

Managementletter

Bedrijfsvoeringseenheid Bommelerwaard

Boekjaar 2023

Aan het bestuur van de
Bedrijfsvoeringseenheid Bommelerwaard
Postbus 10002
5300 DA ZALTBOMMEL

ONDERWERP:
Management letter 2023

Geacht bestuur,

Als onderdeel van de controle van de jaarrekening 2023 van Bedrijfsvoeringseenheid Bommelerwaard 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 in sommige gevallen 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.

De bevindingen komen voort uit onze werkzaamheden in het kader van de jaarrekeningcontrole en zijn opgenomen voor zover wij het van belang achten om deze met u te communiceren. Deze brief bevat daardoor niet alle onvolkomenheden in de interne beheersing, die bij een eventueel uitgebreid en hierop specifiek gericht onderzoek naar voren zouden kunnen komen. Zoals u zult begrijpen, is de managementletter van nature positief 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.

Ondertekening alleen in definitieve versie

Drs. R. Opendorp RA

Inhoudsopgave

CONTACT

drs. R. (Rik) Opendorp RA
Partner Audit
+31 (0)6 10 09 04 64
r.opendorp@bakertilly.nl

E.D (Linda) de Vries MSc RA
Senior Manager audit
+31 (0)6 52 75 99 01
l.devries@bakertilly.nl

KANTOORGEGEVENS
+31 (0)76 525 0000
Bijster 39, 4817 HZ Breda
Postbus 3814, 4800 DV Breda



Bestuurlijke
samenvatting



Interne beheersing



Vorbereiding
controle



Actualiteiten



Bijlagen



Bijlagen
IT Bevindingen

1. Introductie

Doel van de managementletter

Deze managementletter bevat onze bevindingen ten aanzien van de interne beheersing (inclusief de IT-omgeving), die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole 2023. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

Een goede interne beheersing maakt dat de risico's voor de organisatie beter beheersbaar zijn en de jaarrekeningcontrole effectiever en efficiënter kan plaatsvinden. Vanuit onze natuurlijke adviesfunctie willen wij bijdragen aan verbetering van uw bedrijfsvoering, onder andere door het analyseren van de IT-omgeving en de bedrijfsprocessen.

Voorgaande jaren hebben wij onze bevindingen eveneens met u gedeeld. In deze managementletter geven wij u een update van onze bevindingen.

Bestuurlijke samenvatting

In het volgende overzicht (zie de volgende twee pagina's) hebben wij voor u een bestuurlijke samenvatting opgenomen. Deze punten worden in detail besproken in de hierop volgende paragrafen.

1. Bestuurlijke samenvatting

1. Bestuurlijke samenvatting

	Deze managementletter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2023.
	Uw interne beheersing is op orde. We hebben geen significante tekortkomingen in uw AO/IC geconstateerd. Wel hebben we in deze managementletter u een aantal aanbevelingen meegegeven. De belangrijkste betreffen het benutten van de technische mogelijkheden om functiescheiding af te dwingen via de systemen.
	Actie benodigd voor de rechtmatigheidsverantwoording: Vanaf boekjaar 2023 wordt een deel van de decentrale overheden, waaronder uw gemeenschappelijke regeling, zelf verantwoordelijk voor het opstellen van de rechtmatigheidsverantwoording. Tijdens de controle constateerde wij dat er nog <u>geen</u> afspraken gemaakt zijn tussen de verbijzonderde interne controleurs, de gemeenten en de financiële administratie over het toetsen van de begrotingsrechtmatigheid en de kredietrechtmatigheid. Wij willen u erop wijzen dat dit onderdeel is van de rechtmatigheidsverantwoording en <u>door u getoetst</u> moet worden om tot een rechtmatigheidsoordeel te komen. Met de Verbijzonderde interne controleurs is afgestemd dat zij de aanbestedingsrechtmatigheid zullen controleren.
	IT omgeving: Wij constateren geen significante tekortkomingen in de beheersing in uw IT-omgeving. Belangrijkste aandachtspunt vanuit onze controle ziet op de hoge rechten in Key2Financiën en Yourfoce, waardoor mogelijk onrechtmatige transacties zouden kunnen plaatsvinden. Wij vragen u kritisch te kijken of dit wenselijk is.
	Onze samenwerking. Vooruitblik richting jaarrekeningcontrole 2023. De samenwerking met de gemeenschappelijke regeling verloopt op een effectieve en plezierige wijze. We hebben met uw organisatie goede afspraken over de planning van de jaarrekeningcontrole gemaakt. Op voorhand identificeren we een aantal aandachtsggebieden met verhoogde aandacht in onze controle. Dit betreft voornamelijk de werkzaamheden voor het opstellen van de rechtmatigheidsverantwoording.

2. Interne beheersing

2. Interne beheersing

Inleiding

In dit hoofdstuk behandelen wij onze bevindingen ten aanzien van de interne beheersing.

Achtereenvolgens worden de volgende onderwerpen besproken:

- *Evaluatie interne beheersing:*
In dit onderdeel behandelen wij de belangrijkste bevindingen ten aanzien van de IT-omgeving, de primaire processen en de gevolgen van onze bevindingen voor de controleaanpak.
- *Controleomgeving:*
De controleomgeving vormt de basis voor de interne beheersing. In dit onderdeel rapporteren wij onze waarnemingen ten aanzien van de elementen van de controleomgeving (waaronder de samenwerking VIC en het three lines of defense model waarvoor wij verwijzen naar par 2.4).
- *Frauderisicoanalyse en beheersing frauderisico's:*
In dit onderdeel beschrijven wij de belangrijkste frauderisico's, de bijbehorende beheersingsmaatregelen en onze inschatting van het restrisico, rekening houdend met de getroffen maatregelen.
- *IT-omgeving:*
In dit onderdeel geven wij een visuele weergave van de IT-omgeving. Daarnaast geven wij aan welke applicaties in scope zijn, in hoeverre hierop kan worden gesteund en wat de gevolgen zijn als onvoldoende op de applicatie kan worden gesteund.
- *Data-analyse:*
In dit onderdeel geven wij een overzicht van de geplande data-analyses en het effect hiervan op de controle.
- *Detailbevindingen interne beheersing:*
In dit onderdeel worden de detailbevindingen ten aanzien van de IT-omgeving en de processen uitgewerkt.

2. Interne beheersing

2.1 Algemeen

Doel en reikwijdte

Het doel van onze jaarrekeningcontrole is het vormen van een oordeel over de getrouwheid van de jaarrekening (waaronder inbegrepen de rechtmatigheidsverantwoording) als geheel, zoals bedoeld in het Besluit Accountantscontrole Decentrale Overheden (Bado). Vanuit de jaarrekeningcontrole beoordelen wij de kwaliteit van de administratieve organisatie en interne beheersing voor zover relevant voor onze oordeelsvorming en geven wij geen zelfstandig oordeel over de kwaliteit van de administratieve organisatie en interne beheersing. De controle van de jaarrekening omvat het uitvoeren van controlewerkzaamheden, waaronder risicoanalyse, cijferanalyses, beoordeling van de administratieve procedures en het daarmee samenhangende systeem van interne beheersingsmaatregelen en gegevensgerichte controlewerkzaamheden. De samenstelling en omvang van die werkzaamheden zijn noodzakelijk voor het verkrijgen van voldoende controle-informatie ter onderbouwing van ons oordeel.

Risicoanalyse

Onze risicoanalyse richt zich op een betrouwbare totstandkoming van de jaarrekening. Dit betekent dat wij niet alle risico's die voor u als organisatie 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 organisatie onderkende risico's / kernpunten in de controle zijn:

- Invoering van de rechtmatigheidsverantwoording;
- Prestatielevering inkopen;
- Risico dat het management van de organisatie de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw organisatie met name toe op de schattingsposten binnen de overlopende posten.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten. In 2023 is het risico inzake de rechtmatigheidsverantwoording toegevoegd. Daarnaast is het risico op controle van de rechtmatigheid van de inkopen/aanbestedingsrechtmatigheid niet meer van toepassing, deze verantwoordelijkheid ligt nu bij het bestuur en is hiermee impliciet opgenomen onder de risico's rondom de rechtmatigheidsverantwoording.

2. Interne beheersing

2.2 Beeld interne beheersing

Interne beheersing

Wij constateren dat uw organisatie afgelopen jaar stappen heeft gezet in de doorontwikkeling van de interne beheersing. Wij signaleren dat u naar aanleiding van de bevindingen voorgaand jaar (waaronder de registratie van prestatieleveringen) actie heeft ondernomen om de geldende procedures onder de aandacht te brengen bij medewerkers.

Om alle financiële uitdagingen voor uw organisatie de komende tijd in goede banen te leiden worden hoge eisen aan het planning- en control instrumentarium, alsmede het interne beheersingssysteem, gesteld. De invoering van de rechtmatigheidsverantwoording door het bestuur stelt hogere eisen aan het interne beheersingssysteem. De aanwezigheid van een adequaat intern (financieel) beheersingssysteem is daarbij een essentiële randvoorwaarde om te kunnen bijsturen en de betrouwbaarheid van financiële informatie en verslaglegging is van groot belang om dit tijdig en goed te kunnen doen.

Wij constateren dat op dit moment de processen in de basis op orde zijn en dat primaire functiescheiding is ingeregeld. Tijdens onze werkzaamheden voor de jaarrekeningcontrole 2023 constateerden wij ook dat de controlehandeling zichtbaarder nageleefd worden, waaronder een zichtbare registratie van prestatieleveringen. Ook vanuit de verbijzonderde interne controle (VIC) is bij ons aangegeven dat documentatie snel en beter wordt aangeleverd, waardoor controles effectiever verlopen.

Belangrijkste bevinding vanuit onze interim controle

Voorgaand jaar schreven wij dat er nog forse stappen te zetten waren bij de 'overgang' naar de nieuwe applicatie voor financiële administratie. Bij de jaarrekeningcontrole 2022 zijn deze issues opgevolgd, waarmee goede stappen voor een effectieve bedrijfsvoering zijn gezet.

Net als voorgaand jaar constateren wij dat er nog verbeteringen mogelijk zijn in het gebruik van de applicatie door meer gebruikt te maken van autorisation of application controls in het systeem. Doormiddel van deze 'controls' is het mogelijk functiescheiding af te dwingen bij memoriaalboekingen of wijzigingen van crediteurenstamgegevens. Het implementeren van deze 'controls' kan er aan bij dragen dat uw organisatie minder handmatige controles hoeft uit te voeren doordat de functiescheiding standaard in het proces wordt verwerkt.

Ten aanzien van het wijzigen van crediteurenstamgegevens en het autoriseren van betalingen merken wij op dat uw organisatie meerdere controles heeft ingebouwd om vast te stellen dat er betaald wordt aan het juiste bankrekeningnummers. Wij willen u erop wijzen dat het overmatig controleren er ook toe kan leiden dat er bij controles op 'vertrouwd' wordt dat een andere collega hier 'wel' naar gekeken heeft en de effectiviteit juist afneemt. Wij hebben op basis van onze controle overigens geen bevindingen waarbij er een indicatie is dat controles niet kritisch zijn uitgevoerd.

2. Bevindingen en aandachtspunten

2.2 Beeld interne beheersing

Is uw organisatie klaar voor de rechtmatigheidsverantwoording?

Per 1 januari 2023 moet uw organisatie zelf een rechtmatigheidsverantwoording in de jaarrekening opnemen. Voorheen vormde de accountant een oordeel over de rechtmatigheid en bracht hierover verslag uit. Met ingang van boekjaar 2023 wordt het een verplichting voor het bestuur. De van toepassing zijnde wet- en regelgeving (Besluit begroting en verantwoording en Besluit Accountantscontrole Decentrale overheden) is op dit moment in revisie/in consultatie. De verwachting is dat de deze formalisatie de komende tijd gaat plaatsvinden.

De rechtmatigheidsverantwoording zien primair toe op de volgende aspecten:

- Begrotingscriterium
 - Begrotingsrechtmatigheid
 - Kredietrechtmatigheid
- Voorwaardencriterium
 - Aanbestedingsrechtmatigheid
 - Overige aspecten (treasury, subsidies, uitkeringen)
- M&O (Misbruik & Oneigenlijk) – gebruik criterium
 - Vaststellen dat het bestuur het M&O-beleid heeft nageleefd

Op deze drie aspecten dient het bestuur in het jaarrekeningdossier rekening te houden dat er een toereikend onderbouwd oordeel beschikbaar dient te zijn inclusief het onderliggende interne controledossier. Dit dossier dient door de organisatie dusdanig aan ons als accountant gerapporteerd te worden, zodat wij dit als onafhankelijke derde zelfstandig kunnen reviewen en beoordelen. De eisen die aan deze dossiers gesteld worden zijn dus hoger dan voorgaande jaren.

Wij hebben de voorgang van het opstellen van een controledossier besproken met uw organisatie tijdens de interimcontrole en constateren dat met betrekking tot de aanbestedingsrechtmatigheid uw organisatie afspraken gemaakt heeft met de VIC om tot een oordeel inzake aanbestedingsrechtmatigheid te komen. Wij constateren tevens dat er met betrekking tot de volgende aspecten deze afspraken nog niet gemaakt zijn:

- Begrotingsrechtmatigheid
- Kredietrechtmatigheid
- Overige aspecten (op momenten dat deze zich voordoen)
- Naleving M&O-beleid

Wij raden u aan concrete afspraken te maken wie verantwoordelijk is voor welk onderdeel van het 'controledossier' zodat deze meegenomen kunnen worden bij het opstelproces van de jaarrekening.

2. Interne beheersing

2.2 Beeld interne beheersing

Deze managementletter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2023. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw organisatie als geheel.

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

In het overzicht hiernaast zijn de bevindingen opgenomen. Een totaaloverzicht van de detailbevindingen is opgenomen in bijlage 1.

In de tabel rechts is een totaal overzicht opgenomen van het totaal aantal detailbevindingen. De bevindingen en onze aanbevelingen worden op de volgende pagina's van deze managementletter uitgebreider toegelicht.

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

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

aandachtspunten

Aantal nieuwe aanbevelingen	0
Aantal aanbevelingen uit voorgaande jaren	4
Waarvan opgelost in 2023	1
Resterende aanbevelingen uit voorgaande jaren	3
Waarvan reeds acties zijn ondernomen, maar nog niet zijn afgerond	2
Waarvan nog geen acties zijn ondernomen	1
Aantal openstaande aanbevelingen	3

#	Proces	Bevinding	Status	Prioriteit 2023	Prioriteit 2022
1	Inkopen	Prestatielevering	●	Laag	Hoog
2	Inkopen	Registratie inkopen en aanbestedingen	●	Laag	Laag
3	Monitoring	Memoriaalboekingen	●	Laag	Laag
4	Automatiseren	Conversie Decade – Key2F	●	-	Hoog

2. Controleomgeving

2.3 Three lines model



Wij rapporteren via het three lines model. Dat willen zeggen dat wij binnen de processen nagaan op welk niveau in de organisatie de interne beheersmaatregelen worden ondervangen. De volgende niveaus worden hierbij onderkend:

- 1^e lijn: in het primaire proces, onder verantwoordelijkheid van de proceseigenaar.
- 2^e lijn: in de ondersteunende processen zoals financiën en control, waar checks and balances ingericht zijn om fouten te signaleren.
- 3^e lijn: in uw verbijzonderde interne controle achteraf.

Indien de beheersmaatregelen in de 1^e en/of 2^e lijn adequaat zijn ingericht dan is de organisatie optimaal in control en is een voornamelijk systeemgerichte controleaanpak mogelijk. Indien dit niet het geval is kan dit gecompenseerd worden door de gegevensgerichte werkzaamheden van de VIC. In het kader van de rechtmatigheidsverantwoording dient in ieder geval de 3^e lijn (VIC) toereikend te zijn. Onderstaand overzicht geeft zodoende een beeld over de mate van beheersing en controle van uw organisatie.

Nr.	Proces	1 ^e lijn	2 ^e lijn	3 ^e lijn	Opmerking / toelichting
1	Inkopen, aanbestedingen en betalingen	●	●	●	Wij constateren dat er afgelopen jaar een stap gemaakt is met het registreren van de contracten en de aanbestedingsvorm die gekozen is. Daarnaast signaleren wij dat de registratie van de prestatielevering nog niet altijd op het juiste moment in het proces gebeurt en dat financiën andere collega's hierop moet aanspreken. Via Key2F wordt gefaciliteerd dat prestatielevering kan worden geregistreerd bij de inkomende factuur. Hier wordt echter nog niet altijd gebruik van gemaakt. Wij signaleren dat er forse stappen zijn gezet in dit proces. Uit mailwisselingen blijkt wel dat er vanuit de organisatie nog strak gestuurd moet worden op collega's om prestatielevering ook altijd (conform procedure) te documenteren.
2	Lonen en salarissen	●	●	●	Vanuit de VIC over de eerste maanden zijn geen bijzonderheden geconstateerd.
3	Memorialen	●	n.v.t.	n.v.t.	Memoriaalboeking worden niet getoetst als onderdeel van de VIC.

Uit bovenstaande beeld komt naar voren dat wij nog niet optimaal op de processen kunnen steunen maar in samenwerking met de VIC grotendeels een gegevensgerichte aanpak hanteren. Wij bespreken uiteraard graag met u de mate van beheersing en uw gewenste ambitieniveau.

Legenda status:

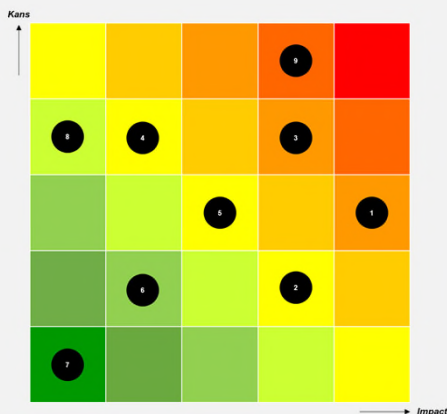
- = geen bevindingen met kans op materiële fouten, enkel aanbeveling ter verdere optimalisatie
 ● = één of enkele bevindingen met geringe impact resteren

- = meerdere bevindingen en aanbevelingen met mogelijk grote impact

2. Interne beheersing

2.5 Frauderisicoanalyse en frauderisico's

Fraude- en corruptierisico's



Frauderisicoanalyse

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude (waaronder corruptie) berust bij het bestuur van uw organisatie. 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.

Voor het opstellen van een frauderisicoanalyse is het raadzaam een template te gebruiken toegespitst op uw organisatie. Hierin kan voor processen waar materiële kostenstromen mee zijn gemoeid, inzichtelijk worden gemaakt:

- welke frauderisico's de organisatie onderkent;
- wat de geschatte kans en impact van deze frauderisico's is;
- wat de risicospons van uw organisatie is, idealiter afgestemd op de risicobereidheid van de organisatie zoals vastgelegd in frauderisicobeleid;
- welke interne beheersmaatregelen reeds getroffen zijn om onderkende frauderisico's te mitigeren;
- welke eventuele restrisico's/leemtes in de interne beheersing resteren en hoe de organisatie deze ondervangt (bijvoorbeeld via de verbijzonderde interne controle).

De kans- en impactweging van frauderisico's kan via een risicomatrix weergegeven worden om op basis daarvan prioriteiten te stellen in de wijze waarop met risico's wordt omgegaan. Een voorbeeld van hoe een risicomatrix eruit kan zien is hiernaast opgenomen.

Voor de duidelijkheid benoemen we graag dat er een relatie is tussen fraude en misbruik en oneigenlijk gebruik (M&O). M&O is namelijk een vorm van fraude waarbij de nadruk ligt op handelingen van derden in relatie tot het verkrijgen van overheidsbijdragen dan wel het betalen van heffingen. Wij raden u aan om bij het opstellen van een frauderisicoanalyse, ook expliciet aandacht te besteden aan M&O-risico's vanwege de verwevenheid tussen fraude en M&O, zie ook 'Kadernota Voorkomen en Bestrijden Misbruik en Oneigenlijk gebruik 2023'.

Tot slot merken wij op dat het uitvoeren van een frauderisicoanalyse en het treffen van interne beheersmaatregelen, onderdeel vormen van het bredere 'frauderisicomanagement'. Frauderisicomanagement omvat namelijk ook het opstellen van frauderisicobeleid (waar M&O-beleid al dan niet onderdeel van kan vormen), het opstellen van een frauderesponsplan voor situaties dat een vermoeden van fraude bestaat en het periodiek intern evalueren in hoeverre frauderisicomanagement voldoende is ingericht en toereikend werkt binnen de organisatie.

2. Interne beheersing

2.6 Beheersing frauderisico's

Fraude- en corruptierisico's

Op basis van onze uitgevoerde interim-controle stellen wij vast dat er binnen de organisatie (in combinatie met de gemeenten Zaltbommel en Maasdriel) aandacht is voor frauderisico's en de preventie daarvan. Wel zijn wij van mening dat hier nog een verbeterslag in te maken is. Wij constateren dat de organisatie een interne frauderisicoanalyse heeft opgesteld op procesniveau. Wij signaleren hierbij de volgende aandachtspunten:

- De frauderisicoanalyse licht wel toe uit welke elementen de 'fraudedriehoek' bestaat, maar maakt deze niet specifiek voor de processen en transactiestromen die uitgevoerd worden door bedrijfsvoeringseenheid. Wij raden u aan om ook specifiek voor de bedrijfsvoeringseenheid een frauderisicoanalyse op te stellen.
- De frauderisicoanalyse is opgezet vanuit de diverse processen, echter een visie op 'omgaan met fraudepreventie' en een analyse op organisatieniveau is niet vastgelegd. Wij adviseren u deze elementen toe te voegen aan de fraude risicoanalyse.
- Wij adviseren u om de risicoanalyse met specifieke frauderisico's uit te breiden en tot een gewogen afweging te komen welke risico's te accepteren en welke risico's te mitigeren middels reeds genomen of nog te nemen interne beheersingsmaatregelen. Dit kan door per risico de mogelijk kans en impact toe te voegen en vervolgens te concluderen of sprake is van een hogere of lagere fraudekans.

De verbijzonderde interne controle kan ook aan waarde winnen als de opdracht hiervoor wordt ingegeven vanuit een interne frauderisicoanalyse, waardoor de werkzaamheden beter aansluiten op de risico's binnen de organisatie. Op deze wijze wordt de verbijzonderde interne controle volwaardiger en volwassener.

Onze frauderisicoanalyse

Op basis van de bedrijfsverkenning en de interim-controle onderkennen wij de volgende frauderisico's bij onze jaarrekeningcontrole:

- Risico dat het management van de gemeenschappelijke regeling de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw organisatie met name toe op de schattingsposten binnen de overlopende posten.

2. Interne beheersing

2.4 IT-omgeving

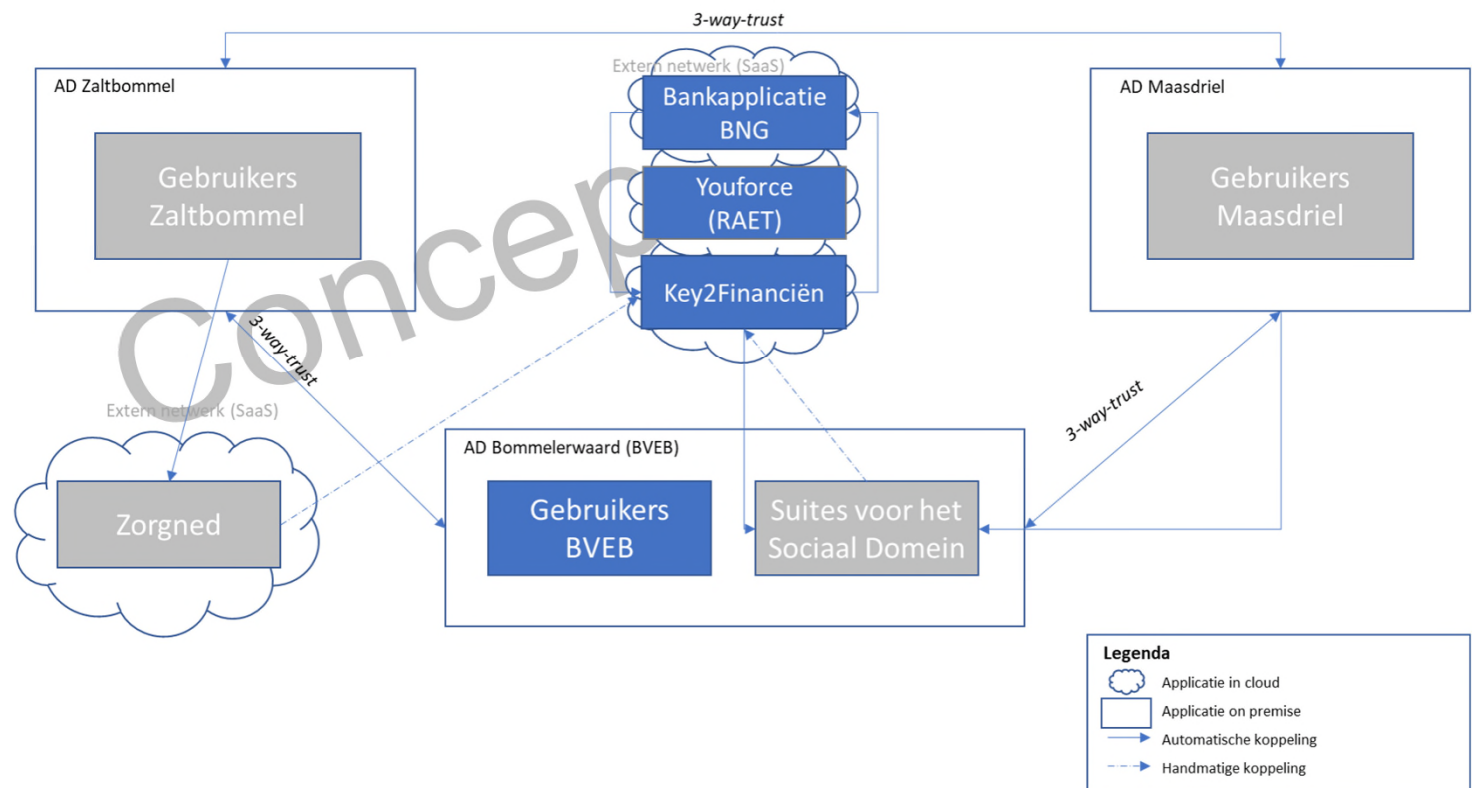
Visuele weergave IT-omgeving:

Het IT-landschap is grafisch in kaart gebracht. De grijze applicaties zijn voor onze controle van de Bedrijfsvoeringseenheid Bommelerwaard out of scope, maar voor de volledigheid van het landschap wel opgenomen.

We hebben vernomen dat er sprake is van een 3-way-trust tussen de Active Directory's (AD) van de verschillende organisaties (Bedrijfsvoeringseenheid Bommelerwaard, gemeente Zaltbommel en gemeente Maasdriel).

De IT-omgeving van uw organisatie, voor zover in scope voor de jaarrekeningcontrole, is als volgt weer te geven:

BVEB



2. Interne beheersing

2.6 Detailbevindingen interne beheersing - Samenvatting

De tabellen op deze pagina geven een overzicht van onze bevindingen ten aanzien van de processen en de IT aandachtsgebieden binnen uw organisatie.

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

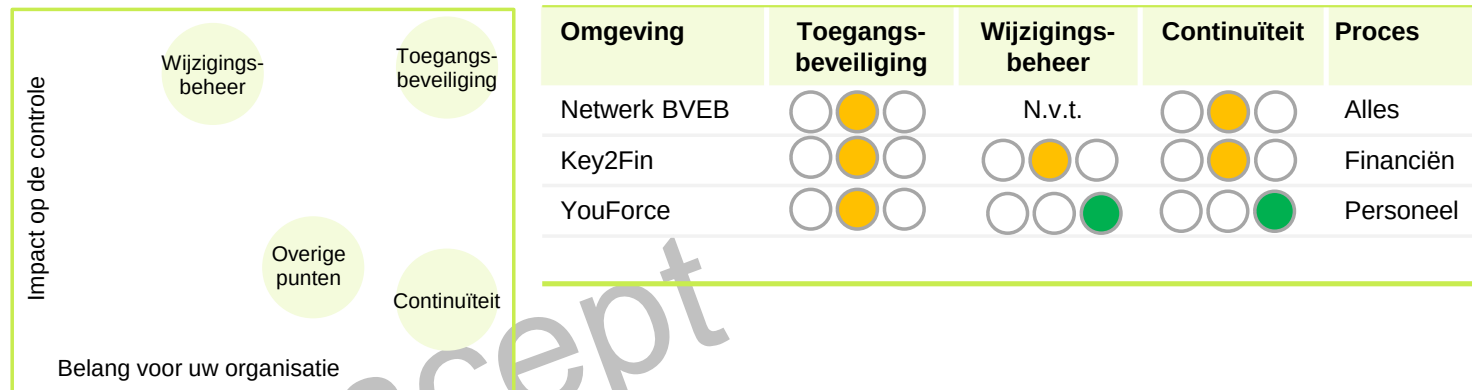
De kleur van de het symbool geeft de status van de constatering aan.

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

Onderstaande symbolen geven de status van onze bevindingen ten aanzien van de overige processen aan.

- Opgelost
- Actie ondernomen, maar nog niet afgerond
- Geen actie ondernomen
- Niet oplosbaar door omvang organisatie
- Nieuwe bevinding

Belangrijkste bevindingen IT beheersing



Belangrijkste bevindingen en aanbevelingen interne beheersing

#	Omgeving	Bevinding	Jaar van Constateren	Status	Kans	Impact
1	Netwerk BVEB	Periodiek wijzigen wachtwoorden 'alle accounts'	2023		Midden	Hoog
2	Netwerk BVEB	Opstellen functie-autorisatiematrix	2023		Laag	Midden
3	Key2Financiën	Beperken hoge rechten	2023		Midden	Hoog
4	Key2Financiën	Procedure wijzigingenbeheer	2023		Laag	Laag
5	Youforce	Beperken hoge rechten	2023		Midden	Hoog

2. Interne beheersing

2.8 Data-analyse

Gebruik van data-analyse in de controle

Om te komen tot een efficiënte en effectieve controle maken wij gebruik van data-analyse.

Onderstaand hebben wij een overzicht opgenomen van de geplande data-analyses. Afhankelijk van de bevindingen naar aanleiding van de data-analyses, voeren wij waar nodig aanvullende (gegevensgerichte) werkzaamheden uit.

Analyse	Effect op de controle
Controle op functiescheiding bij autorisatie van inkoopfacturen	Middels deze analyse kunnen wij op efficiënte wijze vaststellen dat er altijd twee medewerkers betrokken zijn geweest bij een inkoop.
Controle van journaalposten middels journal entry testing met gebruik van een audit file.	Door het analyseren van de boekingen in de administratie, krijgen wij snel en diepgaand inzicht in de financiële transactiestromen binnen uw organisatie.
Controle op functiescheiding bij het aanmaken en/of wijzigen van crediteurenstamgegevens	Middels deze analyse kunnen wij op efficiënte wijze vaststellen dat er altijd twee medewerkers betrokken zijn geweest bij een wijziging van bankrekeningnummers.

3. Voorbereiding jaarrekeningcontrole



3. Voorbereiding jaarrekeningcontrole

3.1 Planning en afspraken

Om aan uw behoeften te kunnen voldoen en om het proces voor de jaareinde controle verder te kunnen verbeteren vinden wij het belangrijk om vooraf afspraken te maken, het proces regelmatig te evalueren en onze bevindingen met u te delen. Om achteraf verrassingen te voorkomen willen wij de volgende werkafspraken met u maken:

Vorbereitung für die Jahresabschlussprüfung 2023

Onderwerp	Toelichting
Planning	Wij starten met de jaarrekeningcontrole op 26 februari 2023. Om de jaarrekeningcontrole efficiënt te laten verlopen is het belangrijk dat vóór deze datum een conceptjaarrekening inclusief sluitende brugstaat en controledocumentatie aanwezig is. Voor de benodigde controle- documentatie (het balansdossier) leveren wij een lijst 'met op te leveren stukken' aan, inclusief deadlines voor de aanlevering van de documentatie.
Deelwaarnemingen en gegevensgerichte werkzaamheden	Bij de jaarrekeningcontrole zullen wij voor bepaalde transactiestromen gebruik maken van de werkzaamheden die door de VIC worden uitgevoerd. Wij hebben om die reden reeds kennisgenomen van de bevindingen van deel 1 van de VIC (eerste 5 maanden) en concluderen vooralsnog geen bijzonderheden die zouden leiden tot aanvullende werkzaamheden.
Kwaliteit van cruciaal belang	Voor een efficiënte controle en korte doorlooptijd is van cruciaal belang om voor oplevering van de control informatie aan ons een interne kwaliteitscheck uit te voeren door de afdeling Financieel beheer op de door uw medewerkers aangeleverde stukken. Dit voorkomt onnodige vragen en zoekwerk gedurende de jaarrekeningcontrole.

4. Actualiteiten

4. Actualiteiten

4.1 Aankomende wetswijzigingen in BBV en Bado

Afgelopen zomer heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld. Samenvattend zijn de belangrijkste voorgestelde wijzigingen opgenomen:

Aanpassing Bado

Met ingang van 2024, mogelijk 2025, veranderen de goedkeuringstoleranties voor de jaarrekeningcontrole. Voorheen werd voor fouten uitgegaan van 1% van de totale lasten inclusief dotaties aan de reserves en voor onzekerheden 3%. Vanaf 2024 worden fouten en onzekerheden samengevoegd en wordt de goedkeuringsgrens gesteld op 2% van de totale lasten (dus zonder toevoeging reserves). Deze wijziging kan een belangrijke impact hebben. Wij adviseren u te evalueren wat dit voor uw situatie betekent en welke stappen gezet dienen te worden ter waarborging dat de fouten en onzekerheden binnen de goedkeuringstoleranties blijven vanaf 2024.

Ten aanzien van de SISa-bijlage houdt de accountant de verantwoordelijkheid om ook de rechtmatigheid vast te stellen.

De volgende tabel zal gehanteerd worden t.b.v. het oordeel:

Materialiteit	Goedkeurende verklaring	Verklaring met beperking	Verklaring van oordeelonthouding /afkeurende verklaring
Fouten in de jaarrekening en onzekerheden in de controle	$\leq 2\%$	$> 2\% - \leq 4\%$	$> 4\%$

Controleverklaring bij de jaarrekening

Vanuit onze beroepsvereniging NBA is aangegeven dat in het BBV duidelijkheid wordt gegeven over de publicatie van de controleverklaring in de jaarstukken van decentrale overheden. In het BBV is nu niet opgenomen dat deze verklaring onlosmakelijk deel uitmaakt van de jaarrekening en dat noch de definitieve jaarrekening en / of de jaarstukken noch de controleverklaring separaat gepubliceerd mogen worden. Hierdoor komt het voor dat jaarstukken van decentrale overheden worden gepubliceerd zonder de daarbij afgegeven controleverklaring.

Het is in het publiek belang dat de jaarstukken altijd met inbegrip van de controleverklaring toegankelijk worden voor het maatschappelijk verkeer, zoals raadsleden, burgers en andere belanghebbenden. Om dit te borgen heeft onze beroepsvereniging suggesties opgenomen ter aanpassing van artikel 24 lid 3 van het BBV, door daarin 'overige gegevens' toe te voegen waarin de controleverklaring wordt opgenomen.

Wij constateren dat de jaarrekening van uw organisatie zonder controleverklaring wordt gepubliceerd. Wij adviseren u om vooruitlopend op deze aanpassing deze werkwijze alvast toe te passen voor de jaarrekening 2023.

4. Actualiteiten

4.1 Aankomende wetswijzigingen in BBV en Bado

Afgelopen zomer heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld. Samenvattend zijn de belangrijkste voorgestelde wijzigingen opgenomen:

Uitbreiding inhoud jaarrekening

De voorgeschreven inhoud van de jaarrekening wordt uitgebreid met de rechtmatigheidsverantwoording. Hiermee bestaat de jaarrekening uit:

- het overzicht van baten en lasten in de jaarrekening en de toelichting;
- de balans en de toelichting;
- **de rechtmatigheidsverantwoording**
- de bijlage met de verantwoordingsinformatie over specifieke uitkeringen;
- een bijlage met het overzicht van de gerealiseerde baten en lasten per taakveld.

De volgende eisen worden gesteld aan de rechtmatigheidsverantwoording:

1. In de jaarrekening is een rechtmatigheidsverantwoording opgenomen, met inachtneming van de verantwoordingsgrens.
2. De rechtmatigheidsverantwoording bevat een toelichting op de rechtmatige totstandkoming van de baten, lasten en balansmutaties.
3. Het bestuur stelt de verantwoordingsgrens vast. De verantwoordingsgrens valt binnen 0 tot 3% van de totale lasten, exclusief de dotaties aan de reserves.
4. Indien het eindbedrag hoger is dan de verantwoordingsgrens licht het bestuur deze afwijking toe in de rechtmatigheidsverantwoording.

De commissie BBV stelt een modeltekst voor de rechtmatigheidsverantwoording op.

Notitie Overhead

De Notitie Overhead van de commissie BBV is in het voorjaar 2023 geactualiseerd en ter consultatie gepubliceerd. Ten opzichte van de notitie overhead 2016 is een belangrijke aanpassing de definitie van het begrip overhead zelf. Deze wordt als volgt gedefinieerd:

“het geheel van functies gericht op de sturing en ondersteuning van de medewerkers in het primaire proces. Hiertoe behoren ook de systemen en aanverwante lasten die deze functies ondersteunen.”

Daarnaast doet de commissie BBV de volgende stellige uitspraken, welke overigens al bestonden.

- De methodiek voor het toerekenen van overhead, zoals opgenomen in het overzicht overhead, aan lokale heffingen en rechten mag niet afwijken van de overige methodieken voor het toerekenen van overhead aan gemeentelijke taakvelden.
- Bij de berekening van de tarieven voor lokale heffingen moet de methodiek voor de toerekening van overhead worden opgenomen in de financiële verordening.

Ook zijn er voorbeelden toegevoegd die antwoord geven op actuele vraagstukken. De notitie treedt na publicatie naar verwachting in werking vanaf begrotingsjaar 2025.

4. Actualiteiten

4.1 Aankomende wetswijzigingen in BBV en Bado

Afgelopen zomer heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld. Samenvattend zijn de belangrijkste voorgestelde wijzigingen opgenomen:

Paragraaf Openbaarheid

Paragraaf Openbaarheid moet ten minste inzicht verschaffen in:

- a. de informatie die op grond van de artikelen 3.1, 3.3 en hoofdstuk 4 van de Wet open overheid openbaar is gemaakt;
- b. de informatiehuishouding;
- c. het aanwijzen en in dienst hebben van een contactpersoon als bedoeld in artikel 4.7 van de Wet open overheid;
- d. de besteding van subsidie voor de uitvoering van de Wet open overheid;
- e. de eventuele andere activiteiten benodigd ter uitvoering van de Wet open overheid;

De op grond van artikel 3.3, eerste en tweede lid, van de Wet open overheid openbaar gemaakte informatie bevat per categorie van informatie ten minste:

- a. op grond van welk artikel van de Wet open overheid de informatie openbaar is gemaakt;
- b. het jaar waarin de openbaarmaking van de informatie naar verwachting verplicht is;
- c. een omschrijving van de verstrekte informatie;
- d. het aantal documenten dat openbaar is gemaakt;
- e. het platform waarop de documenten openbaar zijn gemaakt.

Het inzicht in de besteding van de subsidie bedoeld in het eerste lid, onderdeel d, bevat ten minste een omschrijving van de wijze waarop de subsidie is besteed.

Paragraaf Bedrijfsvoering

Daarnaast worden de eisen t.a.v. de paragraaf bedrijfsvoering worden uitgebreid. Tot en met 2023 is de eis:

“De paragraaf betreffende de bedrijfsvoering geeft ten minste inzicht in de stand van zaken en de beleidsvoornemens ten aanzien van de bedrijfsvoering.”

Na goedkeuring van de voorgestelde wijziging verlangt de wetgever de volgende toelichting in deze paragraaf:

De paragraaf betreffende de bedrijfsvoering bevat ten minste:

- a. De stand van zaken van de bedrijfsvoering;
- b. De beleidsvoornemens ten aanzien van de bedrijfsvoering;
- c. Informatie over de financiële rechtmatigheid;
- d. Welke actie wordt ondernomen om afwijkingen van de financiële rechtmatigheid te voorkomen.

4. Informatieveiligheid

4.2 Is uw organisatie klaar voor de verplichte IT audits die wij in de publieke sector verwachten?

Binnen de publieke sector is informatieveiligheid een hot topic. Organisaties in de publieke sector halen regelmatig negatief het nieuws vanwege incidenten met betrekking tot informatieveiligheid, zoals hacks, CEO-fraude en datalekken. De komende jaren treden verschillende nieuwe wetten op het gebied van informatieveiligheid in werking waar ook uw organisatie mee te maken krijgt.

Van het bestuur wordt verwacht dat de ambtelijke organisatie wordt gefaciliteerd bij de implementatie van deze richtlijnen en wetten. Doel van deze wetten en richtlijnen is dat uw organisatie weerbaarder wordt op het gebied van informatieveiligheid. Daarnaast zal de toezichthoudende rol van het bestuur op het dossier informatieveiligheid ook worden uitgebreid. Verder is het onze verwachting dat de auditlast in relatie tot nu al verplichte IT-audits zal toenemen en dat nieuwe IT-audits hun opwachting zullen maken.

Wij adviseren u in beeld te brengen in hoeverre deze ontwikkelingen voor uw ambtelijke organisatie zijn gefaciliteerd en op basis daarvan vervolgstappen te nemen.

Huidige situatie

Jaarlijks legt het bestuur middels de **ENSIA** verklaring onder andere verantwoording af over informatieveiligheid ten aanzien van DigiD en Suwinet. Van gemeenschappelijke regelingen wordt verwacht dat ieder jaar een interne audit **Wpg** (Wet Politiegegevens) wordt uitgevoerd. Eén keer in de vier jaar wordt een externe Wpg-audit uitgevoerd.

Vanaf 2024 – wijzigingen ENSIA

Tot op heden is de diepgang van de jaarlijkse **ENSIA-audit** beperkt tot 'opzet' en 'bestaan' (beleid en implementatie van het beleid middels beheersingsmaatregelen). Vanaf 2024 wordt op een aantal onderdelen ook 'werking' van beheersingsmaatregelen getoetst in de jaarlijkse ENSIA-audit. Dit vraagt van uw organisatie dat beheersingsmaatregelen gedurende het jaar consequent en aantoonbaar worden uitgevoerd.

Vanaf 2026 – Wet Digitale Overheid

Vanaf 2026 is ook de tweede tranche van de **Wet Digitale Overheid** van toepassing. Dit deel van de wet vraagt van organisaties dat de governance rondom de verschillende basisregistraties en het delen van persoonsgegevens op orde is.

Vanaf 2023 – Wet Digitale Overheid

Met ingang van 2023 treedt het eerste deel (eerste tranche) van de **Wet Digitale Overheid** (WDO) in werking. De Wet Digitale Overheid is gebaseerd op de Europese eIDAS-richtlijn en regelt dat burgers veilig kunnen inloggen bij de overheid. Vanaf 2023 is het gebruik van HTTPS en HSTS verplicht. HTTPS configuraties dienen daarnaast te voldoen aan de laatste TLS-richtlijnen.

Vanaf 2024 – NIS2-richtlijn

Naar verwachting is vanaf eind 2024 de Europese **NIS2-richtlijn** (Network and Information Security Directive) van toepassing. De verwachting is dat de Baseline Informatiebeveiliging Overheid wordt uitgebreid met een aantal verplichte elementen. Vanuit de NIS2-richtlijn heeft uw organisatie een **zorgplicht** en **meldplicht** ten aanzien van informatieveiligheid. Daarnaast zal een toezichthouder **toezicht** houden op naleving van de NIS2-richtlijn middels (externe) IT-audits.

5. Bijlage

Bijlage 1:

Detailbevindingen interne beheersing - Bevindingen per proces

Hierna zijn de detailbevindingen en aanbevelingen ten aanzien van de belangrijkste processen opgenomen.

Per pagina is een bevinding opgenomen met daarbij het risico en de aanbeveling. Bij elke bevinding staat het jaar van de eerste vermelding aangegeven evenals de geschatte kans van voorkomen en impact op uw organisatie.

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

Aan het eind van dit hoofdstuk geven wij (voor zover van toepassing) voor bestaande bevindingen een update van de status van deze bevinding in het huidige boekjaar.

Constatering

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



Applicatie

Relevante IT systemen

Bevinding	TITEL BEVINDING	Kans: Hoog/middel/laag
Jaar van constatering	Boekjaar eerste vermelding	Impact: Hoog/middel/laag
Status bevinding:	Mate waarin door de organisatie opvolging is gegeven aan de constatering	
Risico	Hierbij geven wij aan wat de risico's zijn van de bevinding en wat de gevolgen voor uw organisatie kan zijn.	
Aanbeveling	Hier geven wij u aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.	
Gevolgen jaarrekening-controle	Hier geven wij een update van de bevinding wanneer deze in een eerde boekjaar is geconstateerd. Tevens kan de bevinding gevolgen hebben voor de controleaanpak en de omvang van onze controlewerkzaamheden. Op deze plaats maken wij hier eveneens vermelding van.	

Bijlage 1:

Detailbevindingen interne beheersing

Constatering

Tijdens onze controle hebben wij vastgesteld dat de onderbouwing van de prestatielevering niet altijd op een juiste wijze is onderbouwd.

Opvolging

Wij signaleren dat uw organisatie afgelopen jaar de procedures bij medewerkers onder de aandacht gebracht heeft. De registratie en documentatie van prestatieleveringen is hierdoor verbeterd. Wel signaleren wij dat er nog regelmatig door financiën (achteraf) gevraagd moet worden om de prestatielevering vast te leggen.

Wij onderschrijven het belang om vanuit deze 'financiële' rol hierop te blijven monitoren.

Deze bevinding is in lijn met de conclusies die uit de VIC op inkopen komen.



- Key2Financiën

Applicatie(s)

Bevinding	Prestatielevering inkopen	Kans:	Laag
Jaar van constatering	2018	Impact:	Laag
 Risico	Het risico bestaat dat inkoopfacturen ten onrechte betaald worden, waardoor lasten mogelijk ten onrechte ten laste van de organisatie worden gebracht.		
 Aanbeveling	Wij adviseren u de procedure met betrekking tot de onderbouwing van de prestatielevering bij medewerkers onder de aandacht te brengen en hierop te blijven toetsen in de VIC. Wij adviseren u de bevindingen van de VIC met de organisatie te delen.		
 Gevolgen voor de jaarrekening-controle	Middels beperkte aanvullende gegevensgerichte werkzaamheden willen wij zekerheid verkrijgen over de prestatielevering van de verantwoorde inkopen. Wij zullen hierbij gebruik maken van de verrichte VIC-werkzaamheden.		

Bijlage 1:

Detailbevindingen interne beheersing

Constatering

Afgelopen jaren hebben wij diverse malen gerapporteerd over de volledigheid van registratie van inkopen en aanbestedingen.

Wij constateren dat de aanbestedingsprocedure en documenten in het zaaksysteem geregistreerd staan, maar er geen directie koppeling is met de financiële administratie.

Hierdoor is vanuit de financiële administratie niet zichtbaar of de juiste inkoopprocedure is doorlopen.



- Key2Financiën

Applicatie(s)

Bevinding	Registratie inkopen en aanbestedingen	Kans:	Laag
Jaar van constatering	2019	Impact:	Laag
 Risico	Het risico bestaat dat inkoop of aanbesteding niet in overeenstemming met geldende wet- en regelgeving plaatsvindt. Hierdoor kunnen inkopen onrechtmatig zijn.		
 Aanbeveling	Wij adviseren u om te borgen dat bij inkopen de gevraagde procedure wordt gevolgd en hier intern op te blijven toetsen. Door een koppeling te maken tussen het contractenregister en Key2F kan de rechtmatigheid tussentijds en achteraf eenvoudiger worden gecontroleerd.		
 Gevolgen voor de jaarrekening-controle	Wij zullen de rechtmatigheid inkopen blijven volgen vanuit de controle-informatie die aangeleverd wordt als onderdeel van de rechtmatigheidsverantwoording.		

Bijlage 1:

Detailbevindingen interne beheersing

Constatering

Wij constateren dat er vanuit 2^e of 3^e lijn geen toetsingen plaatsvinden of memoriaalboekingen terecht zijn verantwoord in de administratie.

Wij constateren dat er geen afdwingbare functiescheiding is binnen het proces memoriaalboekingen. Bij de implementatie van de nieuwe financiële administratie is ervoor gekozen om meer specifieke dagboeken toe te voegen waardoor het aantal boekingen die lopen via het memoriaaldagboek sterk is afgenomen en het eenvoudiger is om op de 'bijzondere' boekingen te monitoren. Een 4-ogen-principe is voor deze "bijzondere" boekingen echter nog niet gerealiseerd.

Wij constateren wel dat memoriaalboekingen onderbouwd worden middels mails.



- Key2Financiën

Applicatie(s)

Bevinding	Memoriaalboekingen	Kans:	Laag
Jaar van constatering	2019	Impact:	Middel
 Risico	Door memoriaalboekingen kunnen belangrijke processen en functiescheidingen worden doorbroken, waarmee risico's op fouten en fraude toenemen.		
 Aanbeveling	Wij adviseren om periodiek (achteraf) een controle uit te voeren op de memoriaalboekingen, zodat vastgesteld wordt dat er geen onterechte bijzondere boekingen in de administratie zijn opgenomen Wij adviseren om een controle op memoriaalboekingen af te dwingen via de financiële applicatie door middel van het vier-ogen-principe.		
 Gevolgen voor de jaarrekeningcontrole	Tijdens de jaarrekeningcontrole zullen wij werkzaamheden verrichten met betrekking tot doorvoering van memorialen, omdat deze boekingen van invloed zijn op het afsluit- en schattingsproces binnen de organisatie en er geen waarborgen binnen het systeem zijn.		

6. Bijlage IT bevindingen

Bijlage:

Detailbevindingen interne beheersing - IT General Controls

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 managementletter.

Op basis van de door ons uitgevoerde werkzaamheden op 3-10-2023 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	
 Toegangs-beveiliging	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 gebruikmaken van ingerichte functiescheiding in het systeem. Een adequate inrichting kan preventief risico's voor uw organisaties beperken en tegelijkertijd efficiencyvoordelen opleveren in de controle.
 Wijzigings-beheer	Bij het toetsen van 'wijzigingsbeheer' ofwel change management wordt vastgesteld dat wijzigingen aan de applicatie op gestructureerde en gecontroleerde wijze worden doorgevoerd. Voor uw organisatie heeft wijzigingsbeheer ten doel om te voorkomen dat applicaties zich niet gedragen zoals u verwacht na een wijziging in de software, resulterend in, wellicht niet opgemerkte, (financiële) gevolgen.
 Continuïteits-maatregelen 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 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	Het is voor 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.

Bijlage:

Detailbevindingen interne beheersing - Toegangsbeveiliging Netwerk BVEB

2022	Authenticatie	Autorisatie	2023	Authenticatie	Autorisatie
	☐ ☒ ☐	☐ ☒ ☐		☐ ☒ ☐	☐ ☒ ☐

	Authenticatie	Autorisatie
 Bevinding	De wachtwoordvereisten die afgedwongen worden op het netwerk voldoen aan de best practice, dit mede doordat Multi-Factor Authenticatie (MFA) afgedwongen wordt voor het inloggen. Wij hebben echter vastgesteld dat meerdere accounts (service accounts, meerdere usersaccounts en mailboxen) zijn uitgesloten van het periodiek wijzigen van het wachtwoord. Van deze gebruikers verloopt het wachtwoord niet.	Op het netwerk hebben wij zeventien accounts met hoge rechten geïdentificeerd. Deze accounts worden gebruikt door (IT) medewerkers die onafhankelijk zijn van de primaire processen. Op dit moment worden autorisaties niet toegekend op basis van een functie-autorisatiematrix. Daarnaast worden de toegang tot het netwerk en autorisaties op het netwerk niet periodiek en aantoonbaar gecontroleerd op juistheid en volledigheid.
 Risico	Door het ontbreken van een maximale wachtwoordduur voor verschillende accounts bestaat kans dat gebruikers op een ander gebruikersaccount inloggen met mogelijke onrechtmatigheden tot gevolg. Door de toepassing van MFA wordt dit risico gemitigeerd.	Door het niet structureel controleren van gebruikers en bijbehorende rechten bestaat het risico dat medewerkers over onjuiste rechten op het netwerk beschikken met mogelijke onrechtmatige transacties en mogelijke doorbreking van functiescheiding als gevolg.
 Aanbeveling	Wij bevelen aan om de wachtwoordduur van alle accounts waarmee gebruikers inloggen periodiek te wijzigen conform de vereisten. Daarnaast bevelen wij ook aan om periodiek de wachtwoordinstellingen te controleren.	Wij bevelen aan om een functie-autorisatiematrix op te stellen en te gebruiken bij het toekennen van rechten op het netwerk. Binnen uw organisatie is een functie-autorisatiematrix in ontwikkeling. Daarnaast adviseren wij om periodiek de actualiteit van gebruikers en gebruikersrechten te controleren op basis van de autorisatiematrix.
 Gevolgen voor de jaarrekening controle	De bevindingen ten aanzien van authenticatie leiden tot het niet kunnen verkrijgen van controlezekerheid ten aanzien van de inrichting van authenticatie binnen het netwerk. Voor de accounts waarvan het wachtwoord niet verloopt voeren wij aanvullende werkzaamheden uit om te bepalen of zij transacties hebben ingevoerd of goedgekeurd. Afhankelijk van het aantal transactie dat door 'deze' accounts is behandeld zullen wij detailwerkzaamheden uitvoeren om vast te stellen dat deze transacties nauwkeurig zijn.	De bevindingen ten aanzien van autorisatie leiden tot het niet kunnen verkrijgen van controlezekerheid ten aanzien van de inrichting van de autorisaties binnen het netwerk. Middels aanvullende werkzaamheden zullen wij vaststellen of medewerkers ten onrechte transacties hebben aangemaakt of goedgekeurd.

Bijlage:

Detailbevindingen interne beheersing - Toegangsbeveiliging & wijzigingsbeheer Key2Financien

2022	Authenticatie	Autorisatie	Wijzigingsbeheer	2023	Authenticatie	Autorisatie	Wijzigingsbeheer
							

	Authenticatie	Autorisatie	Wijzigingsbeheer
 Bevinding	Voor het inloggen binnen Key2Financien wordt gebruikt van Single Sign On (SSO). Dit betekent dat de wachtwoordeisen van het netwerk gebruikt worden. Er zijn geen gebruikers binnen Key2Financien uitgezonderd van het afgedwongen wachtwoordbeleid op het netwerk.	Binnen de applicatie hebben wij acht gebruikers met hoge rechten binnen de applicatie geïdentificeerd. Een aantal van deze gebruikers zijn direct betrokken bij het primaire proces van de applicatie. Op dit moment worden autorisaties niet toegekend op basis van een functie-autorisatiematrix. Daarnaast worden de toegang en autorisaties binnen de applicatie niet periodiek en aantoonbaar gecontroleerd.	Gedurende de controleperiode zijn wijzigingen doorgevoerd, echter is er geen bewijs dat er daadwerkelijk getest wordt en dat dit vastgelegd wordt in het daarvoor beschikbare testplan.
 Risico	Geen.	Het risico bestaat dat bedoelde functiescheiding binnen de applicatie wordt doorbroken. Gebruikers met hoge rechten kunnen gebruikers aanmaken en rechten en rollen toekennen om zo functiescheiding te omzeilen.	Doordat er niet vastgelegd wordt hoe wijzigingen doorgevoerd worden, kan niet inzichtelijk gemaakt worden of wijzigingen impact hebben op de bedrijfsvoering.
 Aanbeveling	Geen.	Wij bevelen aan om hoge rechten te beperken en deze te beleggen bij onafhankelijke functionarissen. Wij bevelen aan om een functie-autorisatiematrix stellen en te gebruiken bij het toekennen van rechten. Daarnaast adviseren wij om periodiek actualiteit van gebruikers en gebruikersrechten te controleren op basis van de autorisatiematrix.	Wij bevelen aan om een procedure wijzigingsbeheer te formaliseren en deze te volgen. Daarnaast bevelen wij ook aan om de uitgevoerde testen bij een wijziging vast te leggen om zo inzicht te hebben in de impact van een wijziging.
 Gevolgen voor de jaarrekening-controle 	De bevindingen ten aanzien van authenticatie leiden tot het kunnen verkrijgen van controlezekerheid ten aanzien van de inrichting van authenticatie binnen Key2Financien.	De bevindingen ten aanzien van autorisatie leiden tot het niet kunnen verkrijgen van controlezekerheid ten aanzien van de inrichting van autorisatie binnen Key2Financien. Dit door de beperkingen ten aanzien van functiescheiding en het autorisatieproces. Voor de accounts waarvan het wachtwoord niet verloopt voeren wij aanvullende werkzaamheden uit om te bepalen of zij transacties hebben ingevoerd of goedgekeurd. Afhankelijk van het aantal transactie dat door 'deze' accounts is behandeld zullen wij detailwerkzaamheden uitvoeren om vast te stellen dat deze transacties nauwkeurig zijn.	De bevindingen ten aanzien van de wijzigingsbeheer leiden tot het niet systeemgericht kunnen steunen op de procedures van de organisatie kunnen steunen. Voor de controle dient bij gebruik van (standaard)lijstwerk uit K2F nadere gegevensgerichte controle plaats te vinden. Middels aanvullende gegevensgerichte werkzaamheden zullen wij vaststellen of releasenotes en wijzigingen in de applicatie juist zijn verwerkt.

Bijlage:

Detailbevindingen interne beheersing - Toegangsbeveiliging & wijzigingsbeheer Youforce

2023

Authenticatie

Autorisatie

Wijzigingsbeheer

	Authenticatie	Autorisatie	Wijzigingsbeheer
 Bevinding	De leverancier van YouForce rapporteert jaarlijks middels een ISAE3402-verklaring over haar interne beheersing. Deze verklaring met definitieve scores ontvangen wij naar verwachting begin 2024. De authenticatie binnen de applicatie is in deze ISAE voorgaande jaren positief beoordeeld. Deze voorgaande score hebben wij hier vooralsnog gehanteerd.	Binnen de applicatie hebben wij drie gebruikers met hoge rechten binnen de applicatie geïdentificeerd. Een aantal van deze gebruikers zijn direct betrokken bij het primaire proces van de applicatie.	De leverancier van YouForce rapporteert jaarlijks middels een ISAE3402-verklaring over haar interne beheersing. Deze verklaring met definitieve scores ontvangen wij naar verwachting begin 2024. Graag ontvangen wij nog de ISAE3402 verklaring per einde jaar zodat wij hem kunnen beoordelen. Het wijzigingsbeheer binnen de applicatie is in deze ISAE voorgaande jaren positief beoordeeld. Deze voorgaande score hebben wij hier vooralsnog gehanteerd.
 Risico	Geen.	Het risico bestaat dat bedoelde functiescheiding binnen de applicatie wordt doorbroken. Gebruikers met hoge rechten kunnen gebruikers aanmaken en rechten en rollen toekennen om zo functiescheiding te omzeilen.	Geen.
 Aanbeveling	Geen.	Wij bevelen aan om hoge rechten te beperken en deze te beleggen bij onafhankelijke functionarissen.	Geen.
 Gevolgen voor de jaarrekening-controle		De bevindingen ten aanzien van autorisatie leiden tot het niet kunnen verkrijgen van controlezekerheid ten aanzien van de inrichting van de autorisaties binnen de applicatie. Middels een cijferanalyse en een controle op 'indienst' en 'uitdienst' mutaties zullen wij vaststellen of de verantwoorde lasten nauwkeurig zijn.	



Bijlage:

Detailbevindingen interne beheersing - Continuïteitsmaatregelen 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 ontleen aan de door ons beschreven aandachtspunten.



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: U heeft aangegeven dat in de dagelijkse praktijk bestanden regelmatig hersteld moeten worden wanneer hiertoe verzoeken worden ingediend. Echter worden naast deze activiteiten geen recoverytests uitgevoerd. Wij bevelen u aan om tenminste jaarlijks een recovery test uit te voeren.

Uitwijk: Een uitwijklocatie is ingericht en deze wordt periodiek getest. Echter is aangegeven dat de laatste uitwijktest in 2021 plaats heeft gevonden. Wij bevelen u aan om tenminste jaarlijks een uitwijktest uit te voeren.



Beveiliging

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

Fysieke beveiliging:

De servers zijn ondergebracht op twee locaties. Toegang tot deze ruimtes is beperkt tot noodzakelijke medewerkers.

Remote access:

Remote access is afgeschermd middels een aanvullende authenticatielaag.

Hiernaast is two-factor authenticatie ingesteld voor inloggen op de omgeving, wanneer deze online wordt benaderd. Hiermee wordt gevoelige data in deze omgeving aanvullend beschermd. Wij onderschrijven het belang van een dergelijke risicogerichte aanpak bij beveiligen van verschillende datasets.

Beveiliging (Vervolg)

Preventie en monitoring:

Verschiedende maatregelen zijn getroffen ter voorkoming van een incident. Netwerk Access Control is gepland om aanvullend in te richten. Ten aanzien van monitoring en detectie wordt gebruikgemaakt van de diensten van de Informatiebeveiligingsdienst (IBD). Een pentest om eventuele kwetsbaarheden in het netwerk bloot te leggen is zover wij konden vaststellen niet recent uitgevoerd. Wij adviseren voldoende aandacht te besteden aan het detecteren van kwetsbaarheden in het netwerk en monitoren van bijzonderheden in het netwerkverkeer, conform het beleid en risicoanalyses.

Wij bevelen aan om ten minste jaarlijks een kwetsbaarheidsscan of penetratietest uit te voeren.

Bijlage:

Detailbevindingen interne beheersing - Adviespunten IT zonder directe impact

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 ontleen aan de door ons beschreven aandachtspunten.

Beleid en Plannen

Beleid

Binnen uw organisatie is een uitgewerkt IT beleidsplan aanwezig, waarin de uitgangspunten voor IT-beheer en ontwikkelingen zijn beschreven. Wel is er sprake van informele beleidsvoering, echter is dit niet als zodanig opgenomen als onderdeel van het beleidsplan van de organisatie. Het is niet mogelijk om zonder een beleidsplan monitoring op basis van een plan-do-check-act cyclus toe te passen binnen uw organisatie.

Verantwoordelijkheden en regiefunctie

Wij verwachten dat binnen uw organisatie duidelijke afspraken zijn gemaakt ten aanzien van verantwoordelijkheden over uitvoering en strategie op het gebied van IT.

Verantwoordelijkheden en regiefunctie (vervolg)

Uw organisatie maakt gebruik van externe IT-partijen, met deze partij is een Service Level Agreement overeengekomen. Een periodieke rapportage over de dienstverlening alsmede beoordeling door uw organisatie vindt nog niet plaats. Wij bevelen u aan om de regiefunctie goed in te richten.

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 is er sprake van een ticketsysteem t.b.v. de registratie van incidenten, problemen en verzoeken.

Uitvoering beheersingsmaatregelen IT

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

Uitvoering beheersingsmaatregelen IT (vervolg)

Denk aan een periodieke controle op actieve gebruikers & een periodieke controle op inrichting van wachtwoordbeleid. 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. Wij raden aan om bovenstaande procedures in te richten en (toetsbaar) periodiek te beheersen in de organisatie.

