

Managementletter

Hoogheemraadschap Hollands

Noorderkwartier

Boekjaar 2020

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

Amsterdam, februari 2021

Geachte directie,

Als onderdeel van de controle van de jaarrekening 2020 van het Hoogheemraadschap Hollands Noorderkwartier hebben wij de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing beoordeeld, teneinde onze controlewerkzaamheden in overeenstemming met Nederlands recht waaronder de controlestandaarden te kunnen bepalen.

De opzet en het bestaan 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' en 'belastingopbrengsten') 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 hoofdstuk 3 van 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 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.

Wij geven 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.

Met vriendelijke groet,
Baker Tilly (Netherlands) N.V.

Was getekend

drs. J.M.A. Drost RA

Inhouds- opgave

1. Management samenvatting	4
2. Attentiepunten jaareinde controle en overige aandachtspunten	9
3. Bevindingen IT-Beheersing	12

Bijlage

Detailbevindingen	17
-------------------	----

Management samenvatting

1. Management samenvatting

1.1 Inleiding

Inleiding

Het kalenderjaar 2020 zal de geschiedenisboeken ingaan als een bewogen jaar waarin de COVID-19 pandemie de dagelijkse gang van zaken domineert. Het feit dat we een crisis van deze omvang in de recente historie nog niet eerder hebben meegemaakt als ook de onbekende duur, leidt tot onzekerheden en onduidelijkheden.

De crisis heeft niet alleen een financiële impact – COVID-19 heeft geleid tot het grootste landelijke begrotingstekort ooit - maar ook een belangrijke operationele impact. Ambtenaren zijn lange tijd niet bij het hoogheemraadshap aanwezig geweest, externe overleggen zijn uitgesteld. Ondanks de crisismaatregelen heeft het reguliere beleid goed doorgang gevonden. Ook financieel gezien voelt uw hoogheemraadschap in 2020 en vermoedelijk ook verder, de impact van COVID-19. Daarbij valt te denken aan hogere lasten vanwege wijzigingen in de werksituatie of lagere baten belastingopbrengsten. Deze zaken hebben hun weerslag op uw planning & controlcyclus en daarmee mogelijk ook het proces van de jaarrekeningcontrole en de daarvoor afgesproken deadlines. Uw waterschap is qua informatievoorziening deels afhankelijk van derden voor het opstellen en onderbouwen van de jaarstukken. Mogelijk leveren deze partijen later aan en waarschijnlijk dienen er aanvullende werkzaamheden uitgevoerd te worden, die inherent zijn aan dit crisisjaar.

Wij adviseren u tijdig een inventarisatie te maken welke gevolgen Corona op uw interne planningsproces aangaande de jaarrekening heeft en in welke mate u daarin afhankelijk bent van informatie vanuit derden. Op basis van deze analyse is het zaak om de bestuurlijke planning van het jaarrekeningproces te bepalen.

Aandachtspunten controle 2020

Wij identificeren een aantal aandachtspunten voor de jaarrekeningcontrole 2020. Naast de aandachtspunten die voortvloeien uit onze reguliere risicoanalyse en interim-controle, zien deze ook toe op de gevolgen van COVID-19 op de interne beheersing, prestatielevering inkopen en de voorbereiding op de rechtmatigheidsverantwoording. Deze belangrijkste aandachtspunten lichten we verderop in dit verslag uitgebreid toe.

Algemeen

De bevindingen in deze managementletter zijn gebaseerd op basis van de bevindingen van de interne controle en onze eigen waarnemingen en lijncontroles.

Wij constateren dat uw organisatie aandacht heeft voor de bevindingen die wij voorgaand jaar constateerden. Tijdens de controle hebben wij gesignaleerd dat bevindingen opgepakt zijn, maar nog niet volledig afgewikkeld zijn. Wij vragen uw aandacht voor de afwikkeling van deze eerder geconstateerde bevindingen.

Risicoanalyse

Onze risicoanalyse richt zich op een betrouwbare totstandkoming van de jaarrekening. Dit betekent dat wij niet alle risico's die voor u als waterschap relevant zijn in onze controle meenemen. De risicoanalyse is een continue proces en stellen wij gedurende de controle indien nodig bij.

De belangrijkste bij uw waterschap onderkende risico's / kernpunten in de controle zijn:

- Aanbestedingsrechtmatigheid;
- Onterechte handmatige betalingen.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten.

1. Management samenvatting

1.1 Inleiding

Frauderisicoanalyse

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude berust bij het dagelijks bestuur. 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 uw hoogheemraadschap veel aandacht heeft voor frauderisico's en de preventie daarvan.

Voorgaand jaar hebben wij in onze managementletter gerapporteerd dat uw hoogheemraadschap niet beschikt over een actuele geformaliseerde risicoanalyse. Het afgelopen boekjaar heeft u hier opvolging aan gegeven door een brainstormsessie te houden om te bepalen hoe deze frauderisicoanalyse aangepakt kan worden. Uit het gespreksverslag dat hiervan is opgesteld blijkt dat u de frauderisico's heeft besproken op basis van de fraudedriehoek en risico's en beheersmaatregelen inzichtelijk hebt gemaakt.

Op basis van interviews hebben we vernomen dat P&O inmiddels is begonnen met een inventarisatie risicovolle functies vanuit het integriteitsbeleid (en fraude). Tevens worden de uitkomsten van de brainstormsessie meegenomen in de nieuwe 3 lines of defence interne beheersing discussie. Met daaruit volgend een nieuw Interne Controleplan voor de komende jaren waarin ook VIC beter wordt geborgd. U heeft een projectgroep samengesteld die hieraan werkt.

Ook staat bij de klankbordgroep audit en risico risicomanagement op de agenda, waarin ook het element fraude wordt betrokken. Wij hebben vernomen dat de klankbordgroep audit en risico hieraan in januari 2021 verdere opvolging geeft.

Op basis van het verslag van de brainstormsessie en de verkregen toelichting daarbij constateren wij dat uw risicoanalyse zowel toeziet op beleid en randvoorwaarden en ingaat op frauderisico's binnen de bedrijfsprocessen van het hoogheemraadschap. Mede in het kader van de rechtmatigheidsverantwoording adviseren we u deze lijn in de algehele herinrichting van uw verbijzonderde interne controleaanpak voort te zetten.

1. Management samenvatting

1.1 Inleiding

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.

Van deze processen is de opzet beoordeeld en het bestaan vastgesteld. Daarnaast is de werking van de interne beheersingsmaatregelen 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	1	1
Waarvan opgelost in 2020	0	0
<i>Resterende aanbevelingen uit voorgaande jaren</i>	<i>1</i>	<i>1</i>
<i>Aantal nieuwe aanbevelingen</i>	<i>0</i>	<i>0</i>
Aantal openstaande aanbevelingen	1	1

De overige bevinding wordt in de bijlage bij deze managementletter in detail toegelicht. Voor de bevinding(en) op het gebied van automatisering verwijzen we naar hoofdstuk 3 van deze managementletter.

1. Management samenvatting

1.2 Bevindingen op hoofdlijnen

Inkopen en aanbesteding

Ten behoeve van onze jaarrekeningcontrole hebben wij reeds een gedetailleerde en onderbouwde spendanalyse ontvangen. Ter voorbereiding op onze controle op de aanbestedingsrechtmatigheid hebben wij u een werkprogramma verstrekt. Uw organisatie heeft dit werkprogramma voor het eerste tot en met het derde kwartaal 2020 reeds voorbereid ten behoeve na onze controle over het hele boekjaar.

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 applicaties die gerelateerd zijn aan financiële stromen en processen, en daarmee samenhangende (netwerk)infrastructuur. Voor een uitwerking van onze bevindingen met betrekking tot deze applicaties verwijzen wij naar hoofdstuk 3 van deze managementletter. De belangrijkste constatering hierbij is dat er binnen de applicatie UBW geen wachtwoordbeleid is ingesteld en dat hoge rechten zijn toegekend aan een medewerker in het primaire proces.

De belastingopbrengsten zullen wij controleren op basis van de externe bronnen benadering die jaarlijks door uw organisatie wordt voorbereid.

Hoogwaterbeschermingsprogramma

Gezien de omvang en complexiteit van het Hoogwaterbeschermingsprogramma heeft u ons verzocht een tussentijdse review uit te voeren voor de projecten Markermeerdijken en Durgerdam. Tijdens de tussentijdse review hebben wij de aangeleverde dossiers van Markermeerdijken, Durgerdam 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

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

[illegible]

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 2020

Prioriteit midden: Bevinding op te lossen voor de jaarrekeningcontrole 2021

Prioriteit laag: Bevinding op te lossen op lange termijn

Attentiepunten jaareinde controle en overige aandachtspunten

2. Attentiepunten jaareinde controle en overige aandachtspunten

2.1 Planning jaareinde controle

In de weken 8 tot en met 10 van 2021 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.

2.2 COVID-19

Zoals reeds aangegeven in de inleiding heeft COVID-19 impact op veel beleidsvelden, denk hier bijvoorbeeld aan:

- Uitvoeringslasten (handhaving, thuiswerkfaciliteiten)
- Bedrijfseconomisch (waardering vorderingen, aanspraak garanties)
- Inkomstenderving (belastingen, leges)

Wij hebben vastgesteld dat het waterschap een initiële inventarisatie heeft uitgevoerd ten aanzien van de impact die COVID-19 heeft op het waterschap. De belangrijkste maatregelen zien toe op de lagere baten belastingopbrengsten en de waardering van de vorderingen.

De financiële impact van Corona op de jaarrekening is door de organisatie in beeld gebracht. Wij benadrukken het belang van een dergelijke analyse en verzoeken u dan ook om deze periodiek te analyseren. Wij zullen de uitkomsten van uw analyse meenemen in onze risicoafweging en controleaanpak.

Evenals voorgaand jaar zal er een toelichting in het bestuursverslag en de jaarrekening opgenomen moeten worden inzake de gevolgen van COVID-19. Tevens vragen wij u een position paper jaarstukken 2020 op te stellen in relatie tot COVID-19.

2.3 Prestatielevering inkopen

Op 24 juli 2020 is de BADO-notitie 'Vastlegging en onderbouwing prestatielevering bij inkopen door decentrale overheidsorganisaties' verschenen.

Wij vragen u kennis te nemen van deze notitie en de vereisten inzake functiescheiding, de controle en documentatie van de prestatielevering. Wij willen u wijzen op het belang van deze notitie mede in relatie tot fraudegevallen zoals geconstateerd bij diverse waterschappen. Wij voeren graag tijdig overleg met u over de (interne) controle van prestatielevering. Afhankelijk van de uitkomsten (aard van de fouten en onzekerheden) kan dit leiden tot een verdere uitbreiding van de deelwaarneming en extra werk.

Wij hebben tijdens de controle vastgesteld dat documentatie aanwezig is en de prestatieverklaarders in staat zijn zorgvuldig te onderbouwen waarom de prestatie geleverd is.

2. Aandachtspunten 2020

2.4 Rechtmatigheidsverantwoording

Recent is besloten om de vereisten van de rechtmatigheidsmededeling mee te nemen in de wetswijziging voor de Rekeningkamer. Dit betekent dat met ingang van het boekjaar 2021 het bestuur een rechtmatigheidsverantwoording moet opnemen in de jaarrekening. De accountant dient vervolgens de getrouwheid van deze verantwoording te toetsen. De bewijslast inzake de rechtmatigheid wordt hiermee verplaatst van de accountant naar het bestuur.

De belangrijkste aandachtspunten ter voorbereiding zijn:

- Afstemming reikwijdte met het algemeen bestuur;
- Juiste opzet normenkader en toetsingskader;
- Adequaat vastleggen van procesbeschrijvingen;
- Opzetten controle-plan inclusief uitwerking risicoanalyse;
- Adequaat werkprogramma ter uitvoering VIC.

Wij hebben begrepen dat het waterschap momenteel bezig is met het verder op orde brengen van deze punten. Graag bespreken wij met u de voorbereiding van de rechtmatigheidsverantwoording en de te zetten stappen met betrekking tot de inrichting van de (verbijzonderde) interne controle.

Het definitieve besluit om de vereisten van de rechtmatigheidsmededeling mee te nemen in de wetswijziging voor de Rekeningkamer moet nog worden genomen.

2.5 Afloop vorderingen op belastingdebiteuren

Door de implementatie van het nieuwe systeem was de afloop vorderingen op belastingdebiteuren voorgaand jaar later verwerkt. Het vaststellen van de afloop op basis van de bankafschriften bleek hierdoor arbeidsintensief. Wij verzoeken u voor het komende jaar de afloop tijdig te verwerken en inzichtelijk te maken ten behoeve van de jaarrekeningcontrole. Dit geldt zowel voor de afloop van de vorderingen op belastingdebiteuren die open stonden per 31 december 2020 als de vorderingen op belastingdebiteuren die open stonden per 31 december 2019.

2.6 Voorzieningen baggeren

De voorziening baggeren is in de definitieve jaarrekening 2019 gecorrigeerd ten opzichte van het concept. De oorzaak hiervoor was dat de gewijzigde inzichten aangaande uitgangspunten, waaronder aanwasselheid bagger en overgang van wegsloten nog niet was verwerkt. Wij verzoeken u bij het opstellen van de jaarrekening 2020 rekening te houden met de meest recente uitgangspunten.

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 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 applicaties die gerelateerd zijn aan financiële stromen en processen, en daarmee samenhangende (netwerk)infrastructuur.

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.

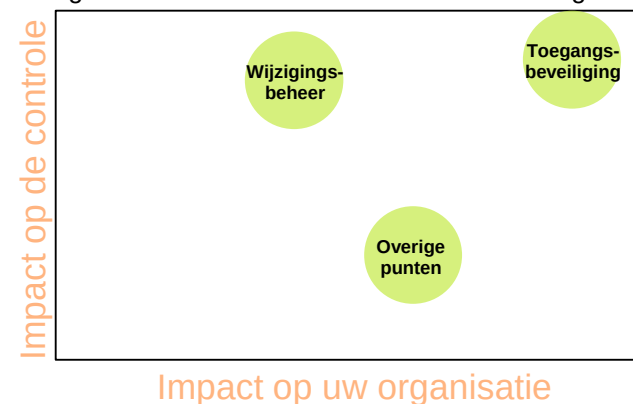
Werkzaamheden

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.



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 van 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.

'General IT'

De conclusies die wij op basis van onze werkzaamheden trekken over de algemene inrichting van IT bij uw organisatie, delen wij op deze pagina met u. Uit de stoplichten valt op te maken in hoeverre we gebruik kunnen maken van de randvoorwaarden die binnen uw organisatie aanwezig zijn voor de controle.

Identificatie & Authenticatie

Door middel van authenticatie wordt geborgd dat de gebruiker zichzelf kan identificeren binnen een geautomatiseerde omgeving. Kort gezegd: de gebruiker toont aan dat hij/zij inlogt met een eigen persoonsgebonden account en daarmee is wie hij/zij claimt te zijn. Wij scharen onder dit onderwerp met name wachtwoordvereisten en herleidbaarheid van accounts.

Autorisatie

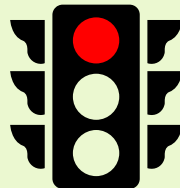
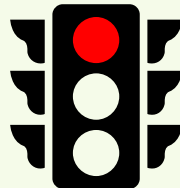
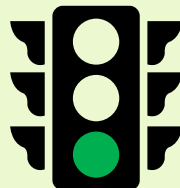
Op het gebied van autorisatie zijn verschillende vormen van diepgang te definiëren. Wat wij onderzoeken als het gaat om de randvoorwaarden rondom autorisatie, zijn de rechten die de mogelijkheid bieden om autorisatie-structuren te wijzigen en of deze rechten belegd zijn bij functionarissen met een onafhankelijke positie ten opzichte van de jaarrekening. Daarnaast is een effectieve procedure voor het wijzigen van rechten noodzakelijk.

Wijzigingsbeheer

Gedurende een (boek)jaar worden wijzigingen doorgevoerd in de IT-omgeving van uw organisatie. Wanneer deze wijzigingen een impact hebben op de functionaliteiten of rapportages die een rol spelen in de jaarrekening (en uw organisatie deze niet signaleert), heeft dit gevolgen voor de controlewerkzaamheden. Wij beoordelen dit onderdeel door te steunen op uw procedure of werkzaamheden uit te voeren op documentatie vanuit de leverancier.

Basware

UBW

Conclusie	Toelichting	Conclusie	Toelichting
	Accounts zijn in basis door een combinatie van herleidbare naamgeving en een adequaat wachtwoordbeleid, afgedwongen door middel van SSO, herleidbaar naar personen. Er zijn echter ook twee accounts die buiten deze systematiek vallen.		Er is binnen de applicatie geen wachtwoordbeleid ingesteld. Hierdoor is er onvoldoende zekerheid ten aanzien van de identificatie en authenticatie van accounts. Er wordt op dit moment reeds gewerkt aan de implementatie van Single Sign On om deze bevinding te verhelpen.
	Er is een proces ingericht voor het beheren van autorisaties. Echter worden binnen dit proces autorisatieverzoeken van de financiële administratie als 'geautoriseerd' beschouwd door applicatiebeheer. Daarnaast wordt in de controle documenten in het kader van de periodieke goedkeuring van autorisaties gewerkt op basis van excel overzichten en niet op basis van een weergave van toegekende rechten uit de applicatie.		De hoge rechten in de applicatie zijn, onder andere, toegekend aan een medewerker die werkzaam is in het primaire proces. Er is een proces ingericht voor het beheren van autorisaties. Echter worden binnen dit proces autorisatieverzoeken van de financiële administratie als 'geautoriseerd' beschouwd door applicatiebeheer. Daarnaast worden in de periodieke goedkeuring van autorisaties de controlehandelingen niet zichtbaar uitgevoerd.
	Er is een formele procedure voor het testen, goedkeuren en in productie nemen van wijzigingen.		Er is in opzet een formele procedure voor het testen, goedkeuren en in productie nemen van wijzigingen. Wij hebben het bestaan van de procedure ten tijde van de interim nog niet kunnen toetsen omdat er nog geen wijzigingen doorgevoerd zijn, dit in verband met de afwikkeling van de implementatie.

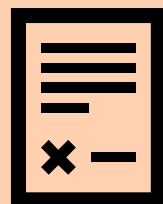
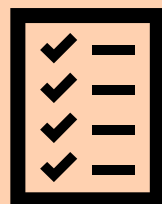
IT adviespunten zonder directe impact op de controle

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 in systemen conform de eisen die aan wachtwoorden worden gesteld vanuit informatiebeveiligingsoogpunt
- Periodieke controle op toewijzing van rechten in applicaties en op het netwerk op basis van een autorisatiematrix

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. Daarnaast wordt er gebruik gemaakt van meerdere anti-virus / malware oplossingen.

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

Bijlage

Detailbevindingen

Detailbevindingen interim-controle

Uitleg opbouw managementletter

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 2020:

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

Detailbevindingen interim-controle

Bevinding	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.

Update 2020

In het afgelopen boekjaar is opvolging gegevens door een brainstormsessie te houden. Hierin zijn de frauderisico's besproken o.b.v. de fraudedriehoek. De uitkomsten worden meegenomen in de 3 lines of defence interne beheersing discussie. Met daaruit volgend een Interne Controleplan voor de komende jaren waarin ook VIC beter wordt geborgd. Er is een projectgroep samengesteld die hieraan werkt.

Contactgegevens

drs J.M.A. (John) Drost RA

Partner

M: 06 – 22 18 93 49

E: j.drost@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.

Entrada 303

Postbus 94124

1090 GC AMSTERDAM

T: 020 – 644 28 40

