Accountants

Baker Tilly (Netherlands) N.V.
Papendorpseweg 99
Postbus 85007
3508 AA Utrecht

T: +31 (0)30 258 70 00
F: +31 (0)30 254 45 77

utrecht@bakertilly.nl
www.bakertilly.nl

KvK: 24425560

Recreatie Midden Nederland
t.a.v. het bestuur
Postbus 8058
3503 RB UTRECHT

Datum
22 maart 2021

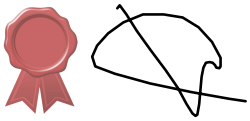
Referentie
2103-09121\1012942\v2.0

Betreft
Managementletter 2020

Geacht bestuur,

Hierbij sturen wij u onze managementletter over het boekjaar 2020. Wij vertrouwen erop u hiermee van dienst te zijn geweest.

Met vriendelijke groet,



G.J. van Luyk AA
Director

Bijlage(n)
• Management letter RMN def

Management letter

Recreatie Midden-Nederland

Boekjaar 2020

Aan het bestuur van Recreatie Midden-Nederland
Postbus 8058
3503 RB Utrecht

ONDERWERP:
Management letter 2020

Geacht bestuur,

Als onderdeel van de controle van de jaarrekening 2020 van Recreatie Midden-Nederland (hierna: RMN) 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, het bestaan en de werking van de interne beheersingsmaatregelen van de belangrijkste bedrijfsprocessen, inclusief de geautomatiseerde gegevensverwerking, in uw organisatie zijn beoordeeld en getoetst, zodat we een terugkoppeling kunnen geven over de betrouwbaarheid van de interne informatievoorziening en de jaarrekening.

Onze bevindingen zijn gebaseerd op de normale werkzaamheden in het kader van de jaarrekeningcontrole. Deze brief bevat daardoor niet alle onvolkomenheden in uw onderneming, 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. Wij hebben tevens de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing met betrekking tot de geautomatiseerde gegevensverwerking beoordeeld.

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 oplossingsrichting-en 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.

G.J. van Luyk AA
Director Audit

Inhoudsopgave

CONTACT

G.J. van Luyk AA
Director
f.vanluyk@bakertilly.nl

S.A. ter Weele RA
Manager
s.terweele@bakertilly.nl

KANTOORGEGEVENS
Baker Tilly (Netherlands) N.V

Bezoekadres
Papendorpseweg 99
3528 BJ Utrecht

Postadres
Postbus 85007
3508 AA Utrecht

+ 31 (0)30 258 70 00

1. Management samenvatting 4
2. Bevindingen IT-beheersing 8
3. Bevindingen interne beheersing 12
4. Overige onderwerpen 15
5. Bijlagen 17

1. Management samenvatting

Management samenvatting

1.1 Bedrijfsprocessen

Deze managementletter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2020. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

Administratieve Organisatie en Interne Beheersing
Voorgaand jaar hebben wij in onze management letter met u diverse aanbevelingen benoemd ter verdere optimalisering van de bestaande administratieve organisatie en interne beheersing. In deze management letter geven wij u een schriftelijke update van onze bevindingen.

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

- Inkopen
- Betalingen
- Lonen en salarissen
- Opbrengsten

Van deze processen is de opzet beoordeeld en het bestaan vastgesteld en waar mogelijk en efficiënt is de werking van de interne beheersingsmaatregelen getest.

Algemeen
Wij zijn van mening dat de AO/IB bij RMN verbeterd is ten opzichte van voorgaand jaar. Wij hebben tijdens onze interim controle ook de inrichting van IT getoetst. Wij hebben in onze controle voor 2020 geen testwerkzaamheden meer verricht ten aanzien van BigBen. De reden hiervoor is dat de doorbelasting naar de schappen plaatsvindt op basis van een vaste verdeelsleutel. Wij zullen om die reden ook niet meer ingaan op onze bevindingen uit voorgaande jaren t.a.v. dit pakket.

Wij zijn van mening dat de AO/IB van RMN van voldoende niveau is om een goedkeurende controleverklaring te kunnen verstrekken.

Inkopen
De inkoopfacturen worden in AFAS gecontroleerd en (indien akkoord) geautoriseerd door de betreffende budgethouder. Voor facturen van meer dan € 1.000 dienen twee (verschillende) personen deze te controleren en autoriseren en facturen boven de € 60.000 dienen door drie functionarissen te worden geautoriseerd.

Wij hebben enkele bevindingen bij de inrichting van AFAS, waardoor wij niet geheel kunnen steunen op deze interne beheersingsmaatregel. Deze bevindingen betreffen de aanwezigheid van niet-onafhankelijke super-users en het ontbreken van een (zichtbare) periodieke monitoring op rollen en rechten. Om deze reden kunnen wij niet met zekerheid stellen dat facturen het gehele jaar door de daartoe bevoegde persoon worden gecontroleerd en geautoriseerd. Wij verwijzen u graag naar paragraaf 3.1.

Betalingen
Voor het verrichten van betalingen wordt gebruik gemaakt van de diensten van BNG. Wij hebben vastgesteld dat de rechten in de bankapplicatie zodanig zijn ingeregeld dat altijd 2 bevoegde functionarissen de betaalbatch moeten autoriseren voordat deze betaald wordt. Daarnaast is er functiescheiding ingeregeld waarbij geen enkele medewerker zelfstandig betalingen kan verrichten.

Daarnaast hebben wij vastgesteld dat de betaaladvieslijst gecontroleerd wordt op rekeningnummer en bedrag. Door Corona is er veel vanuit huis gewerkt en is de vastlegging van deze maatregel op die momenten iets gewijzigd. In plaats van vinkjes en een handtekening op de betaaladvieslijst zijn per mail bestanden gestuurd en is per mail bevestigd dat de controle uitgevoerd is en de betaaladvieslijst is goedgekeurd. Hierdoor is de controle alsnog zichtbaar uitgevoerd en derhalve bruikbaar voor onze controle. Naar verwachting zal in de toekomst het thuiswerken meer blijven bestaan, wij wijzen erop deze maatregel dan voldoende zichtbaar te blijven uitvoeren.

Lonen en salarissen
Om vast te stellen dat de salarismutaties nauwkeurig worden verwerkt, is het van belang dat de salarismutaties worden gecontroleerd op juiste verwerking.

Wij hebben vastgesteld dat de salarismutaties middels een standenregister worden gecontroleerd, waarbij verschillen worden verklaard en onderbouwd middels onderliggende documentatie. Daarnaast wordt zichtbaar akkoord gegeven op de mutaties. Dit is een sterke maatregel waarvan wij hebben vastgesteld dat deze op juiste wijze wordt uitgevoerd. Wij zullen voor onze jaarrekeningcontrole steunen op deze maatregel.

Management samenvatting

1.1 Bedrijfsprocessen

Deze managementletter bevat onze bevindingen die zijn gebaseerd op de onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2020. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

Administratieve Organisatie en Interne Beheersing
Voorgaand jaar hebben wij in onze management letter met u diverse aanbevelingen benoemd ter verdere optimalisering van de bestaande administratieve organisatie en interne beheersing. In deze management letter geven wij u een schriftelijke update van onze bevindingen.

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

- Inkopen
- Betalingen
- Lonen en salarissen
- Opbrengsten

Van deze processen is de opzet beoordeeld en het bestaan vastgesteld en waar mogelijk en efficiënt is de werking van de interne beheersingsmaatregelen getest.

Ook bij het personeelsproces is door het thuiswerken de vastlegging van de maatregel op het standenregister iets gewijzigd. Per mail zijn de bestanden gestuurd naar de medewerker die de controle uitvoert en per mail is bevestigd dat de controle uitgevoerd is en de mutaties akkoord zijn bevonden.

Opbrengsten
In de jaarrekeningen van RMN, SGL en LSD hebben wij meerdere opbrengstenstromen onderkend. Per omzetstroom hebben wij inzichtelijk gemaakt hoe de omzet tot stand komt, evenals onze geplande controle aanpak.

De controle aanpak op de omzet is vooral gegevensgericht in combinatie met de minimaal vereiste aanwezige interne beheersingsmaatregelen. Wij zien hier op basis van onze werkzaamheden geen belemmering in. Daarnaast zien wij geen wijzigingen ten opzichte van vorig jaar (m.u.v. de toegangsgelden voor het strand, zie hiernaast). Wij zullen de opbrengsten gegevensgericht controleren.

De situatie rondom de toegangsgelden van de stranden is in 2020 wel gewijzigd. Het strandgeld werd geïnd middels (veelal) contante betalingen, waardoor er sprake was van een omvangrijk aantal transacties met kasgeld. Als gevolg van de COVID-19 maatregelen in Nederland was reservering (en betaling via iDeal) vooraf verplicht om toegang te verkrijgen tot de stranden. Als gevolg hiervan hebben wij geen testmaatregelen uitgevoerd om de controle op de kasontvangsten te toetsen, daar het strand van april tot en met september open was, waarin de verscherpte maatregelen golden.

Management samenvatting

1.2 IT systemen

Wij beschouwen uw IT omgeving van gemiddeld belang voor uw organisatie en daarmee ook voor onze controle. De reden hiervoor is de met name ondersteunende functie van IT, gerelateerd aan primaire processen binnen uw organisatie.

Het belang van uw IT omgeving leidt ertoe dat uw organisatie wel bedrijfs- en controlerisico's kan lopen als gevolg van tekortkomingen in de beheersing van de IT omgeving, maar dat deze op een andere wijze afgewogen worden dan bij een organisatie waarin primaire processen direct zijn gerelateerd aan de IT-omgeving.

Wij schatten in dat met name het waarborgen van de continuïteit van de IT omgeving en toegangsbeveiliging tot IT systemen van groot belang zijn voor uw organisatie, omdat de impact van tekortkomingen in deze IT aandachtsgebieden uitstroom van middelen en/of uitval van ondersteunende processen kunnen veroorzaken. Uiteindelijk kan uw primaire bedrijfsvoering hierdoor ook geraakt worden.

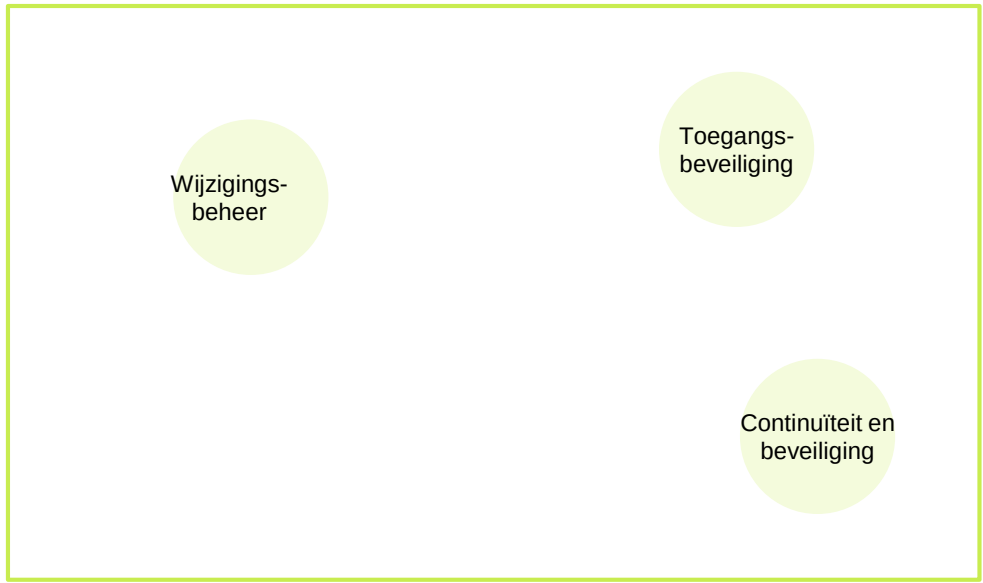
De inrichting van toegangsbeveiliging heeft daarnaast impact op onze controle, net als wijzigingsbeheer. Tekortkomingen hierin kunnen zorgen voor inefficiency in de controle en in het ergste geval het niet meer controleerbaar zijn processen en registraties van uw organisatie.

Overige punten m.b.t. bijvoorbeeld beleid binnen uw organisatie hebben met name een indirecte impact op uw organisatie en de jaarrekeningcontrole.

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

De kleur van de het symbool geeft de status van de constatering aan.

- Benodigd verbetering op (korte) termijn
- Adviespunt, verdere aanscherping mogelijk
- Op dit moment voldoende



Omgeving	Authenticatie	Autorisatie	Wijzigingsbeheer	Continuïteit	Proces
Netwerk	● ○ ○	○ ● ○		● ○ ○	**Alle**
AFAS	● ○ ○	○ ○ ●	○ ● ○	● ○ ○	**Alle**

2. Bevindingen IT-beheersing

2. Bevindingen IT-beheersing

2.1 Algemeen

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 beheersing van uw IT omgeving en rapporteren daarover in deze management letter.

Op basis van de door ons uitgevoerde werkzaamheden op 5-09-2020 hebben wij onze inschatting van de kwaliteit van uw IT systeem en/of applicaties opgenomen. Hierbij hebben wij de volgende onderverdeling gemaakt om de kwaliteit weer te geven:

- Benodigd verbetering op (korte) termijn
- Adviespunt, verdere aanscherping mogelijk
- Op dit moment voldoende

Bij het uitvoeren van onze werkzaamheden hebben wij gekeken naar de algemene onderwerpen rondom de beheersing van uw IT omgeving zoals in de tabel rechts opgenomen. Op de navolgende pagina's zullen wij onze bevindingen rapporteren.

	Onderwerp
	**Toegangsbeveiliging** Bij het toetsen van 'toegangsbeveiliging' wordt onderzocht of de inrichting van de IT-omgeving de authenticiteit van de gebruiker van een gebruikersaccount borgt. Vervolgens onderzoeken wij de mogelijkheden voor het 'steunen' op autorisaties en de processen rondom het verstrekken, muteren en ontnemen van autorisaties binnen de omgeving. Wanneer de randvoorwaarden hiervoor voldoende aanwezig zijn, kunnen wij in de controle gebruik maken van ingerichte functiescheiding in het systeem.
	**Wijzigingsbeheer (Change management)** Bij het doorvoeren van wijzigingen in software-omgevingen kunnen risico's ontstaan voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat er een vaste werkwijze is ingericht voor het doorvoeren van wijzigingen in de functionaliteiten van de applicatie. Daarnaast verwachten wij dat er gebruik wordt gemaakt van een test- en productie omgeving.
	**Continuiteïtsmaatregelen en beveiliging** Onder de noemer continuïteit en beveiliging krijgen wij inzicht in uw beheersing van risico's gericht op continuïteit van uw bedrijfsvoering. Hierbij kan discontinuïteit worden veroorzaakt door menselijk of technisch falen, maar ook door interne of externe kwaadwillenden. Voor continuïteit zijn met name het punt in de tijd aan tot waar u gegevens bij discontinuïteit kunt herstellen en de tijd die het kost om tot een normale bedrijfsvoering te komen bij discontinuïteit van belang. Hiernaast schatten wij uw beheersing van cyber risico's in.
	**Adviespunten zonder directe impact** Gegeven de omvang van uw organisatie en de mate waarin de IT-beheersingsomgeving invloed heeft op de bedrijfsvoering binnen de organisatie, zullen wij de volgende onderwerpen wel analyseren in het kader van onze controle, maar hier niet over rapporteren: ▪ IT-beleid; ▪ Verantwoordelijkheden en regiefunctie; ▪ Procedure beheersing van incidenten; ▪ Uitvoering procedures beheersingsmaatregelen IT (reproduceerbare beheersing van o.a. toegangsbeveiliging en wijzigingsbeheer) Overigens hebben wij omtrent deze onderwerpen geen bevindingen geconstateerd die significante impact hebben voor de jaarrekeningcontrole.

2. Bevindingen IT-beheersing

2.2 Toegangsbeveiliging en wijzigingsbeheer

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. Wij verwijzen u eveneens graag naar bijlagen 1 en 2.

Authenticatie
Door middel van authenticatie wordt geborgd dat een 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 m.n. de wachtwoordvereisten.

Autorisatie
Op het gebied van autorisatie zijn verschillende vormen van diepgang te definiëren. Wat wij onderzoeken en aan u rapporteren 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. Dit geldt voor zowel voor rechten op applicatie- als databaseniveau voor applicaties in scope van onze controle. Daarnaast is een effectieve vaste werkwijze voor het toekennen van rechten noodzakelijk om gedurende een periode te kunnen steunen op het feit dat rechten adequaat beperkt zijn.

Wijzigingsbeheer (Change management)
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.

Authenticatie	Autorisatie	Wijzigings-beheer	Omgeving
Netwerk 			De ingestelde wachtwoordeisen van de Windows Active Directory zijn van voldoende niveau op basis van de Baker Tilly best practice. Er zijn 4 accounts uitgezonderd van het periodiek wijzigen van wachtwoorden. Dit betreffen 3 accounts voor systeemtaken en 1 beheer account dat beheerd wordt door leverancier ISSYS. Het verhoogde risico op onrechtmatige toegang via deze accounts is daarmee beperkt. De hoge rechten in de Windows Active Directory zijn beperkt tot de leverancier ISSYS. Hiermee zijn deze rechten belegd bij onafhankelijke functionarissen. Er is geen functie-autorisatiematrix beschikbaar. Voor muteren van gebruikers en rechten wordt geen traceerbare procedure gebruikt en op de inrichting van rechten vindt geen periodieke controle plaats. Dit heeft als gevolg dat wij niet met zekerheid kunnen stellen dat rollen en rechten het hele jaar op juiste wijze zijn belegd.
Afas 			De ingestelde wachtwoordeisen van Afas voldoen op basis van de Baker Tilly best practice. De hoge rechten voor Afas zijn niet beperkt tot onafhankelijke functionarissen. Er zijn twee accounts actief waarvan het beheer bij dezelfde financieel medewerker ligt. Op basis van het bovenstaande bestaat het risico dat functiescheiding wordt doorbroken en als gevolg daarvan ten onrechte mutaties worden doorgevoerd. Er is daarnaast geen functie-autorisatiematrix beschikbaar. Voor muteren van gebruikers en rechten wordt geen traceerbare procedure gebruikt en op de inrichting van rechten vindt geen periodieke controle plaats Testwerkzaamheden omtrent een nieuwe release van AFAS worden niet zichtbaar vastgelegd. U loopt hiermee het risico dat na een release niet alle functionaliteiten goed werken. Wij beoordelen de ISAE-verklaring om vast te stellen of er wijzigingen zijn geweest die mogelijk van invloed zijn op de interne beheersingsmaatregelen. Deze zal in het eerste kwartaal van 2021 beschikbaar worden.

2. Bevindingen IT-beheersing

2.3 Regiefunctie, continuiteïtsmaatregelen en beveiliging

Let op: de onderwerpen 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 ontlenen aan de door ons beschreven aandachtspunten.

Verantwoordelijkheden en regiefunctie

Wij hebben vernomen dat binnen uw organisatie duidelijke afspraken zijn gemaakt ten aanzien van verantwoordelijkheden over uitvoering en strategie op het gebied van IT. Uw organisatie maakt beperkt gebruik van externe IT-dienstverleners waaronder ISSYS voor het netwerk en AFAS Software voor AFAS Online. Met de leverancier ISSYS wordt de beheersing gemonitord en met de leverancier besproken op basis van Service Level Reports.

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: U heeft aangegeven dat back-ups periodiek en incrementeel worden gemaakt en extern worden opgeslagen. Er wordt een dagelijkse back-up gemaakt, waardoor het dataverlies maximaal 24 uur is.

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 niet recent een recoverytest uitgevoerd. Hierdoor is onbekend binnen wat voor tijdsbestek u na onderbreking weer up-and-running kan zijn.

Uitwijk: U heeft ervoor gekozen om geen uitwijklocatie is te richten omdat medewerkers van buitenaf in kunnen loggen en hun werkzaamheden kunnen uitvoeren.

Beveiliging

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

Fysieke beveiliging: De servers zijn ondergebracht bij externe service- organisaties. Afspraken omtrent de fysieke beveiliging van de serverruimtes staan beschreven de SLA. De netwerk leverancier ISSYS is ISO 270001 gecertificeerd.

Remote access: Voor extern inloggen wordt gebruik gemaakt van een Azure MFA, waarbij met een combinatie van gebruikersnaam en wachtwoord ingelogd wordt en twee-factor-authenticatie benodigd is. Het risico dat externen zich toegang verschaffen tot de Windows omgeving is hierdoor beperkt.

Preventie: Een firewall en virusscanner is aan-wezig.

Monitoring: De IT-leverancier voert platformwide penetratietesten uit hierin is eveneens de RMN omgeving in meegenomen.

3. Bevindingen interne beheersing

3. Bevindingen interne beheersing

3.1 Uitleg opbouw management letter

In dit hoofdstuk zijn de significante bevindingen opgenomen.

Per bladzijde van deze managementletter is een bevinding opgenomen met daarbij het risico en een aanbeveling. Bij elke bevinding staat de datum van de eerste vermelding aangegeven te samen met de gradatie van de constatering. Bij de prioriteit staat de mate van belangrijkheid en urgentie.

Per bevinding zullen wij aangeven welke alternatieve werkzaamheden wij zullen uitvoeren om het geconstateerde risico (gegevensgericht) te ondervangen.

Per bevinding verzoeken wij het management om commentaar te geven.

Voor bestaande bevindingen geven wij tevens een update van de status van deze bevinding in het huidige boekjaar.

Bevinding
In dit blok wordt aangegeven wat gedurende de accountantscontrole is geconstateerd en waarvan wij u graag op de hoogte willen brengen.

Prioriteit	Boekjaar bevinding	Status
Urgentie en belang van de bevinding	Boekjaar eerste vermelding	
	Risico Hierbij geven wij aan wat de risico's zijn van de bevinding en wat de gevolgen voor uw onderneming kunnen zijn.	
	Aanbeveling Hier geven wij u aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.	
	Update boekjaar / Gevolgen jaarrekeningcontrole Hier geven wij een update van de bevinding wanneer deze in een eerde boekjaar is geconstateerd. Tevens kan de bevinding gevolgen hebben voor de controle aanpak / omvang van onze controlewerkzaamheden. Op deze plaats maken wij hier eveneens vermelding van.	
	Management commentaar Na het bespreken van de concept managementletter krijgt u de mogelijkheid om hier uw commentaar op geven.	

De kleur van de het symbool geeft de status van de constatering aan.

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

3. Bevindingen interne beheersing

3.2 Autorisatie inkoopfacturen

Bevinding

AFAS is voor de autorisatie van inkoopfacturen van belang doordat er gebruik gemaakt wordt van een digitale inkoopstraat.
Hierbij dienen de inkoopfacturen in overeenstemming met het mandaat (en budgethouders-
regeling) te worden geautoriseerd door een bevoegd functionaris.

Sinds begin 2018 zijn de budgethouders per grootboek/ projectnummer ingevoerd in AFAS waardoor deze nu allen zijn toegewezen. Hierop kunnen door de financieel coördinator in AFAS wel handmatig aanpassingen op worden verricht. Daarnaast hebben wij geconstateerd dat er twee accounts met super-user rechten worden beheerd door de financieel medewerker. Met deze accounts is het eveneens mogelijk om aanpassingen door te voeren, zoals het wijzigen van rechten of het onterecht goedkeuren van facturen.

Prioriteit	Boekjaar bevinding	Status
Gemiddeld	2018/ 2019/ 2020	

Risico
Het risico is aanwezig dat autorisatie van inkoopfacturen plaatsvindt door een niet daartoe gemachtigde functionaris. Dit resulteert in een onrechtmatige uitstroom van liquide middelen en een onrechtmatige verantwoording van kosten.

Aanbeveling
Wij raden u aan de beheerrechten te beleggen bij onafhankelijke functionarissen. Daarnaast raden we u aan periodiek te onderzoeken in hoeverre inkoopfacturen zijn geautoriseerd door daartoe onbevoegde functionarissen.

Update boekjaar / Gevolgen jaarrekeningcontrole
Wij zullen middels een gegevensgerichte data-analyse vaststellen of de autorisaties in overeenstemming zijn met de mandaten/ budgethoudersregeling. Binnen AFAS is hierbij onderscheid aangebracht voor facturen tot € 1.000, facturen tussen de € 1.000 en € 60.000 en facturen groter dan € 60.000.

Bij aanvang van de balanscontrole ontvangen wij graag van u een export van de digitale inkoopstraat waaruit blijkt welke medewerker welke factuur heeft geautoriseerd.

Management commentaar
Ook in 2021 zullen wij, in het kader van de jaarrekeningcontrole 2020, zelf een data-analyse uitvoeren op de feitelijke aanwezigheid van functiescheiding in het accorderingsproces. Gezien de transitiefase waar Recreatie Midden-Nederland zich momenteel in bevindt, zullen de rollen en het gebruik van superuseraccounts nu niet heroverwogen, danwel aangepast worden. Conform uw verzoek zullen wij bij start van de balanscontrole de gevraagde digitale inkoopstaat opleveren.

4. Overige onderwerpen

4. Overige onderwerpen

4.1 Gevolgen Corona

In het voorjaar 2020 heeft Nederland te maken gekregen met Corona en de impact die dit heeft op onze maatschappij. Ook op de jaarrekening 2020 zal Corona zijn invloed hebben. In dit kader onderkennen wij onder andere de volgende aandachtspunten:

- Waardering materiele vaste activa;
- Waardering vorderingen;
- Impact op begrotingsrechtmatigheid. Onze verwachting is dat de begroting door de impact van Corona tijdig is bijgesteld;
- Toelichting in het jaarverslag en de jaarrekening

Wij verwachten dat bij het opstellen van de jaarrekening tenminste rekening wordt gehouden met de hier genoemde punten. Daarnaast verwachten wij dat de onzekere economische ontwikkelingen en de mogelijke risico's die hiermee gepaard gaan van invloed kunnen zijn op het benodigde weerstandsvermogen. Wij adviseren u tijdig te starten met het actualiseren van de berekening van het weerstandsvermogen.

4.2 Rechtmatigheidsverantwoording

Met ingang van het boekjaar 2021 moet het bestuur een rechtmatigheidsverantwoording 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.

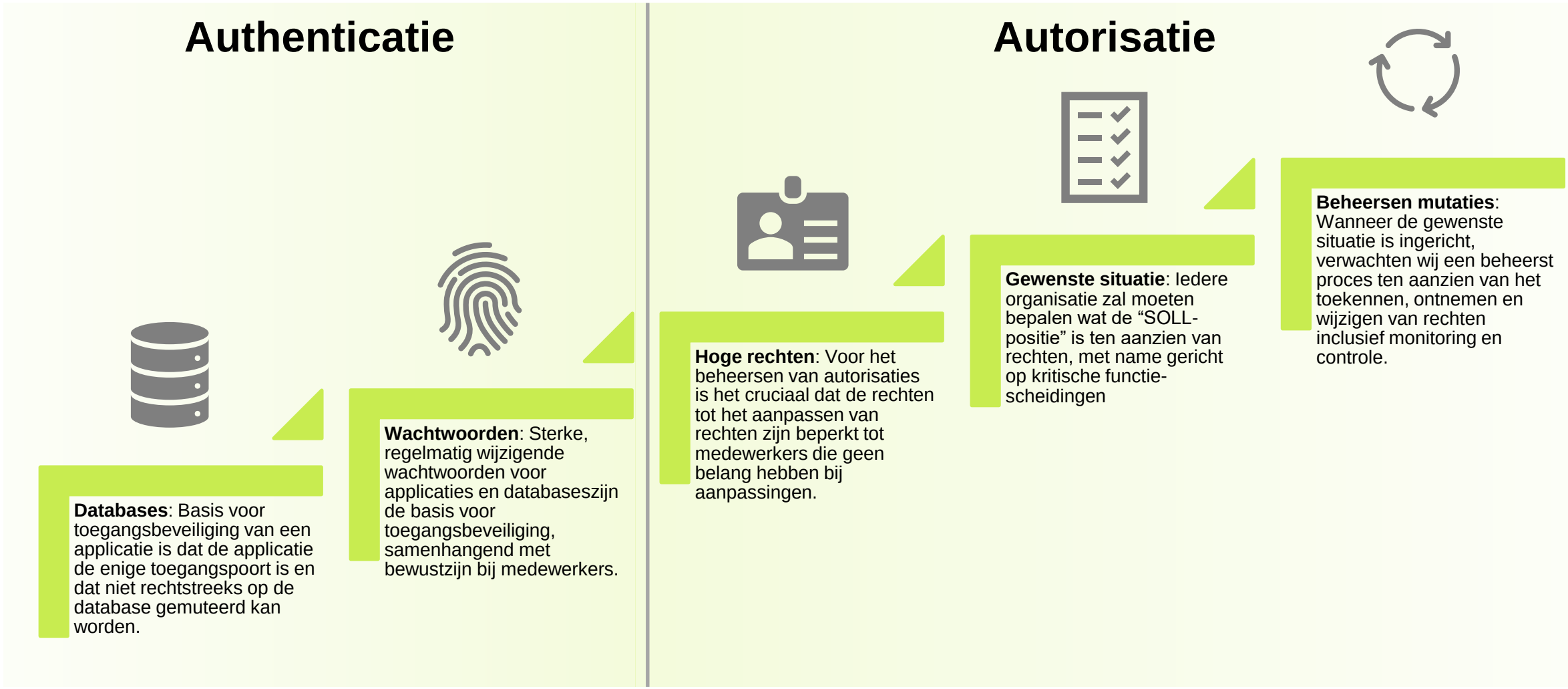
Wij adviseren de RMN de realisatie naar een eigen rechtmatigheidsverantwoording te monitoren. Recent hebben wij kennis genomen van jullie plan van aanpak omtrent de rechtmatigheidsverantwoording, dit is een goede eerste stap om straks aan deze nieuwe vereisten te kunnen voldoen.

5. Bijlagen

Bijlage 1:

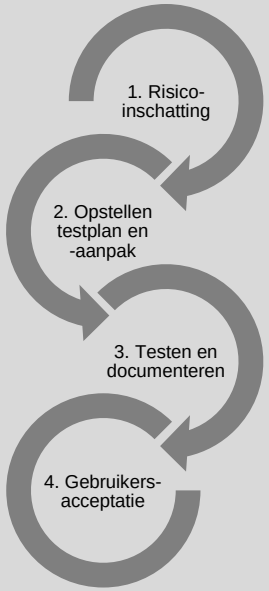
Logische toegangsbeveiliging

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. In het onderstaande figuur zijn de bouwstenen schematisch weergegeven, op de volgende slides geven wij per applicatie weer welke bevindingen wij per applicatie hebben:



Bijlage 2:
Wijzigingsbeheer

Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfs-voering 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. Onder wijzigingen verstaan wij niet alleen nieuwe versie updates, maar ook aanpassing-en in (kritieke) systeemconfiguraties.



Proces	Onze verwachting
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. Daarnaast moet beoordeeld worden welke geïdentificeerde technische en organisatorische wijzigingsrisico's er spelen bij het uitvoeren van de change, in het bijzonder wanneer er sprake is van maatwerk. Hiermee beoordeelt u per wijziging welke nieuwe of gewijzigde functionaliteit een risico vormt voor een goede werking van uw bedrijfsvoering.
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/no-go momenten, het maken van een back up voor implementatie, een fall-back scenario in het geval een implementatie mislukt en het definiëren van de impact op de organisatie (denk bijvoorbeeld aan het opleiden van medewerkers)
Testen en documenteren	Softwarewijzigingen kunnen gestructureerd worden getest, na het correct uitvoeren van de voorgaande twee stappen. Het maken van een gedegen vastlegging van testwerkzaamheden is van belang voor de aantoonbaarheid en controleerbaarheid van de uitgevoerde stappen. Daarnaast kan de vastlegging van testwerkzaamheden een belangrijke bron van informatie zijn als er onverhoopt na het doorvoeren van de wijziging toch verstoringen van uw bedrijfsvoering optreden.
Gebruikers acceptatie	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. Het kan natuurlijk ook voorkomen dat het nodig is om gebruikers te informeren over bijzonderheden als gevolg van de wijziging, zoals veranderingen in de werkwijze of aandachtspunten bij het gebruik van de applicatie.

Contactgegevens

G.J. van Luyk AA
Director Audit
+31 30 258 7000
f.vanluyk@bakertilly.nl

S.A. ter Weele MSc RA
Manager RA
+31 30 258 7000
s.terweele@bakertilly.nl

Kantoorgegevens:
Baker Tilly (Netherlands) N.V.
Papendorpseweg 99
3528 BJ Utrecht

Postbus 85008
3508 AA Utrecht
+31 (0)30 258 7000