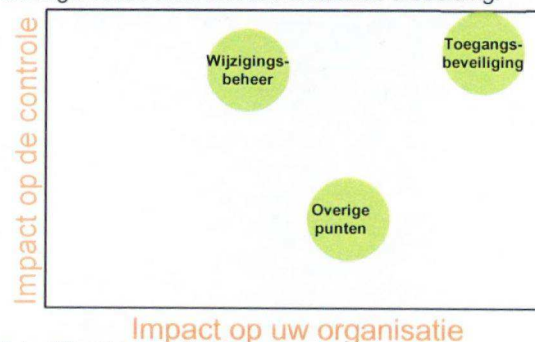
Werkzaamheden

Op basis van de door ons uitgevoerde werkzaamheden hebben wij onze inschatting van de kwaliteit van uw IT systeem en/of applicatie opgenomen. Hierbij hebben wij de volgende onderverdeling gemaakt om de kwaliteit weer te geven:

- Op dit moment voldoende
- Verbetering gewenst
- Verbetering benodigd

Let op: de onderwerpen die niet gerelateerd zijn aan toegangsbeveiliging en wijzigingsbeheer volgen uit interviews en hierop zijn door ons over het algemeen geen testwerkzaamheden uitgevoerd om vast te stellen dat de IT-omgeving is ingericht zoals ons voorgesteld is. Dit beperkt de zekerheid die u kunt ontleen aan de door ons beschreven aandachtspunten.

De mate van risico die u als organisatie loopt bij constatering verschilt per aandachtsgebied. Een grafische inschatting van de impact op de controle en op uw organisatie vindt u in onderstaande afbeelding.



© Baker Tilly, 31 januari 2020

Logische toegangsbeveiliging

Bij het toetsen van 'logische toegangsbeveiliging' wordt onderzocht of de inrichting van de IT-omgeving de authenticiteit van de gebruiker van een gebruikersaccount borgt. Ook onderzoeken wij de mogelijkheden voor het 'steunen' op autorisaties en de processen rondom het verstrekken, muteren en ontnemen van autorisaties binnen de omgeving en de applicaties. Wanneer de randvoorwaarden hiervoor voldoende aanwezig zijn, kunnen wij gebruik maken van eventuele functiescheiding dat in de omgeving of de applicatie is geïmplementeerd.

Wijzigingsbeheer (Change management)

Het doel van 'wijzigingsbeheer' is borgen dat wijzigingen aan de applicatie op een gestructureerde en gecontroleerde wijze worden doorgevoerd. Voor uw organisatie heeft wijzigingsbeheer ten doel om te voorkomen dat applicaties zich niet gedragen zoals u na een wijziging in de software, resulterend in, wellicht niet opgemerkte, (financiële) gevolgen.

Overige punten zonder directe impact

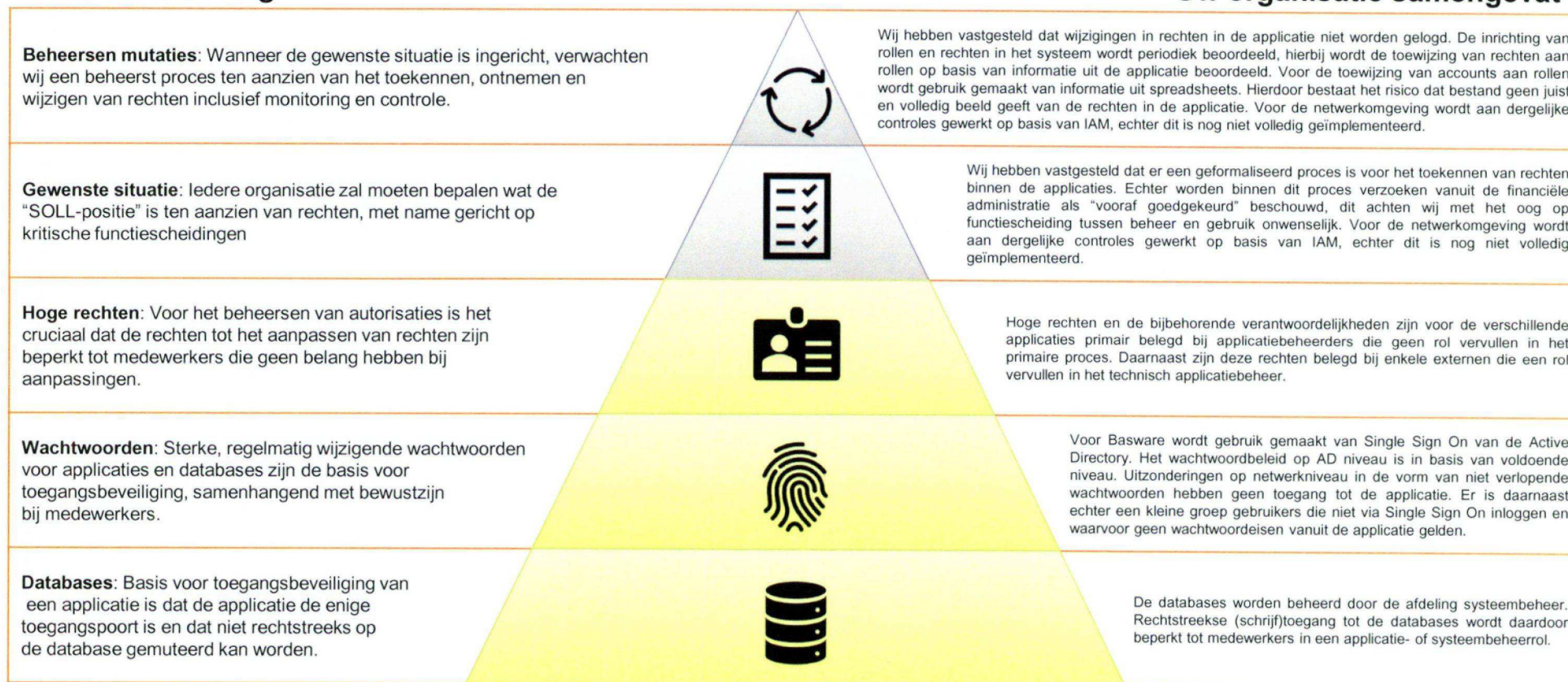
Het is ons van belang om inzicht te krijgen in de verantwoordelijkheden die binnen de organisatie zijn ingericht – of met andere organisaties overeen zijn gekomen (uitbesteding) – ten aanzien van de beheersing van de IT-omgeving. Hierbij kijken wij naar beleidsstukken ten aanzien van IT-strategie, beveiliging en functiescheiding. Ook de interne beheersingsmaatregelen die al dan niet zijn ingericht binnen de IT-omgevingen zijn onderdeel van onze scope. Indien maatregelen periodiek worden uitgevoerd kunnen wij hier gebruik van maken in de jaarrekeningcontrole. Deze adviespunten hebben niet een directe impact op onze controlewerkzaamheden, maar zijn wel wenselijk.

Logische toegangsbeveiliging

Wij onderscheiden vijf bouwstenen ten aanzien van toegangsbeveiliging, waarbij bouwstenen gestapeld, naast een sterke IT-beheersing, ook de meeste controlezekerheid oplevert. Beperkingen in de onderliggende steen, zorgt voor een verzwakking van de bovenliggende stenen. Een toelichting:

Onze verwachting

Uw organisatie samengevat



Wijzigingsbeheer

Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat het proces voor wijzigingen een proces doorloopt, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden. Wij hebben onderstaand aangegeven wat wij verwachten per fase en wat wij hebben geconstateerd tijdens onze controle (deels op basis van interview) en of dit overeen komt met de verwachting. Onder wijzigingen verstaan wij niet alleen nieuwe versie updates, maar ook aanpassingen in (kritieke) systeemconfiguraties.

2. Opstellen testplan en -aanpak:

Vanuit de geïdentificeerde risico's kan een testplan worden gemaakt waarin de te testen elementen van de software benoemd zijn evenals de inhoudelijk uit te voeren testwerkzaamheden op deze elementen. Belangrijke elementen hierin zijn go/nogo momenten, het maken van een back up voor implementatie, wat te doen als een implementatie mislukt en de impact op de organisatie (opleiden van medewerkers)

Uw situatie:

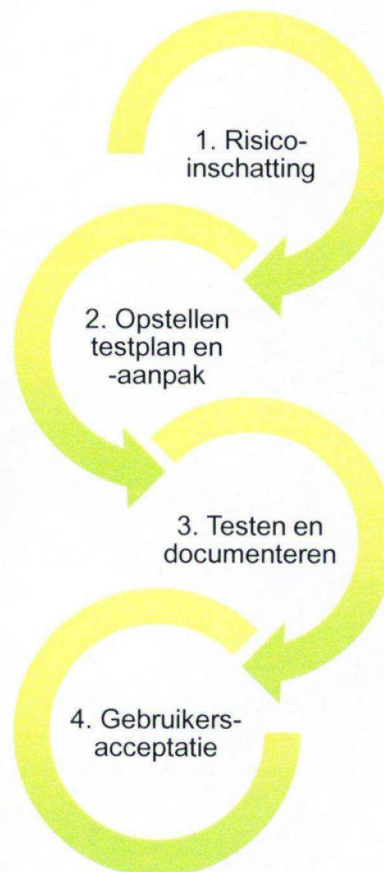
Aan de hand van de beschrijving van de wijziging dan wel releasenotes wordt per wijziging bepaald welke testaanpak er gekozen dient te worden en wordt deze testaanpak uitgevoerd. Dit proces is vastgelegd in een procedure.

4. Gebruikersacceptatie:

Een wijziging is pas effectief als deze niet alleen is geaccepteerd vanuit een technisch oogpunt, maar ook vanuit de gebruikersorganisatie. Wij verwachten daarom een formele goedkeuring vanuit de gebruikersorganisatie, zowel voor implementatie als na de implementatie

Uw situatie:

Wijzigingen worden geaccordeerd door de gebruikersorganisatie alvorens deze in productie worden gebracht. Voor maatwerkwijzigingen wordt dit akkoord in het ticketsysteem gegeven. Voor updates is nog geen centrale registratie tool beschikbaar.



© Baker Tilly, 31 januari 2020

1. Risico-inschatting:

Voor iedere software wijziging is het relevant om te beoordelen wat de risico's zijn die de wijziging met zich mee brengt voor de hoofdprocessen én welke geïdentificeerde technische en organisatorische wijzigingsrisico's worden geraakt bij het uitvoeren van de change, waaronder maatwerk. Per wijziging wordt vastgesteld welke nieuwe of gewijzigde functionaliteit een risico vormt voor een goede werking van uw bedrijfsvoering.

Uw situatie:

Voor maatwerkwijzigingen wordt een specificatie opgesteld en vastgelegd van de uit te voeren wijziging. Voor updates geldt dat op basis van de wijzigingen wordt bepaald welke testwerkzaamheden uitgevoerd moeten worden.

3. Testen en documenteren:

Softwarewijzigingen kunnen gestructureerd worden getest, na het correct uitvoeren van de voorgaande twee stappen. Een vastlegging van testwerkzaamheden is van belang voor de aantoonbaarheid en controleerbaarheid van de uitgevoerde stappen.

Uw situatie:

De voorgenomen testwerkzaamheden worden uitgevoerd en gedocumenteerd. Voor maatwerkwijzigingen vindt deze vastlegging plaats in het ticket systeem. Voor updates is nog geen centrale registratie tool beschikbaar.

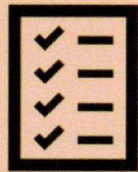
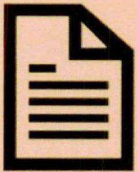
IT adviespunten zonder directe impact op de controle

Beleid en plannen

Beleid

Binnen uw organisatie is een uitgewerkt IT-beleidsplan aanwezig, waarin de uitgangspunten voor IT-beheer en ontwikkelingen zijn beschreven. Het is daardoor mogelijk om monitoring op basis van een plan-do-check-act cyclus toe te passen binnen uw organisatie.

Er zijn in het afgelopen jaar daarnaast stappen gemaakt om op het gebied van informatiebeveiliging een volgend "volwassenheidsniveau" te bereiken. Hiervoor wordt uitgegaan van de BIO, waarbij een jaarplan is opgesteld om invulling te geven aan deze ambitie.



Verantwoordelijkheden en functiescheiding

Wij verwachten dat binnen uw organisatie duidelijke afspraken zijn gemaakt ten aanzien van verantwoordelijkheden over uitvoering en strategie op het gebied van IT. Binnen uw organisatie zijn gebruik, aansturing en beheer van applicaties en infrastructuur doorgaans gescheiden belegd. Het beheer van de technische infrastructuur is hierbij gedeeltelijk uitbesteed.

De afspraken hieromtrent zijn vastgelegd in overeenkomsten met de leveranciers. Er zijn echter nog geen formele en toetsbare processen om het nakomen van deze afspraken door de leveranciers, als onderdeel van de regiefunctie, periodiek te evalueren.

Uitvoering

Beheersing van incidenten

Om de performance van uw IT-systemen en eventueel de performance van uw IT-dienstverlener te monitoren, is registratie van de incidenten en problemen van belang. Hierdoor verkrijgt u inzicht in de performance van uw systemen, maar ook van uw IT-organisatie en kunt u waar nodig uw beleidsplan corrigeren.

Binnen uw organisatie worden incidenten centraal geregistreerd en verholpen door de afdeling ICT en/of de applicatiebeheerders. Waar nodig schakelen zij de hulp in van de diverse leveranciers.

Uitvoering beheersingsmaatregelen IT

Op verschillende vlakken worden (nog) geen toetsbare beheersingsmaatregelen uitgevoerd binnen uw organisatie. Denk aan:

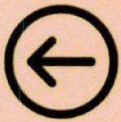
- Periodieke controle op actieve gebruikers in de applicaties en op het netwerk.
- Periodieke controle op inrichting van wachtwoordbeleid.
- Periodieke controle op inrichting van rechten in het systeem conform beleid.

Wij hebben vernomen dat op deze gebieden wel werkzaamheden worden verricht door diverse medewerkers, maar dat deze werkzaamheden niet zichtbaar worden vastgelegd. Hierdoor is de uitvoering voor ons niet toetsbaar.

Deze procedures en daaruit volgende controlemaatregelen zorgen ervoor dat uw organisatie grip houdt op de IT-omgeving en faciliteren dat de randvoorwaarden, die de effectiviteit van ingerichte beheersingsmaatregelen beïnvloeden, van voldoende niveau zijn.

IT adviespunten zonder directe impact op de controle

Continuïteitsmaatregelen



Recovery Point Objective (RPO): De RPO is het punt in de tijd tot waar men minimaal de gegevens moet kunnen herstellen. Het is dus de acceptabele hoeveelheid aan dataverlies uitgedrukt in tijd.

Back-ups: Er worden met verschillende diepgang en tijdsintervallen back-ups gemaakt. Hiervoor wordt gebruik gemaakt van diverse geautomatiseerde tools.



Recovery Time Objective (RTO): Een RTO is de tijd waarna een proces/middel na een onderbreking moet teruggebracht zijn op een aanvaardbaar niveau, om een onacceptabele impact op de organisatie te vermijden

Recovery: Er is geen formeel proces om de volledige back-up op werking te testen. De database back-ups van de belangrijkste applicaties worden echter wel periodiek teruggezet om te beoordelen in hoeverre deze op een juiste manier gemaakt zijn.

Uitwijk: Er is een uitwijkomgeving beschikbaar doordat de IT-infrastructuur redundant uitgevoerd is.

Beveiliging

Beveiliging

De beveiliging van de IT-omgeving delen wij op in verschillende aspecten, welke wij hieronder hebben weergegeven.

Fysieke beveiliging: De serverruimte is voorzien van diverse beveiligingsmaatregelen ten aanzien van temperatuur, klimaat en brandrisico's. Daarnaast wordt fysieke toegang tot de kantooromgeving van het HHNK, alsmede specifieke ruimtes binnen de kantooromgeving, beheerst op basis van toegangspassen.

Remote access: Voor het extern inloggen wordt gebruik gemaakt van extra beveiligingsmaatregelen, in de vorm van twee factor authenticatie. Hierdoor is de omgeving aanvullend beveiligd tegen ongeautoriseerd inloggen van buiten de kantooromgeving.

Preventie: Een firewall is aanwezig en wordt actief beheerd door de leverancier, Kahuna. Daarnaast wordt er gebruik gemaakt van meerdere anti-virus / malware oplossingen.

Monitoring: Er heeft in het afgelopen jaar een attack- en penetration test plaatsgevonden. Daarnaast wordt de omgeving periodiek en automatisch gescand op kwetsbaarheden.

