Management letter

Gemeente Oldebroek
Boekjaar 2024

Aanbiedingsbrief

Aan het College van Burgemeester en Wethouders van de gemeente Oldebroek
Raadhuisplein 1
8096 CP Oldebroek

Onderwerp: Management letter 2024
Kenmerk: definitief d.d. 20 februari 2025

Geacht College,

Als onderdeel van de jaarrekeningcontrole van boekjaar 2024 van de gemeente Oldebroek rapporteren wij u onze bevindingen uit de interim-controle.

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 college 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. E.H.J.D. Damman RA

Inhoud

1 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.
Algemene conclusie interne beheersing	De gemeente Oldebroek heeft de afweging gemaakt om het opvolgen van meerdere bevindingen mee te nemen bij de implementatie van het nieuw financieel systeem per 2025. De verwachting is dat volgend jaar een groot aantal bevindingen worden opgepakt en opgelost. We zien dat de gemeente Oldebroek vanuit prioritering actief bevindingen oppakt binnen de aanwezige mogelijkheden.
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 de applicaties Civision Middelen en Civision Samenlevingszaken bekeken. We hebben geconstateerd dat voor het onderdeel autorisatie de gemeente daar (niet enkel in het kader van de jaarrekeningcontrole) risico loopt. Wij adviseren u daaraan opvolging te geven.
Rechtmatigheids-verantwoording	In oktober 2024 heeft de commissie BBV de Kadernota Rechtmatigheid 2024 gepubliceerd. Hierin is een aantal zaken verder verduidelijkt rondom de rechtmatigheidsverantwoording die moet worden opgesteld door het college van B&W. Daarnaast is de verplichting tot het opnemen van geconstateerd misbruik waarbij het M&O beleid is toegepast en heeft geleid tot bijvoorbeeld terugvorderingen en het opleggen van sancties, in de rechtmatigheidsverantwoording vervallen. Tot slot is de voorgeschreven tekst van de rechtmatigheidsverantwoording aangepast. Deze moet worden overgenomen in de jaarstukken 2024. Daarnaast was vorig jaar sprake van onduidelijkheid in de wet- en regelgeving over bruto en netto begrotingsoverschrijdingen. Aangezien het aanpassen van BBV en BADO waarschijnlijk niet tijdig zal lukken voor de afwikkeling van de jaarrekeningcontrole 2024 betekent dit dat in een oplegnotitie een aantal zaken nader zullen worden geduid uit de Alert 48 die ook in 2024 van toepassing zal zijn. Als uitgangspunt ten aanzien van de weging van de begrotingsafwijkingen in samenhang met de andere rechtmatigheidsfouten en/of onduidelijkheden geldt dat uw college bij de conclusie of ze rechtmatig heeft gehandeld de bruto onrechtmatigheden weegt (zonder onderscheid te maken naar acceptabel en niet acceptabel).
Voorbereidingen jaarrekeningcontrole	We maken met uw gemeente afspraken over de planning van de jaarrekeningcontrole 2024. Op voorhand identificeren we een aantal onderwerpen waarop wij uw aandacht vragen, welke in het afzonderlijke hoofdstuk zijn benoemd.
Actuele ontwikkelingen	Vanuit het oogpunt van onze natuurlijke adviesfunctie in deze management letter 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.

2 Kwaliteit interne beheersing

2. Kwaliteit interne beheersing

Inleiding

Deze management letter 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 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 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 management letter 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 gemeente 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 gemeente onderkende risico's/ kernpunten in de controle zijn:

- Het risico dat inkoopfacturen niet in overeenstemming zijn met de geleverde prestatie omdat de prestatie niet is ontvangen. Dit risico ziet bij uw gemeente met name toe op de investeringen en kosten;
- Risico dat het management van de gemeente de procesafspraken doorbreekt (management override of controls), hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de realisatieruimte binnen budgetten in de exploitatie- en investeringsbudgetten (standaard risico binnen de branche);
- Corruptierisico ten aanzien van inkoopcontracten met een contractwaarde groter dan 3x de uitvoeringsmaterialiteit door mogelijke belangenverstrengeling en kickbacks (standaard risico binnen de branche);
- Onterechte betalingen doordat onjuiste mutaties doorgevoerd worden in crediteurenstamgegevens of in de daadwerkelijke batchopdrachten;

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

Financieel

We hebben geen nieuwe bevindingen geconstateerd in het huidige boekjaar. De openstaande bevinding is onderhanden.

Sociaal Domein

We hebben geen nieuwe bevindingen geconstateerd m.b.t het sociaal domein. Van 2 van de 3 openstaande bevindingen hebben wij ontwikkelingen vernomen ten opzichte van voorgaand jaar.

Subsidie-verstrekking

Van de openstaande bevindingen is ten opzichte van voorgaand jaar een bevinding opgelost.

Status bevindingen

- **Geen actie: 2**
- **Onderhanden: 7**
- **Opgelost: 1**
- **Nieuw: 1**
- **Bewust niet opgevolgd: 1**
- **Geaccepteerd risico: 3**

Aanbesteding, inkoop & betaling

Van de 4 openstaande bevindingen uit voorgaand jaar zijn 3 bevindingen onderhanden.

Personeel

Naast de onderhanden bevinding is ten opzichte van voorgaand jaar één nieuwe bevinding geconstateerd.

IT omgeving

We hebben geen nieuwe bevindingen geconstateerd in het huidige boekjaar. Het onderdeel authenticatie van het netwerk heeft verslechtering laten zien, terwijl dit in Civision Samenlevingszaken is verbeterd.

Omgevings-vergunningen

Op de openstaande bevindingen heeft ten opzichte van voorgaand jaar geen ontwikkelingen plaatsgevonden.

2. Kwaliteit interne beheersing

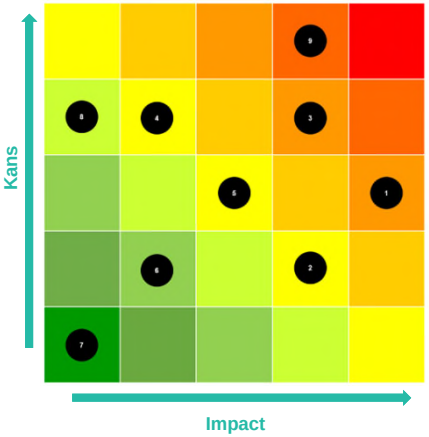
Belangrijkste aanbevelingen

In onderstaand overzicht zijn de belangrijkste aanbevelingen naar aanleiding van onze werkzaamheden opgenomen. Een gedetailleerde beschrijving van de detailbevindingen is opgenomen in bijlage (onderdeel 6 van deze management letter). 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
- Bewust niet opgevolgd

#	Herkomst	Proces	Bevinding	Status
1	2024	Personeel	Uitbesteding salarisverwerking	
2	2023	Betalingen	Zelfstandige betalingsbevoegdheden Rabobank	
3	2022	Betalingen	Belprocedure wijziging crediteurenstamgegevens Civision middelen	
4	2022	Uitkeringen	Collegiale toetsing en kwaliteitsplan	
5	2020	Aanbestedingen	Juiste aanbestedingsvorm	
6	2017	Subsidieverstrekkingen	Verordening	
7	2017	Inkopen	Prestatielevering	
8	2017	Personeel	Standenregister	
9	2017	Sociaal domein	Prestatielevering WMO	
10	2017	Sociaal domein (WMO)	Toets kwaliteits-medewerker	
11	2017	Schattingsposten	Grondexploitatie en voorzieningen	
12	2023	Omgevingsvergunningen	Bouwkostentoets	
	Geaccepteerd risico			
13	2018	Omgevingsvergunningen	Volledigheidscontrole legesregels en factuurregels	
14	2017	Omgevingsvergunningen	Controle bevoegdheden autorisatie	
15	2017	Subsidieverstrekkingen	Functiescheiding	

2. Kwaliteit interne beheersing



Frauderisicoanalyse

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude (waaronder corruptie) berust bij het college van burgemeester en wethouders. 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 gemeente. Hierin kan voor processen waar materiële opbrengsten-/kostenstromen mee zijn gemoeid, inzichtelijk worden gemaakt:

- Welke frauderisico's de gemeente onderkent;
- Wat de geschatte kans en impact van deze frauderisico's is;
- Wat de risicorespons van de gemeente is, idealiter afgestemd op de risicobereidheid van de gemeente 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 de gemeente deze ondervangt (bijvoorbeeld via de verbijzonderde interne controle).

Op basis van onze uitgevoerde interim-controle stellen wij vast dat er binnen de gemeente 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 gemeente een interne fraude-risicoanalyse heeft opgesteld en signaleert welke beheersmaatregelen aanwezig zijn. Vanuit ons optiek zou het plan verder geprofessionaliseerd kunnen worden door de kans- en impactweging van frauderisico's via een risicomatrix weer te geven 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.

Belangrijkste prioriteit die vanuit ons optiek vanuit de interim-controle naar voren komt is het risico dat facturen worden goedgekeurd waar geen prestatie voor uw gemeente tegenover staat. Binnen uw organisatie is namelijk niet technisch (geautomatiseerd) afgedwongen dat facturen door twee personen worden gecontroleerd op prestatielevering (functiescheiding: prestatieakkoordverklaarder en budgethouder).

2. Kwaliteit interne beheersing

Wij merken 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 moet 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.

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 dan wel het betalen van heffingen. 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 gemeente uitvoeren. Dit kan dan tevens betekenen dat wij in vergelijking met voorgaande jaren meer of andere frauderisico's identificeren.

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 deze risico's weergegeven.

#	Fraude-/corruptierisico	Interne beheersingsmaatregel
1	Het risico dat inkoopfacturen niet in overeenstemming zijn met de geleverde prestatie omdat de prestatie niet is ontvangen. Dit risico ziet bij uw gemeente met name toe op de investeringen en kosten;	Nee
2	Risico dat het management van de gemeente de procesafspraken doorbreekt (management override of controls), hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de realisatieruimte binnen budgetten in de exploitatie- en investeringsbudgetten (standaard risico binnen de branche);	Nee
3	Corruptierisico ten aanzien van inkoopcontracten met een contractwaarde groter dan 3x de uitvoeringsmaterialiteit door mogelijke belangenverstrengeling en kickbacks (standaard risico binnen de branche);	Nee
4	Onterechte betalingen doordat onjuiste mutaties doorgevoerd worden in crediteurenstamgegevens of in de daadwerkelijke batchopdrachten.	Ja

Idealiter sluiten de door ons onderkende frauderisico's in onze controleaanpak aan op de frauderisicoanalyse zoals opgesteld door het college, en de toelichting van het college op de eventuele frauderisico's in de paragraaf bedrijfsvoering in de jaarrekening. De passages die wij voornemens zijn op te nemen in de controleverklaring stemmen wij tijdig met u af en zullen wij bij de bespreking van het accountantsverslag met u doornemen.

3 IT-omgeving

3. IT-omgeving

Strategie en ambitie

De IT-strategie van de organisatie is gericht op het verbeteren van de IT-processen en het optimaal inrichten van het IT landschap. Dit vormt de basis voor een goed proces. Wij hebben geconstateerd dat uw organisatie verbetering heeft doorgevoerd op de volgende aspecten in het IT-landschap gedurende 2024:

- Implementatie- en migratietraject voor Unit4 ERPx als nieuw financieel systeem voor de H2O gemeenten is op dit moment in volle gang.
- Vooruitgang in de geplande transities en implementatie van het gewenste IT-landschap voor de toekomst. Denk hierbij aan het in gebruik nemen van Level als nieuwe applicatie voor Waarderings- en Belastingen processen.

Afgelopen jaar hebben we geconstateerd dat IT-processen en controles voor de relevante IT-applicaties niet altijd geschikt zijn om alle relevante IT-risico's in voldoende mate te mitigeren. We hebben vastgesteld dat deze observaties nog steeds van toepassing zijn vanwege:

- Maatregelen worden nog geactualiseerd, en daarna geïmplementeerd (het logische toegangsbeleid wordt op dit moment geactualiseerd, geen periodieke reviews en analyses op actieve gebruikers en periodieke reviews en analyses op functiescheiding worden uitgevoerd op basis van toegewezen gebruikersrechten).

Om de IT-processen en de IT-beheersingsmaatregelen verder te verbeteren, herhalen wij de aanbeveling van vorig jaar om:

- De regiefunctie op Service Level Agreement (SLA)- en contractmanagement (ook bij het monitoren op continuïteit- en beveiligingsmaatregelen van Cloud diensten) zoals opgenomen in het jaarplan Informatie Beveiliging (IB) 2024 te implementeren. Dit wordt in 2025 verder opgepakt;
- Het Strategisch Bedrijfscontinuïteitsplan (BCP) te implementeren;
- Een Information Security Management System (ISMS) tool te implementeren en de belegging van verantwoordelijkheden omtrent cybersecurity te formaliseren.
- Het logisch toegangsbeveiligingsbeleid te implementeren zodra deze is geactualiseerd.

3. IT-omgeving

Samenvatting bevindingen

Als onderdeel van onze controleaanpak hebben wij op 9 oktober 2024 werkzaamheden uitgevoerd om inzicht te krijgen in uw IT-omgeving en de daarbij (eventueel) behorende risico's voor de jaarrekeningcontrole. 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

Omgeving	Authenticatie	Autorisatie	Wijzigings-beheer	Proces
Netwerk			N.v.t.	Algemeen
Civision Middelen				Financiële administratie
Civision Samenlevingszaken				Sociaal Domein
Youforce	N.v.t.	N.v.t.		HR- en Salarisverwerking

3. IT-omgeving

Detailbevindingen interne beheersing – Toegangsbeveiliging netwerk

	Authenticatie	Autorisatie
Constatering	De ingestelde wachtwoordeisen van het netwerk zijn van voldoende niveau. Er zijn H2O-breed 87 actieve accounts uitgezonderd van het periodiek wijzigen van het wachtwoord die langer dan een jaar het wachtwoord niet hebben gewijzigd. Dit zijn voornamelijk service accounts, maar ook 10 accounts met verhoogde rechten op het netwerk. Wij hebben niet kunnen vaststellen dat Multi Factor Authentication (MFA) voor de gehele periode was ingeschakeld voor alle gebruikers. Er wordt een periodieke controle uitgevoerd op actieve gebruikers. Deze controle is echter niet geheel zichtbaar vastgelegd en ziet niet toe op de inrichting van de wachtwoordinstellingen. Ook hebben 89 persoonsgebonden gebruikers gemiddeld genomen al meer dan 2 jaar niet of nooit eerder ingelogd.	De hoge rechten in de Windows Active Directory zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole. Er vindt een systeemtechnische check plaats op de juistheid van administrator accounts. Wij hebben vastgesteld dat hoge administrator rechten na 4 uur vervallen en opnieuw aangevraagd moeten worden met een geldige reden. Er wordt geen zichtbare periodieke controle uitgevoerd op toegangsrechten van gebruikers(groepen) tot gedeelde mappen binnen de netwerkomgeving.
Risico	Het risico bestaat dat ongeautoriseerde personen toegang kunnen krijgen tot het netwerk.	Het risico bestaat dat bedoelde functiescheiding binnen het netwerk, en daarmee in potentie ook tot de applicatie wordt doorbroken. Gebruikers met hoge rechten kunnen gebruikers aanmaken en rechten en rollen toekennen om zo functiescheiding te omzeilen.
Aanbeveling	• Wij adviseren u na te gaan of het uitzonderen van wachtwoordverloop voor deze accounts passend is. Vanuit jaarrekeningcontrole perspectief is ons advies het wachtwoordverloop op alle accounts m.u.v. service accounts van toepassing te verklaren, te implementeren en bewaken; • Wij adviseren daarnaast om accounts die langer dan een jaar niet hebben ingelogd kritisch te bekijken en te bepalen of deze accounts niet verwijderd kunnen worden of inactief kunnen worden gezet, en dit te documenteren.	Wij adviseren om een functie-autorisatiematrix op te stellen (SOLL positie) en om de periodieke controle zichtbaar vast te leggen. Op basis van de functie-autorisatiematrix kunnen de ingerichte autorisaties op netwerkniveau periodiek worden gecontroleerd (IST).
Gevolgen jaarrekening-controle	De beperkingen hebben geen directe impact op de jaarrekeningcontrole. De beperkingen zouden kunnen leiden tot ongeautoriseerde toegang door onbevoegde personen welke uw organisatie zouden kunnen schaden.	

3. IT-omgeving

Detailbevindingen interne beheersing – Toegangsbeveiliging en wijzigingsbeheer Civision Middelen

	Authenticatie	Autorisatie	Wijzigingsbeheer
Constatering	De ingestelde wachtwoordeisen zijn van voldoende niveau. Er zijn 5 actieve accounts uitgezonderd van het periodiek wijzigen van het wachtwoord die langer dan een jaar het wachtwoord niet hebben gewijzigd. 4 van deze accounts beschikken tevens over verhoogde rechten. Wij hebben vernomen dat er een periodieke controle plaatsvindt op actieve gebruikers. De uitvoering van deze controle wordt echter niet geheel zichtbaar vastgelegd. De gehanteerde wachtwoordinstellingen worden niet periodiek gecontroleerd.	De hoge rechten voor Civision Middelen voor het muteren van gebruikers zijn niet belegd bij onafhankelijke functionarissen. Deze medewerkers zijn werkzaam binnen de Financiële Administratie en Belastingen, en zijn hiermee direct betrokken bij primaire processen. Daarnaast zijn hoge rechten belegd bij 1 taxateur en 1 WOZ medewerker. Er vindt geen zichtbare periodieke controle plaats op gebruikers en gebruikersrechten binnen de applicatie o.b.v. een formeel vastgestelde functie-autorisatie matrix.	Er vindt geen zichtbare vastlegging plaats van de risicoanalyse. De testwerkzaamheden worden niet altijd zichtbaar gedocumenteerd. Afsluitend vindt er een goedkeuring plaats voor het doorvoeren van de wijzigingen in de productieomgeving.
Risico	Het risico bestaat dat ongeautoriseerde personen toegang kunnen krijgen tot de applicatie. Van de 5 accounts vormen 4 accounts een verhoogd risico, omdat deze tevens over administrator rechten beschikken.	Het risico bestaat dat bedoelde functiescheiding binnen de applicatie wordt doorbroken, doordat gebruikers met hoge rechten, rechten en rollen kunnen toekennen om zo functiescheiding te omzeilen.	Door het ontbreken van vastlegging van risicoanalyses bestaat de kans dat niet alle risicovolle functionaliteiten met de juiste impact kan worden getest en dat eventuele bevindingen vanuit de testwerkzaamheden niet wordt geadresseerd.
Aanbeveling	• Wij adviseren u om na te gaan of het uitzonderen van wachtwoordverloop voor deze accounts passend is en het wachtwoordverloop op alle accounts m.u.v. service accounts van toepassing te verklaren, te implementeren en bewaken; • Wij adviseren voor accounts die langer dan een jaar niet hebben ingelogd te documenteren of deze accounts niet verwijderd kunnen worden of inactief kunnen worden gezet.	• Wij adviseren u om de accounts met hoge rechten te beleggen bij onafhankelijke functionarissen; • Wij adviseren u om de functie-autorisatie matrix (SOLL) formeel vast te stellen en periodiek te controleren op juistheid en actualiteit; • Wij adviseren u om de periodieke controle zichtbaar vast te leggen aan de hand van de functie-autorisatiematrix (IST).	Wij adviseren u om een risicoanalyse uit te voeren voor het doorvoeren van wijzigingen, en op basis daarvan een testplan op te stellen van de uit te voeren testwerkzaamheden. Vervolgens dient de uitvoering en het go / no go moment naar productie te worden vastgelegd.
Gevolgen jaarrekening-controle	Voor de jaarrekeningcontrole heeft dit tot gevolg dat wij, met uitzondering van 5 accounts, op authenticatie in de applicatie kunnen steunen.	Voor de jaarrekeningcontrole heeft dit tot gevolg dat wij niet op autorisaties in de applicatie kunnen steunen, en mogelijk aanvullende werkzaamheden moeten uitvoeren.	Op basis van de bevindingen kunnen wij niet steunen op uw proces omtrent het gestructureerd doorvoeren van nieuwe wijzigingen en heeft aanvullend tot gevolg dat wij de releasenotes analyseren. Op basis van deze werkzaamheden zijn er geen bevindingen geconstateerd.

3. IT-omgeving

Detailbevindingen interne beheersing – Toegangsbeveiliging en wijzigingsbeheer Civision Samenlevingszaken

	Authenticatie	Autorisatie	Wijzigingsbeheer
Constatering	De ingestelde wachtwoordeisen zijn van voldoende niveau. Er zijn geen actieve accounts uitgezonderd van het periodiek wijzigen van het wachtwoord die langer dan een jaar het wachtwoord niet hebben gewijzigd. Er wordt echter geen zichtbare periodieke controle uitgevoerd op actieve gebruikers en de gehanteerde wachtwoordinstellingen.	De hoge rechten voor Civision Samenlevingszaken voor het muteren van gebruikers is voor 1 medewerker (werkzaam binnen de Financiële Administratie) niet belegd bij onafhankelijke functionarissen en is hiermee direct betrokken bij een primair proces. Er vindt geen zichtbare periodieke controle plaats op gebruikers en gebruikersrechten binnen de applicatie o.b.v. een formeel vastgestelde functie-autorisatie matrix.	Er vindt geen zichtbare vastlegging plaats van de risicoanalyse. De testwerkzaamheden worden niet altijd zichtbaar gedocumenteerd. Afsluitend vindt er een goedkeuring plaats voor het doorvoeren van de wijzigingen in de productieomgeving.
Risico	Door het ontbreken van een zichtbare periodieke controle authenticatiebeheer bestaat een verhoogd risico op ongeautoriseerde toegang tot de applicatie en de kans dat eventuele uitzonderingen op het wachtwoordbeleid niet tijdig worden geïdentificeerd en adequaat worden opgevolgd.	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.	Door het ontbreken van vastlegging van risicoanalyses bestaat de kans dat niet alle risicovolle functionaliteiten met de juiste impact kan worden getest. Daarnaast is het mogelijk dat de impact van eventuele bevindingen vanuit de testwerkzaamheden niet wordt geadresseerd.
Aanbeveling	Wij adviseren u om een zichtbare periodieke controle in te richten op de gehanteerde wachtwoordinstellingen en gebruikers die eventueel een uitzondering vormen op het wachtwoordbeleid, en dit vast te leggen.	• Wij adviseren u om de accounts met hoge rechten te beleggen bij onafhankelijke functionarissen. • Wij adviseren u om de functie-autorisatie matrix (SOLL) formeel vast te stellen en periodiek te controleren op juistheid en actualiteit. • Wij adviseren u om de periodieke controle zichtbaar vast te leggen aan de hand van een functie-autorisatiematrix (IST).	Wij adviseren u om een risicoanalyse uit te voeren voor het doorvoeren van wijzigingen, en op basis daarvan een testplan op te stellen van de uit te voeren testwerkzaamheden. Vervolgens dient de uitvoering en het go / no go moment naar productie te worden vastgelegd.
Gevolgen jaarrekening-controle	Voor de jaarrekeningcontrole heeft dit tot gevolg dat wij op authenticatie in de applicatie kunnen steunen.	Voor de jaarrekeningcontrole heeft dit tot gevolg dat wij niet op autorisaties in de applicatie kunnen steunen, en mogelijk aanvullende werkzaamheden moeten uitvoeren.	Op basis van de bevindingen kunnen wij niet steunen op uw proces omtrent het gestructureerd doorvoeren van nieuwe wijzigingen en heeft aanvullend tot gevolg dat wij de releasenotes analyseren. Op basis van deze werkzaamheden zijn er geen bevindingen geconstateerd.

3. IT-omgeving

Detailbevindingen interne beheersing – Wijzigingsbeheer Youforce

	Wijzigingsbeheer
Constatering	Wij hebben vernomen dat er geen formele procedure is ingericht omtrent wijzigingsbeheer, omdat de leverancier verantwoordelijk is voor het doorvoeren van de wijzigingen. De leverancier rapporteert jaarlijks over de interne beheersing in de vorm van een ISAE 3402 rapportage. Wij hebben vernomen dat deze rapportage niet door u aantoonbaar wordt geëvalueerd om vast te stellen in hoeverre wijzigingen op beheerste wijze worden doorgevoerd. Daarnaast is het voor u van belang om de maatregelen te identificeren die onder de verantwoordelijkheid van de gebruikersorganisatie vallen (de zogenaamde User Entity Controls).
Risico	Het risico bestaat dat bevindingen uit de ISAE 3402 rapportage van Youforce niet tijdig worden opgemerkt en geadresseerd. Daarnaast ontstaat het risico dat maatregelen die onder uw gebruikersorganisatie vallen niet worden geïdentificeerd, en derhalve risico's niet op een adequate wijze worden beheerst.
Aanbeveling	Wij adviseren om de ISAE 3402 rapportage van Youforce jaarlijks te beoordelen zodra deze beschikbaar is, en maatregelen die onder de verantwoordelijkheid vallen van de gebruikersorganisatie te adresseren en op adequate wijze te beheersen. Daarnaast raden wij aan om eventuele bevindingen uit de rapportage te bespreken met de leverancier en hiermee de impact te bepalen voor uw organisatie.
Gevolgen voor de jaarrekening-controle	Op basis van de bevindingen kunnen wij niet steunen op uw proces omtrent het gestructureerd doorvoeren van nieuwe wijzigingen. Voor de jaarrekeningcontrole heeft dit tot gevolg dat wij aanvullende werkzaamheden uitvoeren door de ISAE 3402 rapportage te analyseren.

3. IT-omgeving

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 dagelijks worden gemaakt en op meerdere locaties worden opgeslagen. Daarnaast vindt er monitoring plaats op de uitvoering van de back-ups door de i-Dienst voor de on-premise (lokaal draaiende) systemen. De monitoring op continuïteitsmaatregelen van Cloud diensten moet nog formeel geïmplementeerd worden.
Recovery	De restore procedure wordt jaarlijks op zijn werking getest voor de on-premise systemen. Dit is een verplicht onderdeel vanuit de GBA, waarvoor rapportages worden opgesteld. Hierdoor beschouwen wij het risico op dataverlies en downtime voor uw IT-omgeving als laag. De monitoring op continuïteitsmaatregelen van cloud diensten moet nog formeel geïmplementeerd worden.
Uitwijk	U heeft aangegeven dat er een uitwijklocatie is ingericht. Voor de Windows, kantooromgeving heeft de i-Dienst zelf een uitwijklocatie, twee datacenters. Voor de i-Series (Civision, SAP, GBA etc.) heeft u een uitwijkcontract met Infradax. De laatste uitwijktest heeft echter niet in het afgelopen jaar plaatsgevonden, maar in december 2023. De monitoring op continuïteitsmaatregelen van cloud diensten moet nog formeel geïmplementeerd worden.
Fysieke beveiliging	De servers zijn ondergebracht in het primaire datacenter in Zwolle. Er is een secundair datacenter in Oldebroek aanwezig. Het datacenter heeft beveiligingsmaatregelen getroffen ten aanzien van temperatuur, klimaat, noodstroomvoorzieningen en brandrisico's.
Remote acces	Voor het inloggen vanaf een externe locatie wordt gebruik gemaakt van extra beveiligingsmaatregelen zoals two-factor authenticatie. Hiermee wordt een extra authenticatie stap afgedwongen.

3. IT-omgeving

Cybersecurity NIS2 scan

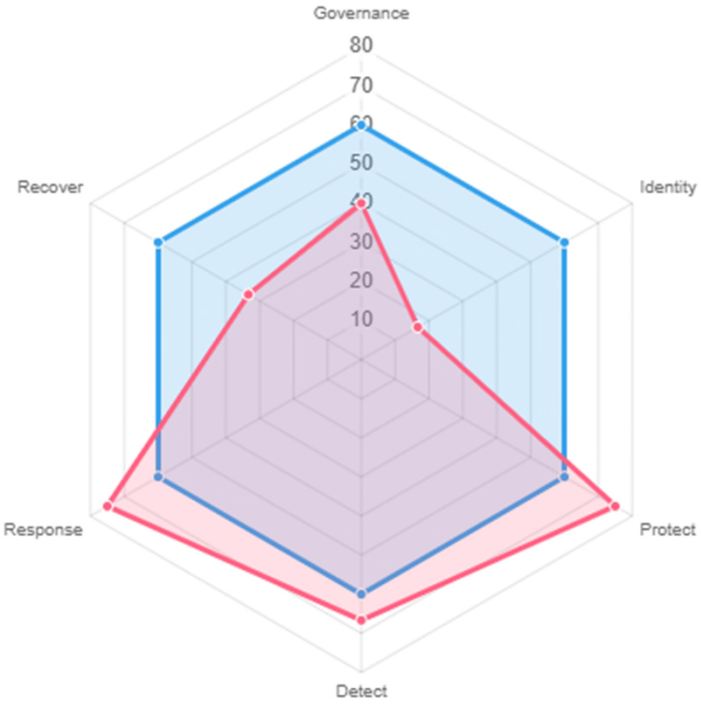
1. Deze scan is bedoeld om u in inzicht te geven in de staat van cyberweerbaarheid van uw organisatie. De lijst is niet uitputtend, maar betreft een focus op de belangrijkste punten. Bij eventuele bevindingen is aangegeven welke BIO 2.0 norm (Baseline Informatiebeveiliging Overheid) hierop van toepassing is.
2. De scan is afgestemd op de vereisten van de EU wetgeving NIS2 en de Nederlandse vertaling in de Cyberbeveiligingswet.
3. Let op: de onderwerpen volgen uit interviews en we hebben 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.
4. De score wordt weergeven als een ratio waar 0 % de laagste en 100 % de hoogste score is.
5. Rood betreft uw score. Blauw betreft de best practice ten aanzien van de EU wetgeving NIS2 en de Nederlandse vertaling in de Cyberbeveiligingswet vallen.

Wij maken voor cyberweerbaarheid onderscheid in:	
Governance	Risicomanagement, communicatie en monitoring van cyber-risico's.
Identificatie	Identificeren van kritieke gegevens en cybersecurity risico's.
Bescherming	Beschermen middels inzet van techniek, mens en procedures.
Detectie	Het monitoren van verdacht gedrag en afwijkingen in de gegevensverwerking.
Reactie	Reageren op incidenten en bijsturen op basis van inzichten.
Herstel	Het herstellen naar normale bedrijfsvoering.

3. IT-omgeving

Cybersecurity NIS2 scan

Resultaten:	
Governance	Wij zien dat er aandacht en prioriteit wordt gegeven aan de kwaliteit van de huidige beveiliging. Er zijn verschillende formele beleidsregels opgesteld t.a.v. informatiebeveiliging (BIO 5.01) en er is een centraal overzicht van bedrijfsmiddelen en de interne en externe stakeholders / eigenaren (BIO 5.09). Ter verbetering kan het bevoegd gezag de verantwoordelijkheden en taken voor cyber-risico's in de eigen organisatie verder formaliseren (BIO 5.02).
Identificatie	Wij zien dat het identificeren van kroonjuwelen, risico's en maatregelen (ook bij leveranciers) directe actie vereist (BIO 5.08, 5.12, 5.19 t/m 5.21 en 5.29). Denk hierbij aan het inzichtelijk maken van systemen, data en processen die essentieel zijn voor de continuïteit van uw bedrijfsvoering, en bepaal de impact wanneer deze niet meer operationeel zijn. Ook dient u adequate beveiligingsmaatregelen inzichtelijk te krijgen en uit te werken waarmee u of uw leveranciers de cyberrisico's afdekken.
Bescherming	De wijze waarop vervolgens de cyberrisico's door middel van maatregelen worden verlaagd is op orde, maar kan verder worden verbeterd. Denk hierbij vooral aan het identificeren van gebruikers op het netwerk en de IT-systemen (BIO 5.16).
Detectie	Op basis van het model zien wij dat aandacht gegeven is aan monitoring, vulnerability scanning en pentesting, maar dat er verbeterpotentieel ligt om de cyberweerbaarheid van uw organisatie te verhogen. Denk hierbij aan het aanscherpen van de procedures omtrent toegangsbeheer (BIO 5.18) en het periodiek beoordelen van externe Assurance en Service Level Rapportages op beveiligingsmaatregelen van externe leveranciers (BIO 5.21 en 5.22).
Reactie	Reageren op incidenten en bijsturen op basis van inzichten is op orde. Op dit onderdeel zien wij in opzet geen aandachtspunten.
Herstel	Het herstellen naar normale bedrijfsvoering vraagt om aandacht. Denk hierbij aan het implementeren van een bedrijfscontinuïteitsplan (BIO 5.29) en het regelmatig oefenen met de back-up voorzieningen van systemen, operationele techniek en data binnen een uitgebreide scope, en of deze adequaat kunnen herstellen (BIO 5.30 en 8.13).



4

Voorbereiding jaarrekening-controle

4. Voorbereiding jaarrekeningcontrole

Planning

Wij starten met de jaarrekeningcontrole op 24 maart 2025. Om de jaarrekeningcontrole efficiënt te laten verlopen is het belangrijk dat vóór deze datum een conceptjaarrekening inclusief sluitende auditfile en controledocumentatie aanwezig is. Voor de benodigde controle-documentatie (het balansdossier) zullen wij een aparte PBC lijst aanleveren, inclusief deadlines voor de aanlevering.

Aanvullende gegevensgerichte werkzaamheden

Voor aanvang van de jaareinde controle zullen wij de belangrijkste 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, bijvoorbeeld de grondexploitaties;
- Tijdige aanlevering van de (volledige) jaarrekening aansluitend met uw administratie en het concept jaarverslag;
- Interne kwaliteitscontrole op jaarrekening en balansdossier;
- Maximaal twee versies van de jaarrekening (concept en definitief);
- Tijdige en volledige aanlevering van het balansdossier volgens de PBC;
- Uw medewerkers zijn voldoende beschikbaar om vragen (tijdig) te beantwoorden. Daarbij is het ook relevant dat de coördinator op het jaarrekeningproces de vragen bij voorkeur dagelijks monitort en tijdig communiceert waar vertragingen spelen.

5

Actualiteiten

5. Actualiteiten

Wethouderspensioen

De nieuwe pensioenwet is op 1 juli 2023 ingegaan. Uiterlijk 1 januari 2027 moeten alle werknemers en gepensioneerden duidelijkheid hebben over de gevolgen daarvan voor hun pensioen, alvorens 1 januari 2028 alle pensioenen worden overgezet. De nieuwe wet heeft ook gevolgen voor de pensioenen van politieke ambtsdragers, waaronder de pensioenen van wethouders. Zij vallen onder de pensioenregeling die is opgenomen in de Algemene pensioen- en uitkeringswet politieke ambtsdragers (Appa). Dit is een op zichzelf staande wettelijke pensioenregeling waarvoor de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verantwoordelijk is. De Pensioenwet en de Wet toekomst pensioenen (Wtp) gelden niet voor deze pensioenregeling. Echter, de bestendige beleidslijn is dat de rechtspositie voor politieke ambtsdragers zoveel als mogelijk geënt is op de rechtspositie van overheidswerknemers bij het Rijk (“normaal waar het kan, bijzonder waar het moet”). Er is volgens BZK geen aanleiding om de bijzondere positie van politieke ambtsdragers in de pensioenregeling Appa tot uitdrukking te laten komen. Het politieke ambt wordt gezien als een stap in een carrière, waar na het aftreden de ambtsdrager zijn loopbaan met pensioenopbouw elders voortzet. Vandaar dat de Appa zoveel mogelijk de ABP pensioenregeling van de overheidswerknemers volgt.

Na de aanvaarding van de Wet aanpassing Appa zijn per 1 juli 2022 de inhoudelijke verschillen tussen het ABP reglement en de Appa opgelost waardoor de Appa en het ABP reglement gelijk zijn getrokken. Voor een groot deel van de politieke ambtsdragers geldt dus dat zij nu materieel al dezelfde pensioenregeling hebben als andere overheidswerknemers (die bij ABP zitten). Nu geldt voor politieke ambtsdragers nog dat de pensioenuitkeringen niet uit een pensioenfonds betaald worden, maar uit de begroting van de gemeenten. De gemeente heeft ter dekking van de toekomstige pensioenlasten in lijn met BBV een voorziening op de balans opgenomen. Het ligt voor de hand de pensioenen van politieke ambtsdragers, die immers ook werkzaam zijn in het overheidsdomein, op te nemen in de nieuwe premieregeling voor overheidswerknemers binnen de wettelijke kaders van de Wtp. Na het onderbrengen van de Appa-pensioenen bij het ABP door middel van een collectieve waardeoverdracht eindigen de structurele pensioenuitgaven uit de begroting.

Tot de uiteindelijk vastgestelde overgangsdatum geldt de huidige Appa. Op de overgangsdatum zullen bestaande Appa-aanspraken worden omgezet naar het nieuwe contract van het ABP. Dit betekent dat de regels van dat nieuwe contract ook van toepassing worden op de vóór de overgangsdatum al bestaande Appa-rechten. Dat kan door de voor de overgangsdatum opgebouwde pensioenaanspraken om te zetten in nieuwe individuele pensioenvermogens. Voor de overdracht van de Appa-pensioenen geldt dat de benodigde individuele pensioenvermogens eerst moeten worden berekend door ABP. Vervolgens moeten deze door de betrokken overheidsinstellingen bij het ABP worden afgefinancierd.

5. Actualiteiten

Dit houdt een collectieve waardeoverdracht door alle betrokken overheden aan het ABP in. Na een dergelijke affinanciering is er met ingang van de definitieve overgangsdatum geen sprake meer van het uit de begroting bekostigen van pensioenuitkeringen, maar is er sprake van fondsfinanciering. Een nog uit te voeren onderzoek door BZK zal zich nader richten op de omvang van de voorziening, de invloed van de rekenrente en de benodigde overdrachtswaarde. Daarbij moet worden aangetekend dat de verschillen tussen afzonderlijke gemeenten groot kunnen zijn. In aanloop naar de overgang moet per gemeente inzichtelijk worden gemaakt in hoeverre een toereikende voorziening is getroffen. Wij achten het van belang de beschreven ontwikkelingen mee te nemen in uw risicoanalyse en wanneer er meer duidelijkheid is, de gevolgen te verwerken in de meerjarenbegroting.

Rechtmatigheidsverantwoording

Met ingang van verslagjaar 2023 hebben gemeenten, provincies en gemeenschappelijke regelingen voor het eerst een rechtmatigheidsverantwoording opgenomen in de jaarrekening. Uit de eerste evaluatie blijkt dat de rechtmatigheidsverantwoording nog niet zoveel toegevoegde waarde heeft gecreëerd voor de Raad als van tevoren was gehoopt. Het échte gesprek tussen het college en de Raad is in veel gevallen uitgebleven. We adviseren daarom om (het proces rondom) de rechtmatigheids-verantwoording 2023 ook bij u intern te evalueren om zodoende te stimuleren dat het gesprek over de rechtmatigheidsverantwoording in 2024 wel gaat worden gevoerd.

Over 2023 hebben veel gemeenten omvangrijke rechtmatigheidsfouten door begrotingsoverschrijdingen gerapporteerd. Daarbij merken we op dat de foutenevaluatie omtrent begrotingsrechtmatigheid per gemeente en accountant verschilt. Dit geldt overigens ook voor het M&O-criterium, waarvoor eenduidige normen ontbreken. Hieruit blijkt dat de kaders nog te onduidelijk waren. Derhalve heeft de Commissie BBV recent de Kadernota Rechtmatigheid 2024 uitgebracht. De belangrijkste wijzigingen zijn:

- De voorbeeldtabel die op 20 november 2023 op de website van de Commissie BBV is opgenomen als voorbeeld voor het inzichtelijk maken van (begrotings-) onrechtmatigheden in de rechtmatigheidsverantwoording is gewijzigd en nu dus opgenomen in de Kadernota zelf (pag. 34 en 35);
- Een verduidelijking van wanneer overschrijdingen ten aanzien van wel of niet tijdig melden als onrechtmatig worden beschouwd en wanneer welke begrotingsonrechtmatigheden als gevolg van overschrijding van lasten en/of investeringen als acceptabel (passend in het beleid) worden beschouwd: dus wel onrechtmatig, maar acceptabel (pag. 33);
- Een tekstuele aanpassing in de modelverantwoording ten aanzien van de geconstateerde bevindingen, specifiek in relatie tot de omvang van niet rechtmatig tot stand gekomen verantwoorde baten, lasten en balansmutaties en welk deel acceptabel is op basis van de vastgestelde afspraken (zie pag. 42). Wij vragen u deze hanteren in de jaarstukken 2024;

5. Actualiteiten

- ❑ Een aangepast hoofdstuk 2 om het bestuurlijk belang van rechtmatigheid voor raadsleden te verduidelijken;
- ❑ Het niet meer in de rechtmatigheidsverantwoording opnemen van geconstateerd misbruik waarbij het M&O beleid is toegepast en heeft geleid tot bijvoorbeeld terugvorderingen en het opleggen van sancties. De jaarrekening is in deze situatie immers getrouw en de financiële effecten van het misbruik zijn teniet gedaan. Wel dient via de paragraaf bedrijfsvoering inzicht te worden gegeven in de aard en (financiële) impact van het bij de gemeente geconstateerde misbruik.

Voor de volledigheid merken wij op dat tot op heden het BBV en BADO nog niet zijn aangepast. Het streven van BZK is nog steeds om BBV en BADO nog dit kalenderjaar aan te passen, maar daarbij is men afhankelijk van de agenda van de Tweede Kamer.

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 gemeenten 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 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. 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 adviseren 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**) belangrijke doelen gesteld voor het behalen van klimaatdoelstellingen. Onderdeel hiervan is het niet meer financieren van organisaties die onvoldoende bijdragen aan deze klimaatdoelstellingen.

Investeerders hechten ook grote waarde aan ESG voor wat betreft de klantacceptatie en kredietverleningen door de BNG Bank. Gemeenten 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 gemeenten 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 college om te bepalen welke aanpassingen binnen uw gemeente gedaan moeten worden naar aanleiding van de notities. Overigens geldt dat deze gelden vanaf boekjaar 2025, maar eerder toepassen is toegestaan.

5. Actualiteiten

Rekenkamer

De Model Verordening gemeentelijke rekenkamer is aangepast aan de Wet versterking decentrale rekenkamers. Dit betekent dat alle gemeenten uiterlijk 1 januari 2024 een onafhankelijke (gemeenschappelijke) rekenkamer moeten hebben. Ook voor gemeenten, die al een onafhankelijke rekenkamer hadden, verandert het één en ander.

Specifieke uitkeringen

In het hoofdlijnenakkoord is het voorstel opgenomen dat de SPUK's (m.u.v. BUIG) per 2026 overgaan naar het gemeentefonds met tegelijk een korting van 10%. De verwachting is dat dit in 2025 verder wordt uitgewerkt en dat bestaande SPUK’s de komende jaren worden afgebouwd. We adviseren u om deze ontwikkelingen nauwlettend in de gaten te houden om de mogelijke impact voor uw gemeente te bepalen.

Omgevingswet

De omgevingswet is op 1 januari 2024 in werking getreden en vervangt 26 bestaande wetten. De omgevingswet heeft een indirecte en directe impact op de gemeentelijke processen en organisatie. Belangrijk is om te toetsen in hoeverre uw processen en procedures voldoen aan de omgevingswet en, waar nodig, aanpassingen te doen, zodat u volledig compliant bent aan de nieuwe omgevingswet.

De risico’s van het inhuren van zzp’ers

Wet deregulering beoordeling arbeidsrelaties (Wet DBA)

Door de Wet DBA is de Verklaring Arbeidsrelatie (VAR) per mei 2016 vervallen. Opdrachtgevers en opdrachtnemers maken binnen hun arbeidsrelatie afspraken. Samen beoordelen zij of er sprake is van loondienst. Bij twijfel kan een modelovereenkomst zekerheid geven.

Wanneer is sprake van loondienst?

Als sprake is van alle kenmerken van loondienst: werkgeversgezag, de verplichting tot het leveren van (persoonlijke) arbeid en een beloning.

5. Actualiteiten

Recente ontwikkelingen Deliveroo
Deliveroo maakte gebruik van modelovereenkomsten. De fietskoeriers werkten op basis van een opdrachtovereenkomst gebaseerd op vrije vervanging. Door het ontbreken van het kenmerk ‘de verplichting tot het leveren van (persoonlijke) arbeid’ is daarbij het standpunt ingenomen dat de fietskoeriers hun werkzaamheden als ZZP’ers verrichtten. FNV spande met succes een zaak aan omdat ze van mening waren dat de fietskoeriers in loondienst waren.
Gevolg: modelovereenkomsten gebaseerd op vrije vervanging zijn per 1 januari 2024 vervallen.

Wetsvoorstel: Wet verduidelijking beoordeling arbeidsrelaties en rechtsvermoeden (VBAR)
De VBAR heeft als doel schijnzelfstandigheid tegen te gaan door de open norm ‘werken in dienst van’ verder in te kleuren aan de hand van recente rechterlijke uitspraken. Verder wordt een zogenaamd rechtsvermoeden geïntroduceerd op grond waarvan werkenden met een lager uurtarief dan € 32,24 per uur worden geacht hun werkzaamheden te verrichten op basis van een arbeidsovereenkomst. Drie essentiële factoren die van belang zijn bij het onderscheid tussen loondienst en een ZZP’er:

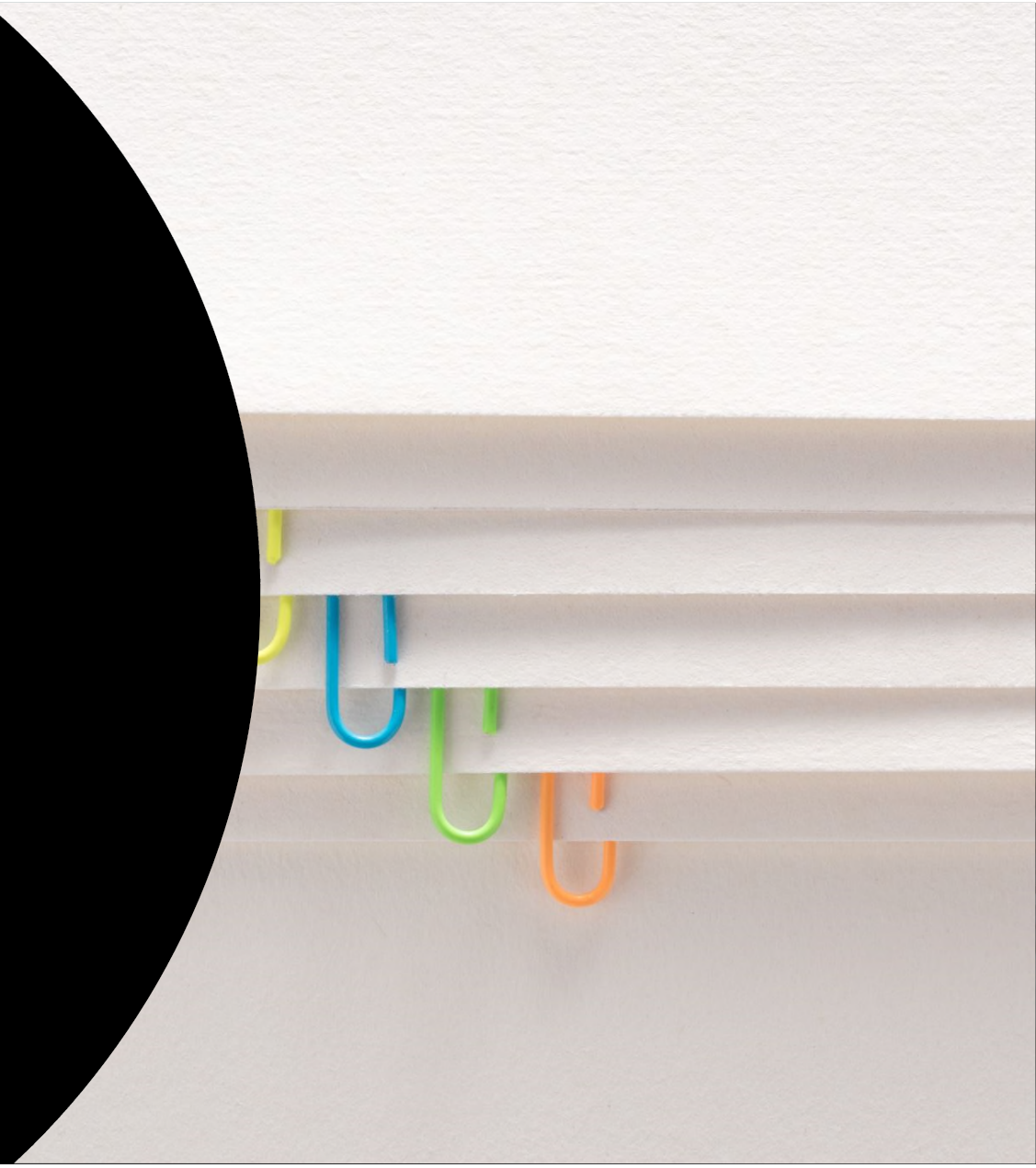
- Werkinhoudelijke aansturing;
- Organisatorische inbedding;
- Eigen rekening en risico.

Invoering VBAR uitgesteld nu begin 2025 niet realistisch blijkt te zijn.

Handhavingsmoratorium
Op basis van het huidige handhavingsmoratorium wordt in de relatie tussen opdrachtgevers en ZZP`ers, alleen corrigerend opgetreden (opleggen van correctieverplichtingen, naheffingen en eventueel boetes) als er sprake is van kwaadwillendheid. Of als opdrachtgevers aanwijzingen van de Belastingdienst, gegeven na 1 september 2019, niet (of in onvoldoende mate) binnen een redelijke termijn opvolgen. De overheid wil met ingang van 1 januari 2025 vooralsnog actief gaan handhaven op schijnzelfstandigheid, ondanks uitstel van invoering van de VBAR.

Advies
We adviseren u om modelovereenkomsten opnieuw te beoordelen en op basis van de recente ontwikkelingen de arbeidsrelatie met ingehuurde ZZP’ers te heroverwegen.

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 de ontwikkelingen en gevolgen voor de jaarrekeningcontrole. Bij elke bevinding is het jaar van de eerste vermelding vermeld. Daarnaast hebben wij de voortgang van de bevinding aangegeven.

Bevinding / Risico / Aanbeveling / Gevolgen controle			
Bevinding In dit blok wordt aangegeven wat gedurende de accountantscontrole is geconstateerd en waarvan wij u graag op de hoogte willen brengen.	*Ontwikkelingen* Hier geven wij u de opvolging met betrekking tot de bevinding en waar nodig een aanbeveling tot een mogelijke oplossing voor de bevinding.	*Gevolgen jaarrekening* Hier geven wij aan wat de gevolgen zijn van de bevinding in relatie tot de verdere werkzaamheden voor de jaarrekening-controle.	*Status 2024* De voortgang in hoeverre de bevinding is opgelost.

6. Bijlagen

Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze management letters van voorgaande jaren. Indien wij in de hoofdrapportage gerapporteerd hebben over een onderwerp kan dit ten opzichte van voorgaand jaar als niet opgelost worden beschouwd. Om niet in herhaling te vervallen, rapporteren wij hierover niet separaat in dit hoofdstuk.

- Opgelost
- Actie ondernomen, maar nog niet afgerond
- Geen actie ondernomen
- Nieuwe bevinding
- Bewust niet opgevolgd

Jaar	Proces	Bevinding	Ontwikkelingen	Gevolgen jaarrekening	Status 2024
2024	Personeel	Uitbesteding salarisverwerking	De salarisverwerking is uitbesteed aan Govers. Tijdens de interim-controle hebben wij vernomen dat de gemeente onvolledige of foutieve verwerkingen heeft geconstateerd door met name handmatige mutaties. Mogelijk kan dit ook fiscale gevolgen met zich meebrengen. Daarnaast hebben we vernomen dat de medewerkers HR die de mutatiecontroles uitvoeren ook zelf kunnen invoeren in Youforce en Beaufort. Dit resulteert in functievermenging.	Wij vragen u een position paper op te stellen met daarin de bevindingen en overwegingen in relatie tot de kans op een afwijking van materieel belang. Wij vragen u daarnaast de invoerrechten voor de medewerkers HR te beperken.	
2023	Betalingen	Zelfstandige betalingsbevoegd-heden Rabobank	U geeft aan bezig te zijn geweest met het inperken van het limiet voor zelfstandig betalen, zodat een 2e handtekening wordt vereist.	Gezien de mutaties tot op heden zeer gering zijn heeft dit naar verwachting geen directe impact op de controle.	
2022	Betalingen	Belprocedure wijziging crediteurenstam-gegevens Civision middelen	U heeft een position paper opgesteld met moverende redenen om af te zien van de belprocedure. Op basis daarvan schat u het risico als laag in en accepteert het risico.	Het 4-ogenprincipe verlaagt het risico onvolledig, waardoor we gegevensgericht vaststellen of het bankrekeningnummer daadwerkelijk toebehoort aan de crediteurnaam.	
2022	Uitkeringen	Collegiale toetsing en kwaliteitsplan	U geeft aan een kwaliteitsplan te gaan opstellen, waarbij de inhoud van zowel de collegiale toetsing als de toetsing door de kwaliteitsmedewerker wordt uitgewerkt. Door in het kwaliteitsplan werkinstructies op te nemen, welke ten minste ten tijde van de toetsing in acht dienen te worden genomen, en deze instructies kenbaar te maken aan de toetsers, ontstaat er een duidelijk kader op de inhoud van de controles.	Wij zullen gegevensgerichte waarnemingen verrichten om voldoende zekerheid te verkrijgen over de nauwkeurigheid van de verantwoorde uitkeringen.	

6. Bijlagen

Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze management letters van voorgaande jaren. Indien wij in de hoofdrapportage gerapporteerd hebben over een onderwerp kan dit ten opzichte van voorgaand jaar als niet opgelost worden beschouwd. Om niet in herhaling te vervallen, rapporteren wij hierover niet separaat in dit hoofdstuk.

- Opgelost
- Actie ondernomen, maar nog niet afgerond
- Geen actie ondernomen
- Nieuwe bevinding
- Bewust niet opgevolgd

Jaar	Proces	Bevinding	Ontwikkelingen	Gevolgen jaarrekening	Status 2024
2020	Aanbestedingen	Juiste aanbestedings-vorm	U bent bezig met het inrichten van het contractenregister ISPnext. In 2025 zullen wij de ontwikkelingen nagaan en zo mogelijk of daarmee de beheersing op het tijdig aanbesteden geborgd wordt.	Ten aanzien van de jaarrekeningcontrole 2024 vragen wij u een spendanalyse op te stellen over de periode 2021-2024.	
2017	Subsidie-verstrekkingen	Verordening	U past per 1 mei 2024 een nieuwe subsidieverordening toe. Hierdoor is helder welke accountantsverklaring wordt vereist voor de betrouwbaarheid van de subsidieverantwoordingen.	Geen	
2017	Inkopen	Prestatielevering	U bent bezig met het implementeren van een nieuw financieel pakket. Hierin wordt de controle op de prestatielevering ingericht.	De gegevensgerichte werkzaamheden over 2024 zijn vergelijkbaar met vorig boekjaar.	
2017	Personeel	Standenregister	Vanaf 2023 is Youforce in gebruik, waardoor de invoercontrole geautomatiseerd is afgedwongen. Gezien de salarisverwerking is uitbesteed adviseren wij u een standenregister in te richten, waarbij een soll-positie wordt gecreëerd voor de bruto salariscomponenten door een onafhankelijke functionaris. Om de volledigheid van de mutaties te waarborgen wordt periodiek bezettingsoverzichten verstrekt aan de afdelingsmanagers. Echter ontbreekt zichtbare controle of het dienstverband per medewerker correct is.	De controle op de nauwkeurigheid van de salarismutaties zullen wij gegevensgericht controleren. Voor de volledigheidscontrole zullen we bij de jaarrekeningcontrole vragen het bezettingsoverzicht per afdelingsmanager te laten bevestigen.	
2017	Sociaal domein	Prestatie-levering WMO	Tot op heden wordt er gebruik gemaakt van de controle-verklaringen bij de productieverantwoordingen. U geeft aan te onderzoeken hoe u de prestatielevering WMO in het nieuwe softwarepakket kunt ondervangen, door te bekijken welke vastleggingen van de prestatielevering er zijn, of deze voldoende zijn en hoe die inzichtelijk gemaakt kunnen worden.	Om de prestatielevering WMO bij de zorgaanbieders vast te stellen, wordt gebruik gemaakt van controleverklaringen bij de productie-verantwoordingen.	

6. Bijlagen

Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze management letters van voorgaande jaren. Indien wij in de hoofdrapportage gerapporteerd hebben over een onderwerp kan dit ten opzichte van voorgaand jaar als niet opgelost worden beschouwd. Om niet in herhaling te vervallen, rapporteren wij hierover niet separaat in dit hoofdstuk.

- Opgelost
- Actie ondernomen, maar nog niet afgerond
- Geen actie ondernomen
- Nieuwe bevinding
- Bewust niet opgevolgd

Jaar	Proces	Bevinding	Ontwikkelingen	Gevolgen jaarrekening	Status 2024
2017	Sociaal domein (WMO)	Toets kwaliteits-medewerker	Medio mei 2024 heeft de raad het besluit genomen om budget beschikbaar te stellen voor het robuuster maken van het Sociaal Team en de uitkeringsadministratie. Het adviesrapport 'Robuust Sociaal Team' geeft de belemmeringen weer en de oplossingsrichtingen hoe de robuustheid op korte en middellange termijn versterkt kan worden. Onder meer gaat het rapport in op de positionering van de kwaliteitsmedewerker. Wij adviseren u vanuit de kwaliteitscontrole een aanpak vanuit risicogedachten over de verschillende stromen binnen de WMO nader onder te verdelen.	Wij zullen aanvullende gegevensgerichte werkzaamheden moeten verrichten om de juistheid en rechtmatigheid van de lasten WMO vast te stellen.	
2017	Schattingsposten	Grondexploitatie en voorzieningen	Sinds 2020 is het proces voor de MPG beschreven en is een checklist opgesteld, waaruit blijkt welke controles plaatsvinden. Diverse controlemomenten lopen door tot februari in het opvolgend boekjaar. Tijdens de interim-controle 2024 is derhalve uitgegaan van de checklist behorende bij de jaarrekening 2023. Daaruit blijkt echter nog niet zichtbaar en herleidbaar wie op welk moment de controle daadwerkelijk heeft uitgevoerd.	Wij vragen u om de controlemomenten tot februari 2024 in de checklist zodanig zichtbaar te maken, zodat blijkt wie wanneer het onderdeel daadwerkelijk heeft uitgevoerd.	
2023	Omgevings-vergunningen	Bouwkostentoets	Casemanagers mogen beschikkingen omgevingsvergunningen die binnen het bestemmingsplan vallen zelfstandig autoriseren. Beschikkingen die buiten het bestemmingsplan vallen, moeten nog wel door de Teammanager Ruimte geautoriseerd worden. Door de gewijzigde procedure bestaat de mogelijkheid dat Casemanagers zelfstandig beschikkingen verstrekken (geen 4-ogen principe),	Wij zullen voor de jaarrekeningcontrole aanvullende gegevensgerichte werkzaamheden verrichten om de nauwkeurigheid en volledigheid van de legesopbrengsten vast te stellen.	

6. Bijlagen

Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze management letters van voorgaande jaren, maar waarvan de gemeente de bewuste keuze heeft gemaakt geen opvolging te geven en het risico accepteert.

Jaar	Proces	Bevinding	Ontwikkelingen	Gevolgen jaarrekening
Geaccepteerd risico				
2017	Omgevings-vergunningen	Controle bevoegdheden autorisatie	Wij hebben vastgesteld dat de manager Ruimte namens het B&W de beschikking na controle door de casemanager autoriseert. De geautoriseerde beschikking en besluitbrief worden door de casemanager verstuurd naar de administratie omgevings-vergunning en die controleert of de stukken getekend zijn door een daartoe bevoegde persoon. Echter vindt deze controle niet zichtbaar plaats. U geeft aan dat het KCC de beschikkingen en verzendbrieven opslaat in RX Mission, dit is zichtbaar middels logging. Volgens u zal het vergunningenloket deze stap niet uitvoeren wanneer de beschikking door een onbevoegde functionaris is ondertekend. Tevens geeft u aan dat de beschikkingen worden bewaard en er dus getoetst kan worden of deze getekend zijn door (een) bevoegde functionaris(sen).	Doordat de controle van het KCC niet herleidbaar is en beschikkingen niet worden geautoriseerd in SquitXO, zullen wij voor de jaarrekeningcontrole aanvullende werkzaamheden verrichten om de nauwkeurigheid van de legesopbrengsten vast te stellen.
2018	Omgevings-vergunningen	Volledigheids-controle legesregels en factuurregels	Wij vragen uw aandacht voor de controle van de legesregels versus de factuurregels (beiden gegevens uit RX Mission) om de volledigheid van de legesopbrengsten te waarborgen. Door de gemeente wordt de controle jaarlijks achteraf uitgevoerd. De gemeente accepteert het risico dat eventuele onjuistheden niet tijdig worden onderkent.	Wij verzoeken u de genoemde controle over het gehele jaar uit te voeren ten behoeve van de jaarrekeningcontrole.
2017	Subsidie-verstrekkingen	Functiescheiding	Via het zaaksysteem Djuma zijn de processtappen gelogd en geeft de teamleider in de workflow haar goedkeuring, waarmee een inhoudelijke controle is verricht. Echter is achteraf niet herleidbaar op basis waarvan de teamleider goedkeuring heeft gegeven. U geeft aan dat alle dossiers eerst langs een collega gaan voordat deze aan de manager worden aangeboden. Hierbij steunt de teamleider op het voorliggende proces met de daarin opgenomen checks. Echter ook vanuit de collegiale-toetsing ontbreekt de zichtbaarheid van de inhoudelijke toetspunten.	Wij verrichten werkzaamheden in het kader van de rechtmatigheidsverantwoording of de subsidies zijn verstrekt in overeenstemming met de subsidieverordening.

6. Bijlagen - IT-omgeving

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.

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.

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.

6. Bijlagen – IT-omgeving

Bijlage: Logische toegangsbeveiliging

Wij onderscheiden vijf bouwstenen ten aanzien van toegangsbeveiliging. De bouwstenen leveren gestapeld, naast een sterke IT-beheersing, ook de meeste controlezekerheid op. Beperkingen in de onderliggende steen zorgen voor een verzwakking van de bovenliggende stenen. Onderstaand zijn de bouwstenen schematisch weergegeven.

6. Bijlagen – IT-omgeving

Bijlage: Wijzigingsbeheer

Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat wijzigingen een proces doorlopen, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden. Onderstaand hebben wij per fase onze verwachting aangegeven. Onder wijzigingen verstaan wij niet alleen nieuwe versie updates, maar ook aanpassingen in (kritieke) systeemconfiguraties.

Proces	Verwachting
Risico-inschatting	Voor iedere softwarewijziging is het relevant om te beoordelen wat de risico's zijn die de wijziging met zich meebrengt voor de hoofdprocessen. Daarnaast moet beoordeeld worden welke geïdentificeerde technische en organisatorische wijzigingsrisico's er spelen bij het uitvoeren van de change, in het bijzonder wanneer er sprake is van maatwerk. Hiermee beoordeelt u per wijziging welke nieuwe of gewijzigde functionaliteit een risico vormt voor een goede werking van uw bedrijfsvoering.
Opstellen testplan en aanpak	Vanuit de geïdentificeerde risico's kan een testplan worden gemaakt, waarin de te testen elementen van de software benoemd zijn evenals de inhoudelijk uit te voeren testwerkzaamheden op deze elementen. Belangrijke elementen hierin zijn go/no-go momenten, het maken van een back-up voor implementatie, een fall-back scenario in het geval een implementatie mislukt en het definiëren van de impact op de organisatie (denk bijvoorbeeld aan het opleiden van medewerkers).
Testen en documenteren	Softwarewijzigingen kunnen gestructureerd worden getest na het correct uitvoeren van de voorgaande twee stappen. Het maken van een gedegen vastlegging van testwerkzaamheden is van belang voor de aantoonbaarheid en controleerbaarheid van de uitgevoerde stappen. Daarnaast kan de vastlegging van testwerkzaamheden een belangrijke bron van informatie zijn als er onverhoopt na het doorvoeren van de wijziging toch verstoringen van uw bedrijfsvoering optreden.
Gebruikersacceptatie	Een wijziging is pas effectief als deze niet alleen is geaccepteerd vanuit een technisch oogpunt, maar ook vanuit de gebruikersorganisatie. Wij verwachten daarom een formele goedkeuring vanuit de gebruikersorganisatie, zowel voor implementatie als na de implementatie. Het kan natuurlijk ook voorkomen dat het nodig is om gebruikers te informeren over bijzonderheden als gevolg van de wijziging, zoals veranderingen in de werkwijze of aandachtspunten bij het gebruik van de applicatie.

6. Bijlagen - IT-omgeving

Cybersecurity

Als onderdeel van de jaarrekeningcontrole hebben wij inzicht gekregen in de cybersecurity-gerelateerde risico's die zouden kunnen leiden tot een potentiële afwijking van materieel belang in de jaarrekening (met betrekking tot zowel financiële als niet-financiële informatie). Hiervoor hebben wij inzicht gekregen in de mate waarin, en de overweging waarom de organisatie bepaalde informatiebeveiligingsmaatregelen heeft genomen om deze cyberrisico's te beperken.

Om het risico van cyberbeveiligingsbedreigingen (d.w.z. continuïteit van de dienstverlening en integriteit van de financiële verslaglegging) te verlagen, heeft uw organisatie een mix van beveiligingsmaatregelen geïmplementeerd. Zie de Cybersecurity NIS2 scan in de bijlage.

We zijn geïnformeerd dat zich in het boekjaar geen cyberbeveiligingsincidenten hebben voorgedaan die hebben geleid tot een afwijking van materieel belang in de jaarrekeningcontrole van uw organisatie. Onze controlewerkzaamheden zijn niet primair gericht op het doen van uitspraken over cyberbeveiliging en we hebben ook geen instructies van het management in die zin ontvangen voor het uitvoeren van meer diepgaande werkzaamheden.

6. Bijlagen - IT-omgeving

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 nog niet definitief gemaakt waarvan invoering naar verwachting in het najaar 2025 gaat plaatsvinden. 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.

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.

Contact

drs. E.H.J.D. (Edwin) Damman RA
Partner Audit
T +31 (0)6 13 74 45 08
e.damman@bakertilly.nl

L.F. (Lisanne) van Goor MSc RA
Manager Audit
T +31 (0)6 22 38 50 55
l.vangoor@bakertilly.nl

Kantoorgegevens
Baker Tilly (Netherlands) N.V.
Postbus 508
8000 AM ZWOLLE
T +31 (038) 425 86 00