

Concept Management letter



Bedrijfsvoeringseenheid Bommelerwaard Boekjaar 2024



Aanbiedingsbrief



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

Onderwerp: Management letter 2024

Geacht bestuur,

Als onderdeel van de jaarrekeningcontrole van boekjaar 2024 van de Bedrijfsvoeringseenheid Bommelerwaard (hierna BVEB) brengen wij een management letter uit.

In deze management letter rapporteren wij de bevindingen naar aanleiding van onze controle, de belangrijkste risico's, ons beeld van de interne beheersing, relevante ontwikkelingen in wet- en regelgeving en indien van toepassing andere veranderingen die voor u relevant kunnen zijn. In de bijlage hebben wij een gedetailleerd overzicht opgenomen van onze bevindingen en aanbevelingen.

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. De bevindingen en aanbevelingen dienen te worden gelezen als constructieve aanwijzingen voor het bestuur als onderdeel van een continue proces van het veranderen en verbeteren van de beheersing van de organisatie.

Deze management letter is door ons opgesteld voor uw informatie en mag niet zonder onze uitdrukkelijke toestemming geheel of gedeeltelijk aan derden ter beschikking worden gesteld. Wij danken u en uw medewerkers voor de samenwerking en zijn graag bereid tot het verstrekken van nadere toelichting.

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

drs. R. Opendorp RA



Inhoud

1. Management Samenvatting
2. Kwaliteit interne beheersing
3. IT-omgeving
4. Voorbereiding jaarrekeningcontrole
5. Actualiteiten
6. Bijlagen



Management samenvatting





1. Management samenvatting

In dit overzicht is een samenvatting van de belangrijkste punten naar aanleiding van onze werkzaamheden opgenomen.

Onderwerp	Toelichting
Timing van de werkzaamheden	Deze management letter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2024. Wij hebben bij de interim controle tevens controles uitgevoerd op de VIC over de maanden januari – mei.
Algemene conclusie interne beheersing	Wij concluderen dat er afgelopen jaren goede verbeteringen zijn doorgevoerd met betrekking tot de interne beheersing. Met name vanwege de verdere ontwikkeling en inrichting van Key2 zijn er afdwingende functiescheidingen in het inkoopproces, betaalproces en bij de boekingen van memorialen aanwezig, waardoor het risico op onnauwkeurige transacties met interne beheersing wordt afgevangen. Tijdens de interim-controle constateerden wij wel dat bij het aanbestedingsproces niet altijd alle documenten (tijdig) worden geregistreerd, waardoor afwegingen die gemaakt zijn niet altijd meer te herleiden zijn. Wij vragen u aandacht voor dit proces, mede omdat dit kan leiden tot onrechtmatige inkopen. Afgelopen jaren heeft de organisatie veel nadruk gelegd op het registeren en onderbouwen van de prestatieleveringen. De resultaten hiervan zijn zichtbaar in de uitkomsten van de VIC. Wel constateren wij dat dit een blijvend aandachtspunt is, zeker bij het 'inwerken' van nieuwe medewerkers.
IT-omgeving	In het kader van onze jaarrekeningcontrole hebben we de interne beheersing rondom uw IT omgeving onderzocht. Wij hebben in dat kader het netwerk en Key2 onderzocht. Ten aanzien van het 4-ogen principe bij de goedkeuring van facturen constateren wij dat deze kan worden doorbroken door vervangende functionarissen voor goedkeuring te selecteren. Wij adviseren u in te regelen dat alleen vervangende functionarissen geselecteerd kunnen worden, waarmee het 4-ogenprincipe kan worden gewaarborgd.

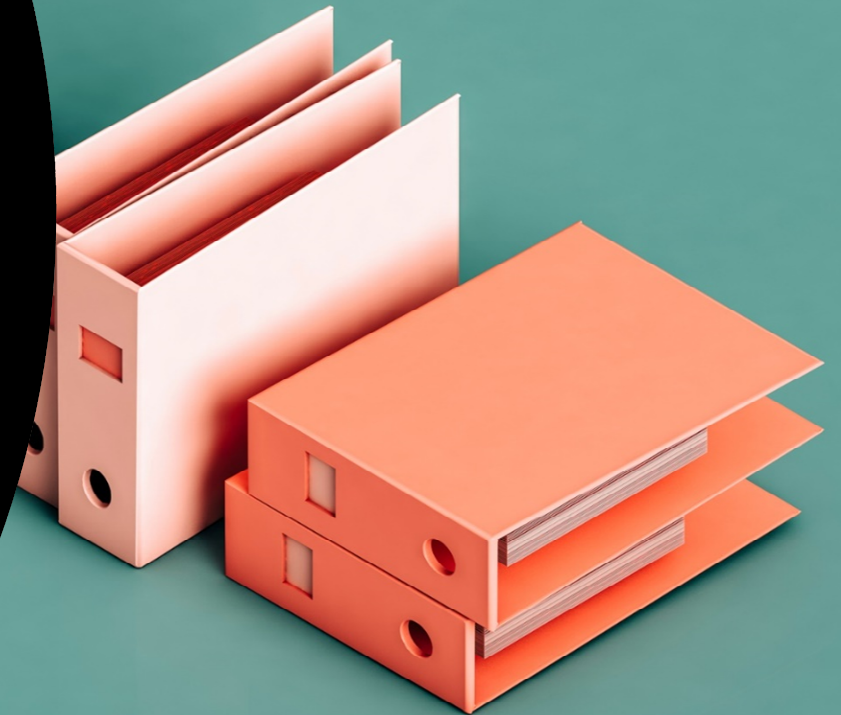


1. Management samenvatting

Onderwerp	Toelichting
Voorbereidingen jaarrekeningcontrole 2024	We maken met uw organisatie afspraken over de planning van de jaarrekeningcontrole 2024. Op voorhand identificeren we een aantal onderwerpen met verhoogde aandacht in onze controle. Dit betreffen met name het opstellen van de rechtmatigheidsverantwoording. Wij vragen u het controleproces voor de jaarrekening 2024 goed voor te bereiden.
Rechtmatigheids- verantwoording	Uw organisatie heeft voorgaand jaar de financiële verordening, controleprotocol en normenkader vastgesteld. Vanwege diverse aanscherpingen t.a.v. de rechtmatigheidsverantwoording adviseren wij u kritisch te beoordelen of deze verordeningen nog voldoen aan de huidige verwachtingen bij de rechtmatigheidsverantwoording en zo nodig de verordening hierop aan te scherpen. Met name inzake de wijze waarop omgegaan wordt met begrotingsrechtmatigheid en toetsing M&O beleid is verder aangescherpt ten opzichte van voorgaand jaar. In dit kader verwijzen wij u ook naar de actualiteiten in hoofdstuk 5.
Actuele ontwikkelingen	Vanuit het oogpunt van onze natuurlijke adviesfunctie hebben we een bijlage opgenomen met actuele ontwikkelingen. Wij vragen u hiervan kennis te nemen en hier indien noodzakelijk rekening mee te houden bij het opstellen van de jaarrekening 2024.
Onderlinge samenwerking	We hebben met de BVEB duidelijke afspraken gemaakt met betrekking tot de controle van de processen / interne beheersing en de jaarrekeningcontrole. Wij ervaren de samenwerking met de medewerkers van BVEB als plezierig en constructief.

2

Kwaliteit interne beheersing





2. Kwaliteit interne beheersing

Inleiding

Deze managementletter bevat onze bevindingen ten aanzien van de interne beheersing (inclusief de IT-omgeving), die zijn gebaseerd op de onze werkzaamheden in het kader van de jaarrekeningcontrole 2024. 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, processen efficiënter verlopen waardoor er meer grip is 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.

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:

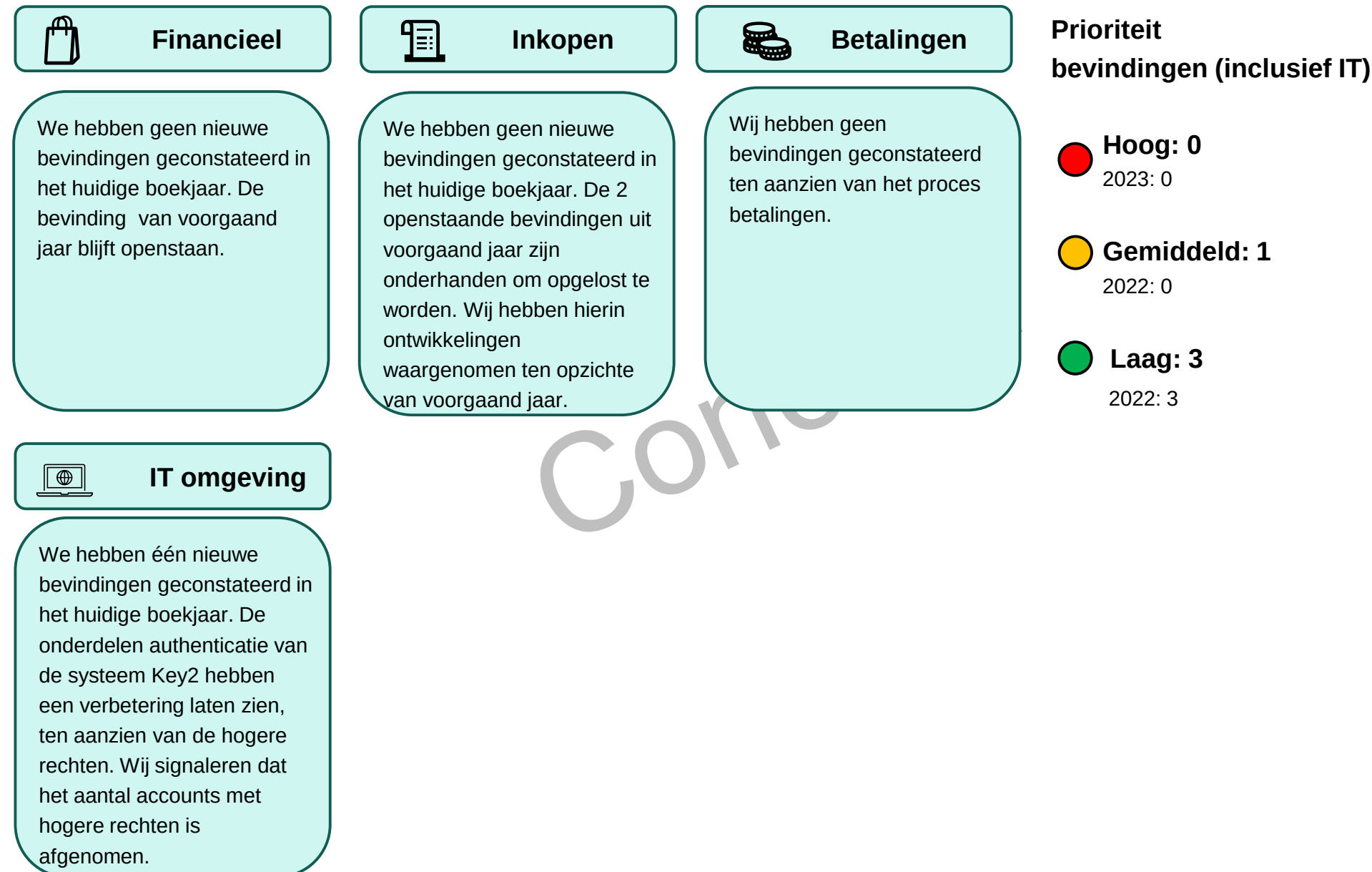
- De rechtmatigheidsverantwoording;
- Prestatielevering inkopen;
- De betalingsomgeving;
- Risico dat het management van de organisatie de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw organisatie met name toe op het inschatten van de nog te betalen kosten per jaareinde.

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

2. Kwaliteit interne beheersing



Samenvatting van de bevindingen voor de belangrijkste processen





2. Kwaliteit interne beheersing

Belangrijkste aanbevelingen

In onderstaand overzicht zijn de belangrijkste aanbevelingen naar aanleiding van onze werkzaamheden opgenomen. Wij hebben per bevinding een beknopte omschrijving opgenomen. Een gedetailleerde beschrijving van de detailbevindingen is opgenomen in bijlage (onderdeel 6 van deze managementletter). 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

#	Proces	Bevinding	Status	Prioriteit 2024	Prioriteit 2023
1	Inkopen	Prestatielevering		Laag	Laag
2	Inkopen	Registratie inkopen en aanbestedingen		Laag	Laag
3	Monitoring	Memoriaalboekingen		Laag	Laag
4	IT-omgeving	Autorisaties bij goedkeuring inkoopfacturen		Midden	nvt

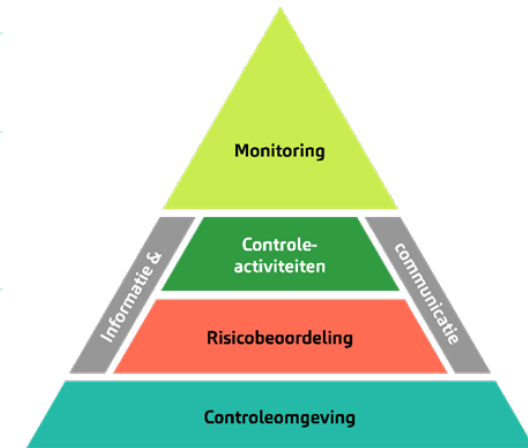


2. Kwaliteit interne beheersing

Waarnemingen controleomgeving

De controleomgeving vormt de basis voor de opzet en effectieve werking van de processen binnen uw organisatie. Onderstaand hebben wij onze waarnemingen ten aanzien van de verschillende elementen van de controleomgeving weergegeven. Naar ons oordeel biedt de controleomgeving een goede basis voor de interne beheersing als geheel.

	Elementen controleomgeving	Waarnemingen
1	Monitoring	• Bestuur houdt actief toezicht.
2	Informatie & communicatie	• De bestuursrapportage is tijdig beschikbaar en wordt gedeeld met het management en het bestuur
3	Controleactiviteiten	• Ons algemene beeld is dat de belangrijkste processen voldoende zijn ingericht. • Middels de bestuursrapportage worden afwijkingen onderkend en waar nodig vindt bijsturing van het budget plaats.
4	Risicobeoordeling	• Er is geen sprake van een formeel risico-inschattingsproces, wel worden er Verbijzonderde Interne Controles uitgevoerd op de belangrijkste processen • De directie is op de hoogte van de belangrijkste risico's en streeft ernaar deze te ondervangen door passende interne beheersingsmaatregelen in te stellen.
5	Controleomgeving	• Er is sprake van oogtoezicht door de directie. • Primaire functiescheiding is ingericht. • Positieve "tone at the top".





2. Kwaliteit interne beheersing

Frauderisicoanalyse

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude (waaronder corruptie) berust bij het bestuur. Deze verantwoordelijkheid betreft ook het onderhouden van een zodanige interne beheersing om het opmaken van de jaarrekening mogelijk te maken zonder dat deze afwijkingen van materieel belang bevat als gevolg van fraude of fouten.

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

- welke frauderisico's uw organisatie onderkent;
- wat de geschatte kans en impact van deze frauderisico's is;
- wat de risicorepons van uw organisatie is, idealiter afgestemd op de risicobereidheid van uw organisatie zoals vastgelegd in frauderisicobeleid;
- welke aandacht er is voor soft controls om fraude te voorkomen;
- welke interne beheersmaatregelen reeds getroffen zijn om onderkende frauderisico's te mitigeren;
- welke eventuele restrisico's/leemtes in de interne beheersing resteren en hoe uw 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.

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

Op basis van onze uitgevoerde interim-controle stellen wij vast dat er binnen uw organisatie aandacht is voor frauderisico's en de preventie daarvan, echter is dit nog niet uitgewerkt in een frauderisicoanalyse die specifiek toeziet op de BVEB. Vanwege toenemende aandacht voor Fraude, Integriteit en M&O beleid adviseren wij u deze wel op te stellen.



2. Kwaliteit interne beheersing

De verbijzonderde interne controle kan 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. 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.

Naleving M&O-beleid

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. Aangezien de naleving van het M&O-beleid onderdeel is van de rechtmatigheidsverantwoording, zou de toetsing op het naleven van het M&O beleid onderdeel moeten zijn van de werkzaamheden die gedaan worden ten behoeve van het opstellen van deze verantwoording. 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'.

Onze frauderisicoanalyse

In de afgelopen jaren is de aandacht voor fraude alleen maar toegenomen. Ook de rol van de accountant bij het signaleren van frauderisico's is afgelopen jaren veelvuldig besproken. Naar aanleiding van de rapportage van de AFM 'Scherper op frauderisico's' van 8 juni 2023 heeft onze beroepsorganisatie de aanpak van frauderisico's in de controle geëvalueerd en is deze zomer de concept Handreiking 1153 'Frauderisicoanalyse' gepubliceerd.

Tevens wijzen wij u op de gepubliceerde handreiking 1137 'Corruptie, werkzaamheden van de accountant', waarin aandacht geschonken wordt aan corruptierisico's. Wij willen u vragen om ook in de eigen frauderisicoanalyse aandacht te hebben voor mogelijke corruptierisico's binnen uw organisatie. De nadere guidance in Handreiking 1153 en 1137 kan er toe leiden dat dit gevolgen heeft voor de frauderisicoanalyse die wij voor onze controle van uw organisatie uitvoeren. Dit kan dan tevens betekenen dat wij in vergelijking met voorgaande jaren meer of andere frauderisico's identificeren.

In onze controle onderkennen wij, onder andere op basis van nieuwe inzichten op frauderisico's, de volgende fraude-risico's:

- Onrechtmatige betalingen
- Verschuiving van kosten tussen de BVEB en de gemeenten; en
- Doorbreken van interne beheersing door het management teneinde de resultaten te verbeteren

In onze controle zullen wij specifieke werkzaamheden uitvoeren om deze risico's ten behoeve van de jaarrekeningcontrole te ondervangen. Naar aanleiding van de interim-controle hebben wij geen aanwijzingen voor mogelijke fraude.



2. Kwaliteit interne beheersing

Beheersing fraude- en corruptierisico's

Als onderdeel van de interim-controle hebben wij beoordeeld of ten aanzien van de belangrijkste fraude- en corruptierisico's beheersingsmaatregelen zijn getroffen en in hoeverre wij kunnen steunen op deze maatregelen. In onderstaande tabel zijn de door ons geïdentificeerde frauderisico's opgenomen en aangegeven welke interne beheersing uw organisatie hierop heeft ingericht.

#	Fraude-/corruptierisico	Beheersingsmaatregel	Restrisico
1	Onrechtmatige betalingen	• Functiescheiding bij het autoriseren en wijzigingen van crediteurenstamgegevens • Controle op juistheid bankrekeningnummers bij betalingen • Functiescheiding in de betaalomgeving (BNG bankieren)	Laag
2	Verschuiving van kosten tussen de BVEB en de gemeenten	• Budgethouders zijn slechts verantwoordelijk voor budgetten binnen één organisatie Wij constateren dat er enkele budgethouders zijn die in meerdere organisaties terugkomen. Wij zullen bij de jaarrekeningcontrole gegevensgerichte werkzaamheden uitvoeren op lasten die door hen geautoriseerd zijn.	Midden
3	Doorbreken van interne beheersing door het management teneinde de resultaten te verbeteren	Niet te ondervangen middels interne beheersing	Midden

In onze controle zullen wij specifieke werkzaamheden uitvoeren om deze risico's ten behoeve van de jaarrekeningcontrole te ondervangen. Naar aanleiding van de interim-controle hebben wij geen aanwijzingen voor mogelijke fraude.



2. Kwaliteit interne beheersing

Samenwerking en Verbijzonderde Interne Controle

Onderwerp	Omschrijving
Organisatie	Als voorbereiding op de interim-controle hebben wij een evaluatie gedaan van het controleproces van voorgaand jaar en zijn er tussen ons en de organisatie heldere afspraken gemaakt over de verwachtingen voor het controleproces van 2024 (bijvoorbeeld ten aanzien van inkopen en aanbestedingen). Tijdens de interim-controle hebben wij op een prettige en constructieve wijze samengewerkt met uw organisatie. Belangrijke elementen in de samenwerking hierbij zien onder andere toe op: • proactieve afstemming van bijzonderheden en/of belangrijke aandachtsgebieden, bijvoorbeeld ten aanzien van opleveringen VIC en lijncontroles • inspanning om te zorgen dat alle gewenste informatie op een adequate wijze en voor aanvang van de controle aanwezig is, waarbij wij wel opmerken dat de oplevering ten aanzien van de IT-omgeving niet aanwezig waren toen onze controle was gepland • bereidheid en beschikbaarheid van medewerkers om onze vragen op een adequate wijze en tijdig te beantwoorden
Inrichting en kwaliteit VIC	Een belangrijk onderdeel van de interne beheersing is de (verbijzonderde) interne controlefunctie. Voor de uitvoering hiervan maakt u gebruik van externe inhuur en een gecertificeerd systeem om selecties en uitwerkingen in vast te leggen. Een kwalitatief goed intern controleplan bevat in onze optiek een opbouw die gebaseerd is op de financiële omvang van posten en stromen, waarin deze posten en stromen vervolgens worden gekoppeld aan relevante wet- en regelgeving en waarin de daaruit voortkomende relevante risico's zijn gedefinieerd. Wij constateren dat de VIC op deze wijze is ingeregeld. Ten tijde van de interim-controle hebben wij kennis genomen van de VIC over periode 1 (januari-mei 2024). Wij constateren dat alle geplande controles zijn uitgevoerd. Bij de VIC die uitgevoerd is op het inkoopproces zijn twee bijzonderheden geconstateerd ten aanzien van de getrouwheid en de rechtmatigheid. De eerste constatering ziet op het boeken in de juiste periode en de tweede bevinding op het vastleggen van de prestatielevering. Ten aanzien van het opstellen van de jaarrekening vragen wij u aandacht voor het beoordelen van de overlopende posten (o.a. nog te ontvangen facturen over 2024), zodat lasten toegerekend worden aan het juiste boekjaar. Volledigheidshalve merken wij op, alhoewel dit niet om materiële bedragen gaat, dat wij afgelopen jaren hier bevindingen in geconstateerd hebben, Ten aanzien van de vastleggingen prestatieverklaring merken wij op dat dit blijvende aandacht vergt. In dit kader verwijzen wij u ook naar onze detailbevinding.



2. Kwaliteit interne beheersing

Onderwerp		Omschrijving			
Three Lines Model BVEB De kleur van het symbool geeft de status van de constatering aan.		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: 1e lijn: in het primaire proces, onder verantwoordelijkheid van de proceseigenaar. 2e lijn: in de ondersteunende processen zoals financiën en control, waar checks and balances ingericht zijn om fouten te signaleren. 3e lijn: in uw verbijzonderde interne controle achteraf. Indien de beheersmaatregelen in de 1e en/of 2e 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 3e lijn (VIC) toereikend te zijn. Onderstaand overzicht geeft zodoende een beeld over de mate van beheersing en controle van uw organisatie.			
● 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					
Nr.	Proces	1 ^e lijn	2 ^e lijn	3 ^e lijn	Toelichting
1	Inkopen	●	●	●	Wij constateren dat er zowel een 1^e, 2^e, als 3^e lijn is ingericht. Wij constateren ten aanzien van de eerste lijn 2 aanbevelingen: - Aandacht voor tijdige en juiste vastlegging prestatielevering - Aandacht voor volledige documentatie van aanbestedingsdossiers
2	Lonen en Salarissen	●	●	●	Vanuit de VIC over de eerste maanden zijn geen bijzonderheden geconstateerd.
3	Memoriaalboekingen	●	Nvt	nvt	Memoriaalboekingen worden niet getoetst als onderdeel van de VIC, tevens wordt er geen gebruik gemaakt van de afgedwongen functiescheiding in Key2

3 IT omgeving





3. IT-omgeving

Inleiding

Als onderdeel van onze controleaanpak hebben wij op 16 september, 26 september en 15 oktober 2024 werkzaamheden uitgevoerd om inzicht te krijgen in uw IT-omgeving en de daarbij (eventueel) behorende risico's voor de jaarrekeningcontrole. Tijdens onze interim-controle hebben wij controlewerkzaamheden uitgevoerd op relevante IT-beheersingsmaatregelen die uw organisatie heeft genomen in de IT-processen; beheersen van de IT-operatie (IT-continuïteitsmaatregelen en uitbestede diensten), beheersen van updates (ontwikkelen en implementeren van nieuwe functionaliteit), beheersen van de identiteit van gebruikers (opzetten passende beveiligingsinstellingen) en beheersen van de bevoegdheden van gebruikers (verlenen en onderhouden van toegang). Afhankelijk van het belang van de IT-applicatie voor de jaarrekeningcontrole en uw organisatie hanteren wij een bepaalde scope waarbij wij de uitkomsten van uw IT-inrichting toetsen. Zie de onderstaande tabel op de volgende pagina voor de relevante IT-applicaties en de evaluatie van de IT-processen die door ons zijn gecontroleerd.

Samenvatting bevindingen

De tabel op de volgende pagina geeft een overzicht van onze bevindingen ten aanzien van de IT-aandachtsgebieden binnen uw organisatie. De risico's kunnen per aandachtsgebied verschillen. Bij de tabel is onze inschatting van de impact op de controle en op uw organisatie opgenomen.

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

-  Verbetering nodig
-  Adviespunt
-  Voldoende



3. IT-omgeving

Samenvatting bevindingen

Omgeving	Toegangs-beveiliging	Wijzigings-beheer	Continuïteit	Belangrijkste bevindingen en gevolgen voor de controle
Netwerk		N.v.t.		Diverse accounts zijn uitgesloten van het periodiek wijzigen van het wachtwoord. Daarnaast heeft één account van een onafhankelijke functionaris hoge rechten op het netwerk. Verder zijn er geen volledige recovery- en uitwijktesten uitgevoerd dit controlejaar.
Key2Financien				Wijzigingen worden niet aantoonbaar getest en vastgelegd. Daarnaast beschikt één onafhankelijke functionaris over hoge rechten binnen de applicatie.

Zie detailbevindingen over de IT-omgeving in de bijlagen.

4

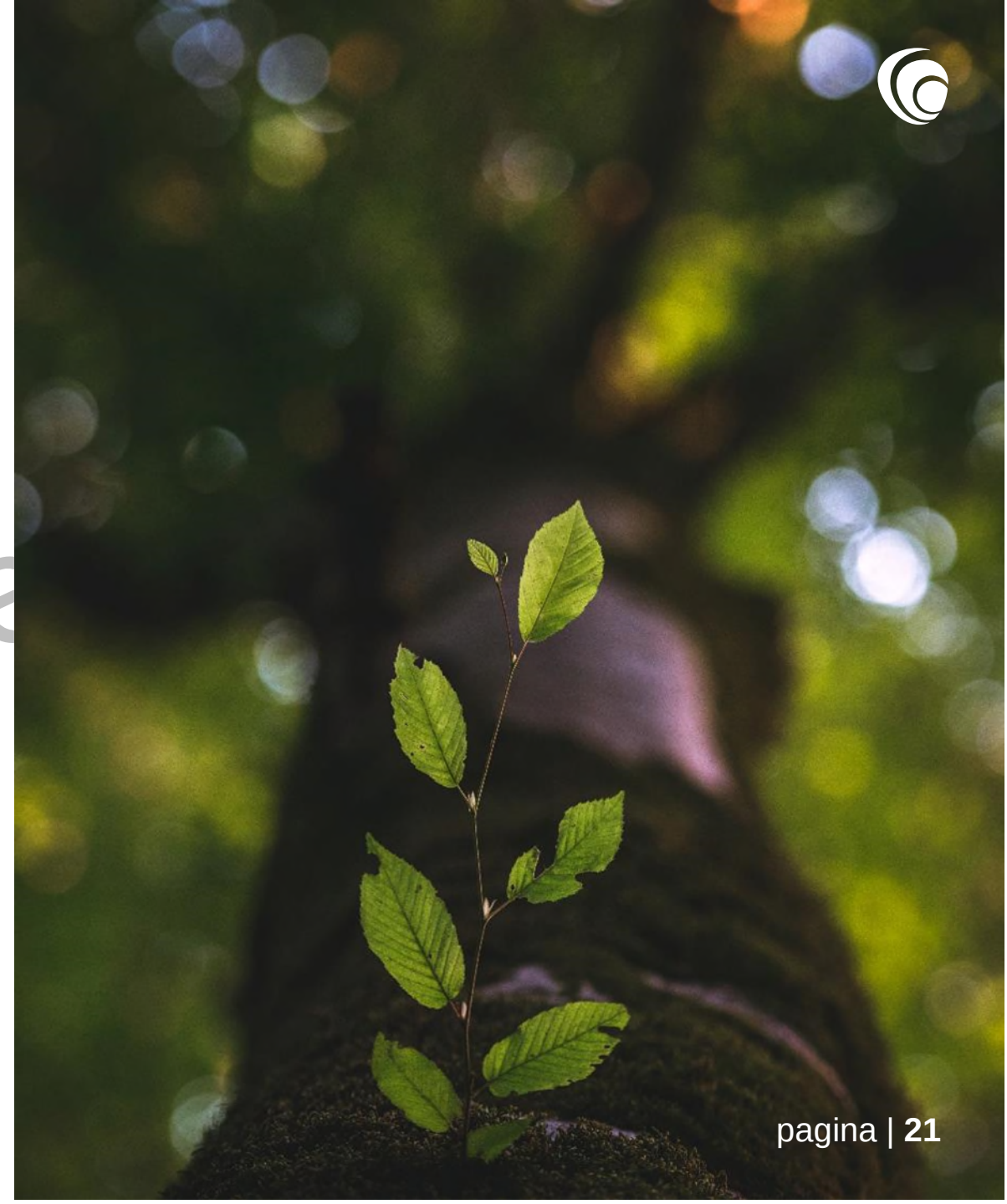
Vorbereitung jaarrekening- controle



4. Voorbereiding jaarrekening- controle

Inleiding

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





4. Voorbereiding jaarrekeningcontrole

Planning

Wij starten met de jaarrekeningcontrole op 17 februari 2025. Om de jaarrekeningcontrole efficiënt te laten verlopen is het belangrijk dat vóór deze datum een conceptjaarrekening inclusief sluitende burgstaat en controledocumentatie aanwezig is. Voor de benodigde controle-documentatie (het balansdossier) zullen wij een aparte PBC lijst aanleveren, inclusief deadlines voor de aanlevering van de documentatie.

Aanvullende gegevensgerichte werkzaamheden

Voor aanvang van de jaareinde controle zullen wij voor de belangrijkste posten (die geen onderdeel zijn van de VIC) deelwaarnemingen uitzetten. Hiervoor is het noodzakelijk dat u tijdig de administratie(s) afsluit en de auditfile(s) aan het controleteam verstrekt. Het vooraf uitzetten van onze selecties heeft als bijkomend voordeel dat uw medewerkers de benodigde controle documentatie op een door hun gekozen moment (voor aanvang van de controle) kunnen verzamelen.

Onze verwachtingen

Om een kwalitatief goede en efficiënte controle uit te voeren verwachten wij van u:

- Complexe vraagstukken worden vooraf met ons afgestemd op basis van uw eigen standpunt;
- Tijdige aanlevering van de (volledige) jaarrekening aansluitend met uw administratie en het concept jaarverslag;
- Maximaal twee versies van de jaarrekening (concept en definitief);
- Tijdige en volledige aanlevering van het balansdossier volgens de LOTS lijst;
- Uw medewerkers zijn voldoende beschikbaar om vragen (tijdig) te beantwoorden;
- Na het opmaken van de jaarrekening wordt niet meer geboekt in de administratie van het te controleren boekjaar.



4. Voorbereiding jaarrekeningcontrole

Jaarrekeningcontrole & Data-analyse

Gebruik van data-analyse in de jaarrekeningcontrole

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.
Controle op kosten die geboekt zijn door een budgethouder die budgetten beheert van meerdere organisaties (BVEB, gemeenten Zaltbommel of Maasdriel)	Middels deze analyse kunnen wij op efficiënte wijze vaststellen of kosten terecht op de juiste organisatie zijn verantwoord

5

Actualiteiten



5. Actualiteiten

Rechtmatigheidsverantwoording

Met ingang van verslagjaar 2023 hebben gemeenten, provincies en gemeenschappelijke regelingen voor het eerst een rechtmatigheidsverantwoording opgenomen in de jaarrekening. Vanaf 1 januari 2023 is de nieuwe Wet Decentrale Rekenkamers van kracht geworden. Met de aangepaste wetgeving streefde de overheid naar meer transparantie en controle op de uitgaven. Inmiddels zijn, zo goed als, alle jaarrekeningen 2023 afgetekend en zijn de eerste ervaringen met de rechtmatigheidsverantwoording duidelijk geworden.

Veel organisaties rapporteerden omvangrijke rechtmatigheidsfouten door begrotingsoverschrijdingen. Daarbij merken we op dat de foutenevaluatie omtrent begrotingsrechtmatigheid per organisatie en accountant verschilt. Dit geldt overigens ook voor het M&O-criterium, waarvoor eenduidige normen ontbreken.

Hieruit blijkt dat de kaders nog te onduidelijk zijn. Maar naast onduidelijke kaders hebben we ook nog te maken met ontbrekende wet- en regelgeving. Tot op heden is het BBV en BADO nog niet aangepast. Het streven is nog steeds om BBV en BADO in 2024 aan te passen, maar dat is afhankelijk van de agenda van de Tweede Kamer. Wel heeft de Commissie BBV de Kadernota 2024 uitgebracht. In deze aangepaste versie worden opgehaalde ervaringen verwerkt. Denk bijvoorbeeld aan een tekstuele wijziging in de rechtmatigheids-verantwoording met betrekking tot de bevinding van de verantwoording van begrotingsonrechtmatigheden. Dit alles met het doel om tot verdere verbeteringen ten komen.

Uit de eerste ervaringen blijkt dat de rechtmatigheidsverantwoording niet zoveel toegevoegde waarde heeft gecreëerd voor het bestuur als van tevoren was gehoopt. Het échte gesprek tussen de directie en het bestuur is in veel gevallen uitgebleven. Voor 2024 is het belangrijk dat het bestuur en directie in gesprek met elkaar blijven om te leren van de ervaringen uit 2023 en de kaders aan te scherpen voor 2024. We adviseren daarom om (het proces rondom) de rechtmatigheidsverantwoording 2023 te evalueren, om het rechtmatigheidsgesprek over boekjaar 2024 te bevorderen.

5. Actualiteiten

Impact van duurzaamheidsverslaggeving steeds beter zichtbaar

Met de invoering van de verplichte verantwoording over duurzaamheid / ESG in de jaarrekening van grote ondernemingen per 1 januari 2025 zien wij de aandacht hiervoor bij gemeenschappelijke regelingen ook sterk toenemen. Beleidsmatig zien we dit concreet terug in initiatieven zoals bijvoorbeeld 'Global Goals' ([Global Goals voor Gemeenten | VNG](#)). Op het gebied van verantwoording, financiën en verslaggeving constateren wij dat steeds meer wordt gevraagd van gemeenschappelijke regelingen en gemeenten. Enkele voorbeelden uit de praktijk:

- Invoering Rapportageverplichting werkgebonden personenmobiliteit per 1 juli 2024 voor de Co2-uitstoot van auto's van werknemers bij organisaties van meer dan 100 werknemers;
- Vanaf 2025 zal het hebben van een klimaatactieplan, op bedrijfs- of activaniveau, voor de meeste klanten een voorwaarde zijn om in aanmerking te komen voor BNG-financiering. De impact hiervan is hieronder nader toegelicht;
- Stakeholders in het gemeentelijk domein (BNG, Ministerie en enkele (grote) gemeenten) werken in een groep met de naam 'coalition of the willing' vanaf 2023 samen om uniforme verslaggeving voor duurzaamheid te ontwikkelen.

Onder andere als gevolg van de bovenstaande ontwikkelingen heeft de commissie BBV duurzaamheidsverslaggeving ook op haar agenda gezet. Een eerste belangrijke stap voor het ontwikkelen van verslaggevingseisen voor gemeenten op het gebied van duurzaamheid. Als Baker Tilly dragen we op landelijk niveau bij door mee te denken over een goede, maar ook praktisch uitvoerbare, route naar duurzaamheidsverslaggeving voor gemeenten en gemeenschappelijke regelingen. Uit onze ervaring bij de invoering van ESG bij grote ondernemingen weten wij dat analyses van de belangrijkste te rapporteren waarden (door middel van een materialiteitsanalyse) en het betrouwbaar registreren van deze waarden essentieel zijn om tot een goede verantwoording te komen. Op tijd starten is daarom belangrijk. Wij helpen u als organisatie graag om de ontwikkelingen scherp te volgen en hierin de eerste stappen te zetten.



5. Actualiteiten

Impact van Sustainability op kredietverlening BNG Bank

De BNG Bank verduurzaamt haar eigen activiteiten en streeft naar een klimaatneutrale bedrijfsvoering. Sustainability heeft een centrale plek in de strategie van de BNG Bank. De BNG Bank wil gezamenlijk optrekken met de grootste sectoren waarin de bank actief is, om de uitstoot van de eigen organisatie én de emissies verbonden aan de kredietportefeuille terug te dringen. De BNG Bank heeft in haar Klimaatplan ([Klimaatplan – Going Green \(bngbank.nl\)](https://www.bngbank.nl/klimaatplan)) belangrijke doelen gesteld voor het behalen van klimaatdoelstellingen. Onderdeel hiervan is het niet meer financieren van organisaties die onvoldoende bijdragen aan deze klimaatdoelstellingen.

Investerders hechten ook grote waarde aan ESG voor wat betreft de klantacceptatie en kredietverleningen door de BNG Bank. Gemeenschappelijke regelingen hebben er baat bij om duurzaamheid in beeld te brengen om daarmee het investerend vermogen bij de BNG Bank te borgen. Als investeerders zich terugtrekken heeft dit namelijk gevolgen voor de financieringskosten voor de BNG Bank en drijft het de rente van kredietverlening omhoog. In het Sustainability beleidsdocument beschrijft de BNG Bank dat bij hun klanten voortgang op maatschappelijke doelstellingen wordt verwacht. Hiervoor gebruikt de BNG Bank strategische klantgesprekken en een ESG-rating model. Daarbij wordt informatie gebruikt rondom Co2-intensiteit en omgang met klimaatrisico's. Daarbij is het noodzaak voor organisaties om te beschikken over een eigen klimaatdoelstelling.

Notities BBV

Per 1 januari 2024 zijn verschillende notities ingrijpend gewijzigd. Dat zijn:

- Notitie grondbeleid in begroting en jaarstukken
- Notitie rente
- Notitie overhead

Wij vragen aandacht voor deze notities en we verzoeken het bestuur om te bepalen welke aanpassingen binnen uw organisatie gedaan moeten worden naar aanleiding van de notities. Met name de notitie overhead zal voor uw organisatie relevant zijn.



5. Actualiteiten

IT- NIS2

In Nederland is de Cyberbeveiligingswet (verder: Cbw) in ontwikkeling welke vanaf 2025 verplicht zal worden en de EU richtlijn NIS2 (verder: Network and Information Systems Directive) implementeert. De wet is uit de consultatieronde en wordt na de zomer definitief gemaakt voor invoering naar verwachting in voorjaar 2025. Dit heeft betrekking op meerdere sectoren, waaronder de sector waar uw organisatie onder valt.

Er worden strengere eisen gesteld aan de beveiliging van netwerk- en informatiesystemen. Organisaties worden onder de Cbw meer dan nu verplicht om te zorgen voor de beveiliging van de hele keten waar zij deel van uitmaken. Op basis van het risico in de leveringsketen zullen zij cybersecurity maatregelen moeten opleggen aan hun leveranciers. Die groep leveranciers zal ook digitaal veiliger moeten gaan werken. Daarnaast komt er een verplichte registratie en meldplicht voor incidenten (naast degene die al bestaat voor privacy). Er worden maatregelen ingevoerd om de naleving van de NIS2 richtlijn te verzekeren, inclusief financiële sancties voor niet-naleving. Tenslotte dient het bestuur zich beter te laten voorlichten over inhoud en status van de cyberbeveiliging.

Wij adviseren om vanuit een actueel inzicht in de IT-objecten en gegevens in de keten waarvan uw organisatie deel uitmaakt de risico's te benoemen en maatregelen en contractuele afspraken scherp in beeld te hebben. Daarop aanvullend dienen vervolgens een aantal basis hygiëne maatregelen conform de nieuwe wet ingericht te worden. Wij hebben hiervoor een stappenplan ontwikkelt en kunnen u hierbij ondersteunen. Wij adviseren u een gap analyse uit te voeren in relatie tot de vereisten vanuit NIS2 zodat u vast kan stellen welke maatregelen eventueel nog geïmplementeerd dienen te worden.

6 Bijlagen





6. Bijlagen

Detailbevindingen interne beheersing – Bevindingen per proces

Op de volgende pagina's zijn de detailbevindingen ten aanzien van de belangrijkste processen opgenomen. Per pagina is een bevinding opgenomen met daarbij het risico en de aanbeveling. Bij elke bevinding is het jaar van de eerste vermelding vermeld, evenals de geschatte kans van voorkomen en de impact op uw organisatie. Daarnaast hebben wij de gevolgen voor de controle beschreven. Tot slot verzoeken wij het management om een reactie te geven op de bevindingen.

Bevinding	Titel bevinding	Kans:	Hoog/middel/laag
Jaar van constateren	Boekjaar eerste vermelding	Impact:	Hoog/middel/laag
Constatering	Status bevinding: Nieuw / (Geen) Actie ondernomen / Opgelost		
Risico	In dit blok wordt aangegeven wat gedurende de accountantscontrole is geconstateerd en waarvan wij u graag op de hoogte willen brengen.		
Aanbeveling	Hier beschrijven wij de risico's van de bevinding en wat de gevolgen voor uw onderneming kunnen zijn.		
Gevolgen voor de jaarrekening-controle	Hier geven wij u aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.		
	Op deze plaats beschrijven wij de gevolgen van de bevinding voor de controleaanpak en de omvang van onze controlewerkzaamheden.		



6. Bijlagen

Detailbevindingen interne beheersing – Bevindingen per proces

Bevinding	Autorisaties bij goedkeuring inkoopfacturen		Kans:	Middel
Jaar van constateren	2024	Status bevinding: Nieuw	Impact:	Middel
Constatering	Wij constateren dat bij afwezigheid vervangende functionarissen geselecteerd kunnen worden om een inkoopfactuur goed te keuren. In de applicatie is niet ingeregeld dat hierbij het 4-ogenprincipe wordt afgedwongen. Tevens is het mogelijk om hier medewerkers van de financiële afdeling voor te selecteren.			
Risico	Bij het goedkeuren van inkoopfacturen kan een vervangende functionaris (functionarissen die bij afwezigheid de autorisaties in de workflows overnemen) gekoppeld worden, waarbij het risico bestaat op het doorbreken van het 4-ogenprincipe.			
Aanbeveling	Wij raden aan om deze autorisaties te bespreken en te beleggen bij onafhankelijke functionarissen.			
Gevolgen voor de jaarrekening-controle	Gezien de beperkingen ten aanzien van het de autorisaties kan bij de controle niet op de control ten aanzien van 4-ogenprincipe op het inkoopproces worden gesteund. Hiervoor dient per einde jaar data-analyse plaats te vinden, om vast te stellen of het 4-ogenprincipe het gehele jaar is toegepast.			



6. Bijlagen

Detailbevindingen interne beheersing – Follow-up overige bevindingen voorgaande jaren

Onderstaande tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze managementletters van voorgaande jaren, voor zover deze niet afzonderlijk zijn behandeld bij de detailbevindingen.

#	Bevinding	Follow-up 2024	Status 2024
1	Tijdens onze controle hebben wij vastgesteld dat de onderbouwing van de prestatielevering niet altijd op een juiste wijze is onderbouwd.	Wij constateren dat het instrueren van uw medewerkers blijvende aandacht vraagt. Voornaamste aandachtspunt is hierin het tijdig en juist instrueren van de nieuwe medewerkers.	Blijvend aandachtspunt
2	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.	Vanuit de organisatie is aangegeven dat het juist en volledig documenteren van het aanbestedingsdossier nog steeds aandacht vergt.	Aanbeveling t.a.v. aansturing bij inkoopprocedures
3	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.	Ten opzichte van voorgaand jaar zijn er geen wijzigingen in het proces.	Vanwege andere prioritering niet verder opgevolgd.



6. Bijlagen

Bijlage: IT General Controls

Wij hebben de beheersing van uw IT-omgeving onderzocht. Op basis van onze werkzaamheden hebben wij een inschatting gemaakt van de kwaliteit van de IT-omgeving. Bij onze werkzaamheden hebben wij aandacht besteed aan onderstaande onderwerpen. Op de volgende pagina's rapporteren wij onze bevindingen.

Onze bevindingen ten aanzien van de IT-omgeving zijn als volgt geclassificeerd:

-  Verbetering nodig
-  Adviespunt
-  Voldoende

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 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.



6. Bijlagen

Wijzigingsbeheer

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.

Continuïteit 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.

Overige adviespunten

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.



6. Bijlagen

IT - Detailbevindingen interne beheersing – Toegangsbeveiliging netwerk

	Authenticatie 	Autorisatie 
Constatering	De wachtwoordvereisten die afgedwongen worden op het netwerk voldoen aan de Baker Tilly best practice. Wij hebben echter vastgesteld dat meerdere accounts (w.o. 3 persoonlijke) zijn uitgesloten van het periodiek wijzigen van het wachtwoord. Van deze gebruikers verloopt het wachtwoord niet.	Op het netwerk hebben wij 17 gebruikers met hoge rechten geïdentificeerd. Één gebruiker is direct betrokken bij het primaire proces en wordt derhalve niet onafhankelijk. Op dit moment worden autorisaties niet toegekend op basis van een functie-autorisatiematrix. Er is een start gemaakt met het controleren van de toegang tot het netwerk, echter vindt er nog geen aantoonbare controle plaats op de autorisaties.
Risico	Door het ontbreken van een maximale wachtwoordduur bestaat de kans dat gebruikers op een ander gebruikersaccount kunnen inloggen. Echter gezien deze persoonlijke accounts niet hebben ingelogd in 2024, betreft dit geen verhoogd risico voor de jaarrekeningcontrole. Wel dient de logging van deze persoonlijke accounts zonder wachtwoordperiodiciteit in de gaten te houden.	Het risico bestaat dat bedoelde functiescheiding binnen het netwerk wordt doorbroken. Gebruikers met hoge rechten kunnen gebruikers aanmaken en rechten en rollen toekennen om zo functiescheiding te omzeilen. 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 systeemtechnisch een maximale wachtwoordduur af te dwingen waarbij het wachtwoord minimaal jaarlijks gewijzigd dient te worden. Daarnaast bevelen wij aan om periodiek de wachtwoordinstellingen te controleren en te beoordelen.	Wij bevelen aan om hoge rechten te beperken en deze te beleggen bij onafhankelijke functionarissen. Daarnaast 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
Gevolgen voor de jaarrekeningcontrole	Gezien de beperkingen ten aanzien van de toegangsbeveiliging kan hier bij de controle niet op worden gesteund. De beperkingen tot de authenticatie op het netwerk hebben geen directe impact op de jaarrekeningcontrole, aangezien wij voor Key2Financien hebben vastgesteld dat de gebruikers in dit systeem niet uitgezonderd zijn van het periodiek wijzigen van het wachtwoord.	



6. Bijlagen

IT - Detailbevindingen interne beheersing – Toegangsbeveiliging en wijzigingsbeheer Key2Financiën

	Authenticatie 	Autorisatie 	Wijzigingsbeheer 
Constatering	Voor het inloggen binnen Key2Financiën wordt gebruikt van Single Sign On (SSO). Dit betekent dat de wachtwoordeisen van het netwerk gebruikt worden. Er zijn geen gebruikers binnen de applicatie uitgezonderd van het afgedwongen wachtwoordbeleid op het netwerk.	Binnen de applicatie hebben wij 4 gebruikers met hoge rechten geïdentificeerd. Eén van deze gebruikers is direct betrokken bij het primaire proces. 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 in een testplan. Hiervoor hebben we echter vernomen dat momenteel een voorbeeldtestplan wordt bestudeerd voor de komende release.
Risico	-	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. De kans bestaat dat er wijzigingen worden doorgevoerd met impact op de betrouwbare gegevensverwerking van de applicatie.
Aanbeveling	-	Wij bevelen aan om hoge rechten te beperken en deze te beleggen bij onafhankelijke functionarissen. Daarnaast om een functie-autorisatiematrix stellen en te gebruiken bij het toekennen van rechten. Tenslotte 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	Gezien de beperkingen ten aanzien van het autorisatie en change management proces kan bij de controle niet op worden gesteund. Per jaareinde zullen wij kijken naar de autorisaties en goedkeuringen van functionarissen met hogere rechten, waardoor het resterende risico wordt ondervangen.		



6. Bijlagen

IT - Detailbevindingen interne beheersing – Continuïteitsmaatregelen en beveiliging

Onderstaande onderwerpen volgen uit interviews. 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.

Onderwerp	Bevinding
Back-up	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	Wij hebben vernomen dat in de dagelijkse praktijk bestanden regelmatig hersteld moeten worden wanneer hiertoe verzoeken worden ingediend, naast deze activiteiten worden geen recoverytests uitgevoerd. Wij bevelen u aan om tenminste jaarlijks een recovery test uit te voeren. Echter hebben wij hiervoor vernomen dat recoverytesten zullen plaatsvinden na de nieuwe infrastructuur inrichting.
Uitwijk	Een uitwijklocatie is ingericht, echter is aangegeven dat de laatste uitwijktest in 2021 plaats heeft gevonden. Wij bevelen u aan om tenminste jaarlijks een uitwijktest uit te voeren. Ook hiervoor hebben wij vernomen dat de uitwijktest plaats zal vinden na de nieuwe inrichting van de infrastructuur.
Fysieke beveiliging	De servers zijn ondergebracht op twee locaties. Toegang tot deze ruimtes is beperkt tot noodzakelijke medewerkers van het cluster ICT.
Remote acces	Voor extern inloggen wordt gebruik gemaakt van een VPN verbinding, middels een versleutelde verbinding. Het risico dat externen zich toegang verschaffen tot de Windows omgeving is hierdoor beperkt. Daarnaast is two-factor authenticatie ingesteld voor inloggen op de Office 365 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.
Incident	Uit het interview is vernomen dat er een incident heeft plaatsgevonden waarbij servers corrupt zijn geraakt. Hierbij is ons medegedeeld dat dit is hersteld zonder dat dit impact heeft gehad op de financiële data. Bij de balanswerkzaamheden kan hier nog op terug gekomen worden door de accountant.

Contact

Drs. R. (Rik) Opendorp RA

Partner Audit

r.opendorp@bakertilly.nl

E.D. (Linda) de Vries RA MSc.

Senior Manager Audit

l.devries@bakertilly.nl

Kantoorgegevens

Baker Tilly Breda

Bijster 39

4817 HZ Breda

T: 076 525 00 00

Baker Tilly (Netherlands) N.V. trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

