



Management letter

Gemeente Rheden
Boekjaar 2024



Aanbiedingsbrief



Aan het College van Burgemeester en Wethouders en de gemeentesecretaris
van de gemeente Rheden
Postbus 9110
6994 ZJ DE STEEG

Onderwerp: Management letter 2024
Kenmerk: 06-01-2025

Geacht college, geachte gemeentesecretaris,

Als onderdeel van de jaarrekeningcontrole van boekjaar 2024 van de gemeente Rheden 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.

Ondertekening alleen in definitieve versie

M.C.J.M. Bekker 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.
Algemene conclusie interne beheersing	De gemeente Rheden hecht belang aan een goede interne beheersing en heeft de ambitie om de interne beheersing naar een hoger niveau te tillen. Met het programma “Versterking Financiële Functie Rheden 2024-2027” geeft u hier invulling aan. Wij constateren dat de gemeente veel punten onderhanden heeft en daarop vooruitgang laat zien (zie pagina 10 en 11). Het voorgaande laat onverlet dat bij diverse processen nog wel verbeteringen mogelijk c.q. noodzakelijk zijn. Belangrijke onderdelen zijn daarbij het inrichten van, en bij andere processen ook het technisch afdwingen van (controle-technische) functiescheiding.
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 drie applicaties bekeken (Unit4, Cision Samenlevingszaken en Youforce). Als onderdeel van onze jaarrekeningcontrole komt uit onze IT-audit naar voren dat op de door ons geïdentificeerde aandachtsgebieden van automatisering belangrijke onderdelen, zoals het netwerk en de financiële applicatie, nog verbeteringen mogelijk c.q. noodzakelijk zijn. Enerzijds in verband met de risico's die er mee samenhangen. Anderzijds om de IT-omgeving de bedrijfsvoering zo goed mogelijk te laten faciliteren. De bevindingen zien met name toe op de wachtwoordlengte van het netwerk en periodiciteit van de controles op het informatie beveiligingsbeleid. Verder adviseren wij u om de verbeteracties van De Connectie te blijven monitoren ten behoeve van de ISAE 3402 Type 2.



1. Management samenvatting

Onderwerp	Toelichting
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.
Vorbereidingen jaarrekeningcontrole 2024	We hebben met uw gemeente afspraken gemaakt over de planning van de jaarrekeningcontrole 2024. Op voorhand identificeren we een aantal onderwerpen/posten (o.a. waardering gemeentehuis, grondexploitatie, reserves en voorzieningen) met verhoogde aandacht in onze controle. Deze onderwerpen/posten stemmen wij voorafgaand aan de controle met u af, zodat de uitgangspunten en de verwerkingswijze in de jaarrekening tijdig zijn afgestemd. Daarnaast dient uw gemeente zich te focussen op een duidelijke interne planning met verantwoordelijkheden en interne kwaliteitscontroles voor het opstellen van de jaarrekening en onderliggend dossier om de controle soepel te laten verlopen. Wij vragen u het controleproces voor de jaarrekening 2024 goed voor te bereiden.
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.
Onderlinge samenwerking	Wij ervaren een prettige en constructieve wijze van samenwerken met de ambtelijke organisatie. Voorbeelden hierbij zijn de afstemming over de steekproeven en de afstemming over de nota inzake reserves. In onze werkwijze nemen wij de uitkomsten van de evaluatie met de organisatie mee. We hebben met de gemeente Rheden duidelijke afspraken gemaakt met betrekking tot de controlemomenten en op te leveren stukken. De gemaakte afspraken zijn tot op heden nagekomen.

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 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 gemeente relevant zijn in onze controle meenemen. De risicoanalyse is een continue proces en stellen wij gedurende de controle indien nodig bij.

De belangrijkste kernpunten in de controle bij uw gemeente zijn:

- Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de schattingsposten in de grondexploitatie en voorzieningen en sturing in budgetten en kredieten.
- Waardering van uw grondexploitatie;
- Waardering van het nieuwe gemeentehuis;
- Reserves en voorzieningen;
- De rechtmatigheidsverantwoording;
- Prestatielevering inkopen;
- Prestatielevering lasten WMO en Jeugdzorg;
- Handmatige c.q. spoedbetalingen.

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

Van de tien openstaande bevindingen uit voorgaand jaar (zowel management letter als accountantsverslag) zijn twee bevindingen afgerond en twee bevindingen onderhanden.

Sociaal Domein

We hebben geen nieuwe bevindingen geconstateerd m.b.t het sociaal domein. Van de vier openstaande bevindingen uit voorgaand jaar zijn twee bevindingen onderhanden.

Subsidies

De openstaande bevinding vanuit voorgaand jaar is afgerond en een nieuwe bevinding is opgenomen.

**Prioriteit
bevindingen (exclusief IT)**

-  **Geen wijziging : 9**
-  **Onderhanden: 11**
-  **Afgerond: 3**
-  **Nieuw: 2**

Inkopen & aanbesteding

Van de drie openstaande bevindingen uit voorgaand jaar zijn alle bevindingen onderhanden.

Betalingen

Van de openstaande bevinding uit voorgaand jaar hebben wij beperkte ontwikkelingen waargenomen ten opzichte van voorgaand jaar.

Baten

We hebben een nieuwe bevinding geconstateerd in het huidige boekjaar (onderdeel leges). De openstaande bevindingen uit voorgaande jaren zijn onderhanden (leges en subsidiebaten).

IT omgeving

Wij hebben geconstateerd dat er verbeteringen zijn doorgevoerd in de IT-omgeving. Daarnaast onderkennen wij een aantal adviespunten. Dit is uitgewerkt in hoofdstuk 3.



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 de bijlage.

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

#	Herkomst	Proces	Bevinding	Status
1	2024	Baten (leges)	Aansluiting subadministratie met en financiële administratie	
2	2024	Subsidieverstrekkings	Onvoldoende structuur in administratieve verwerking subsidies	
3	2021	Aanbestedingen	Startformulier niet gehanteerd	
4	2021	Betalings	Zelfstandig betaalbevoegdheden bij de Rabobank voor de Burgemeester	
5	2020	Sociaal Domein	Signaleringslijsten onvoldoende gecontroleerd	
6	2020	Sociaal Domein	Bevoegdheden per functionaris onlogisch	
7	2020	Inkopen	Bij het autoriseren van inkoopfacturen wordt de prijs en prestatie onvoldoende onderbouwd	
8	2020	Inkopen	Geen zicht op naleving aanbestedingsrichtlijn	
9	2020	Baten (leges)	Geen zichtbare toets op heffingsgrondslag bij leges voor omgevingsvergunningen	
10	2020	Subsidieverstrekkings	Onvoldoende structuur en documentatie bij subsidieverstrekkings en –vaststellingen	
11	2020	Financieel (administratie)	Onvoldoende controle op verwerking van begrotingswijzigings	
12	2020	Financieel (treasury)	Onduidelijke afspraken over treasurybeheer	
13	2020	Financieel (treasury)	Het treasurystatuut is verouderd	
14	2019	Sociaal Domein	Geen functiescheiding bij aanmaken en muteren van stamgegevens crediteuren	
15	2019	Sociaal Domein	Onvoldoende documentatie en collegiale toetsing in dossiers	



2. Kwaliteit interne beheersing

Belangrijkste aanbevelingen - vervolg

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

#	Herkomst	Proces	Bevinding	Status
16	2018	Financieel (administratie)	Onvoldoende functiescheiding tussen maken, verwerken en controleren van memoriaalboekingen	●
17	2018	Baten (subsidiebatens)	Geen geformaliseerde procedure voor het aanvragen, registreren en monitoren van subsidiebatens	●
18	2016	Financieel (grondexploitatie)	Geen zichtbare interne beheersing bij actualisaties grondexploitaties	●
<i>Onderstaande bevindingen vloeien voort uit de voorgaande accountantsverslagen</i>				
19	2023	Financieel	Onderbouwing afschrijvingstermijn gemeentehuis opstellen	●
20	2023	Financieel	Verbeteren inzicht in investeringskredieten	●
21	2023	Financieel	Wij adviseren om de nota reserve & voorzieningen te actualiseren en de bestemmingsreserves op te schonen.	●
22	2023	Financieel	Voorzieningen adequaat onderbouwen met actueel meerjarenonderhoudsplan	●
23	2023	Financieel	SiSa-regelingen onvoldoende gemonitord en onderbouwd	●
24	2022	Baten	Tijdig opboeken opbrengsten	●
25	2022	Baten	Debiteurenposities strakker monitoren.	●

2. Kwaliteit interne beheersing



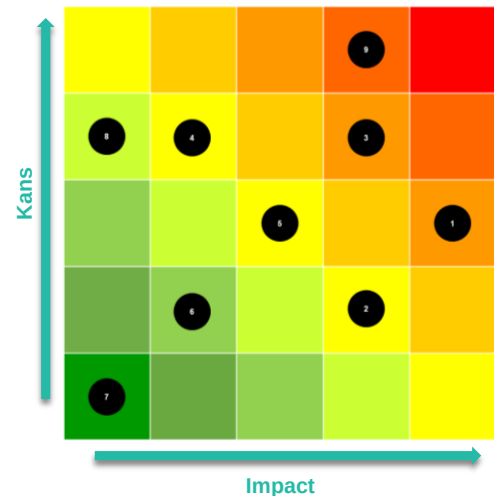
Frauderisicoanalyse

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 risicospons 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. Gemeente Rheden heeft enkele jaren geleden een fraude-risicoanalyse laten opstellen door een externe partij. Actualisering van deze frauderisico-analyse heeft echter tot op heden nog niet plaatsgevonden. U geeft aan in regionaal verband een risicoscan samen met de gemeente Arnhem, de gemeente Renkum en de Connectie te ambiëren. 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. De risico-afweging kan door de kans- en impactweging van frauderisico's via een risicomatrix worden weergegeven 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.





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

Fraude- en corruptierisico's

Op basis van de aanscherping, de kennis van uw organisatie en de interim-controle onderkennen wij de volgende frauderisico's bij onze jaarrekeningcontrole:

Nr	Fraude-/corruptierisico	Risico
1	Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op schattingsposten in de grondexploitatie en voorzieningen en sturing in budgetten en kredieten.	Hoog
2	Corruptierisico ten aanzien van omvangrijke contracten	Midden
3	Het risico dat handmatige c.q. spoedbetalingen uitgevoerd worden aan niet-rechthebbenden. Dit risico ziet bij uw gemeente met name toe op de kosten.	Midden
4	Bedrijfslasten zijn niet nauwkeurig verantwoord doordat de inkoopfactuur niet in overeenstemming is met de geleverde prestatie.	Midden

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.



2. Kwaliteit interne beheersing

Samenwerking en ontwikkelingen

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 gemeentelijke 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 in een prettige en op constructieve wijze samengewerkt met de gemeente. Belangrijke elementen in de samenwerking hierbij zien onder andere toe op: • proactieve afstemming van bijzonderheden en/of belangrijke aandachtsgebieden, bijvoorbeeld ten aanzien van de grondexploitatie; • inspanning om te zorgen dat alle gewenste informatie op een adequate wijze en voor aanvang van de controle aanwezig is; • 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 (VIC). Wij merken op dat de kwaliteit van de VIC de afgelopen jaren is verbeterd. Wij zien dit vooral terugkomen in de uitwerkingen en het zelfstandig trekken van de selecties. Ook bent u bezig met het intensiveren van de samenwerking tussen de VIC inzake de getrokken steekproeven en de kwaliteitscontroles door kwaliteitsmedewerker, waardoor efficiëntie kan worden behaald. Verdere verbetermogelijkheden zien toe op: • opzet van het controleplan waarin aandacht is besteed aan de risicoanalyse; • meer uniforme werkwijze met gebruik van standard formats; • het nader concretiseren van de VIC werkzaamheden d.m.v. het opstellen van een jaarplanning.
Versterken financiële functie	Voor het verbeteren van de interne beheersing en de kwaliteit van de financiële verslaggeving bent u in 2024 het programma “Versterken Financiële Functie Rheden” gestart. Wij onderschrijven de doelstellingen van dit programma. Aangezien het programma veel aspecten binnen de gemeente raakt is het belangrijk het programma op te knippen in kleinere onderdelen. Het afbaken zorgt voor overzicht en hiermee kunnen tussentijds successen gevierd worden. De basis is hiervoor gelegd in het programma en wij adviseren de planning nader te concretiseren in de deelplannen. Verder is het goed om te vernemen dat u beseft dat dit tijd en geld kost. Het vrijmaken van capaciteit is dus een vereiste om succes te behalen. Bovendien is het belangrijk dat iedereen binnen de gemeente beseft wat zijn of haar verantwoordelijkheden zijn omtrent financiën en het afleggen van verantwoording, want de financiële functie kan niet alleen versterkt worden door afdeling Financiën of Control, maar vraagt verantwoordelijkheid en cultuuromslag binnen de gehele gemeente.



2. Kwaliteit interne beheersing

Samenwerking en ontwikkelingen

Onderwerp	Omschrijving
Prestatielevering zorglevering	In de huidige situatie is uw gemeente in belangrijke mate afhankelijk van de productieverantwoordingen (met bijbehorende controleverklaringen) van zorgaanbieders voor zorg in natura (op basis van het landelijke ISD-controleprotocol) voor het aspect prestatielevering. Het biedt onder andere de volgende voordelen om als gemeente zelfstandig de prestatielevering van de zorg te monitoren: • Minder tot geen onzekerheden in de controle wat voordelen biedt richting de verwachte aanpassing van de materialiteit naar 2% voor fouten en onzekerheden gezamenlijk vanaf 2025. • Een indicatie voor zorgfraude wordt eerder gesignaleerd doordat analyses mogelijk zijn om patronen te onderzoeken • Tussentijdse sturing op afspraken wat leidt tot een hoger kwaliteitsniveau van de zorglevering. De gemeente kan zelfstandig de prestatielevering meten door een controlemix aan beheersingsmaatregelen, waaronder het inrichten en genereren van sturingsinformatie vanuit de herindicatiegesprekken. Vanuit Baker Tilly kunnen wij meedenken in het dashboards van dergelijke informatie. Wij adviseren u een plan van aanpak te maken welke maatregelen de prestatielevering van de zorg voldoende kan onderbouwen.

3

IT omgeving





3. IT-omgeving

Inleiding

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

Samenvatting bevindingen

De tabel op deze 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	Toegangs-beveiliging	Wijzigings-beheer	Continuïteit	Proces
Netwerk		N.v.t.		Algemeen
Unit4 Financials				Financiële administratie
Civision Samenlevingszaken	N.v.t.			Sociaal Domein
Youforce	N.v.t.			HR- en Salarisverwerking





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 er verbeteringen zijn doorgevoerd op de volgende aspecten in het IT-landschap gedurende 2024:

- Vooruitgang in de geplande transities en implementatie van het gewenste IT-landschap voor de toekomst. Hiervoor heeft de gemeente in samenwerking met andere deelnemers uit G3DC (Gemeenten Arnhem, Renkum en Rheden en De Connectie) de Regionale Enterprise Architectuur verder geactualiseerd op basis van de GEMMA principes en de vernieuwde blik op Common Ground voor informatiebeheer. Dit plan vormt de link tussen strategie en missie en de vormgeving door de bedrijfsarchitectuur.

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 voor Civision Samenlevingszaken zijn niet formeel vastgelegd en geïmplementeerd (geen formele procedure wijzigingsbeheer, 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 de uitbesteedde processen t.b.v. het technisch beheer van de IT infrastructuur en Unit4 adequaat in te richten en te monitoren. Denk hierbij aan het periodiek analyseren van de Service Level Rapportages (SLR) op de gemaakte afspraken in de Service Level Agreement (SLA) en het jaarlijks beoordelen van Assurance rapportages op bevindingen en maatregelen die onder uw eigen verantwoordelijkheid vallen (de zogeheten User Entity Controls).

3. IT-omgeving

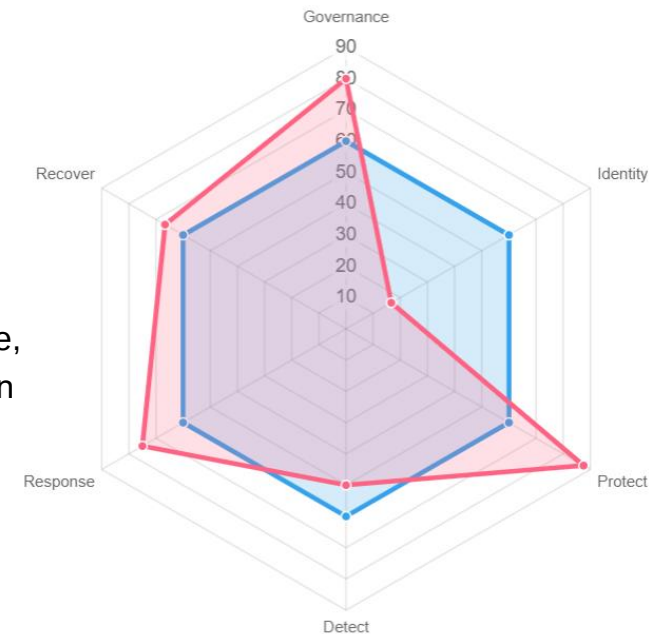
Cybersecurity

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.

In het spinnenweb is uw score weergegeven als een ratio waar 0 % de laagste en 100 % de hoogste score is. Rood betreft uw score. Blauw betreft de best practice ten aanzien van de EU wetgeving NIS2 en de Nederlandse vertaling in de Cyberbeveiligingswet vallen. Op veel vlakken scoort u beter dan de best practice, aandachtsgebieden zitten bij identificatie van kritieke gegevens, cyberrisico's en maatregelen en detectie van verdacht gedrag. In de bijlage 6.2 is de Cybersecurity NIS2 scan verder uitgewerkt.

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.





3. IT-omgeving

NIS2

In Nederland is de Cyberbeveiligingswet (verder: Cbw) in ontwikkeling welke vanaf 2025 verplicht zal worden en de EU richtlijn Network and Information Systems Directive (verder: NIS2) 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.

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.

4

Vorbereitung jaarrekening- controle





4. Voorbereiding jaarrekeningcontrole

Planning

In april controleren wij een aantal specifieke posten. Wij starten met de jaarrekeningcontrole op 12 mei 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 LOTS-lijst aanleveren, inclusief deadlines voor de aanlevering van de documentatie.

Aanvullende gegevensgerichte werkzaamheden

Voor aanvang van de jaareinde controle zullen wij de belangrijkste deelwaarnemingen gezamenlijk uitzetten. Het vooraf in samenwerking uitzetten van de selecties heeft als bijkomend voordeel dat de steekproeven correct worden getrokken om te kunnen hanteren in ons controledossier en dat de medewerkers de benodigde controledocumentatie 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 waardering gemeentehuis, grondexploitatie, reserves en voorzieningen;
- 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 LOTS. Wij kunnen begin 2025 een informatiesessie organiseren voor de LOTS;
- Wij vernemen graag eind 2024 welke posten eerder gereed zijn voor de controle in april 2025.
- 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
Journal entry testing op basis van auditfile	Door het inlezen van de auditfile in onze data factory, krijgen wij snel en diepgaand inzicht in de financiële transacties binnen uw organisatie.
Bankanalyse uitgaande betalingen	Door het inlezen van de CAMT.053 en SEPA bestanden in onze data factory, krijgen wij snel en diepgaand inzicht in alle uitgaande betalingen die zijn verricht vanuit de betaalomgeving van de BNG.
Analyse workflow inkoopfacturen	Door het verkrijgen van de juiste extractie uit de financiële administratie krijgen wij inzicht in de workflow van inkoopfacturen en kunnen wij beoordelen of de interne beheersingsactiviteit (de autorisatie van inkoopfacturen komt in functiescheiding tot stand) gedurende het jaar heeft gewerkt.
Analyse workflow crediteurenstamgegevens	Door het verkrijgen van de juiste extractie uit de financiële administratie krijgen wij inzicht in de workflow van de crediteurenstamgegevens (specifiek gericht op de IBAN) en kunnen wij beoordelen of de interne beheersingsactiviteit (de mutatie van crediteurenstamgegevens komt in functiescheiding tot stand) gedurende het jaar heeft gewerkt.
Analyse workflow memoriaalboekingen	Door het verkrijgen van de juiste extractie uit de financiële administratie krijgen wij inzicht in de workflow van de memoriaalboekingen (specifiek gericht op de module aanvragen memoriaal) en kunnen wij beoordelen of de interne beheersingsactiviteit (memoriaalboekingen komen in functiescheiding tot stand) gedurende het jaar heeft gewerkt.

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 premiereregeling 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 worden pensioenen niet meer direct betaald vanuit de gemeente. Daarnaast zal hiermee de pensioenvoorziening voor (voormalig) wethouders verdwijnen.

5. Actualiteiten

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 gefinancierd. 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 voor veel gemeenten 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 niet gevoerd. Wij begrijpen dat hier in Rheden wel sprake van is, desondanks adviseren we om (het proces rondom) de rechtmatigheidsverantwoording 2024 bij u intern te evalueren.

5. Actualiteiten

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;
- ❑ 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.



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 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 duurzaamheidsverslag-geving 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 helpen u als gemeente 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.

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.



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.

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.

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.

6 Bijlagen



6.1 Bijlagen



Detailbevindingen interne beheersing – Bevindingen per proces

Op de volgende pagina's zijn de detailbevindingen ten aanzien van de belangrijkste processen opgenomen. Per bevinding is het advies en de status weergegeven.

Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze managementletters 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 - Gemeente heeft besloten bevinding niet op te volgen	Nr	Jaar	Proces	Bevinding	Ontwikkelingen	Status 2024
	1	2024	Leges	Aansluiting tussen subadministratie en financiële administratie	Wij vragen uw aandacht voor tussentijdse aansluiting van de opgelegde leges volgens de subadministratie RX Mission met de financiële administratie zodat tijdig eventuele verschillen uitgezocht kunnen worden. Dit verbetert de kwaliteit van de financiële administratie. Deze bevinding is eveneens door concern control van uw gemeente geconstateerd.	
	2	2024	Subsidie-verstrekkings	Onvoldoende structuur in administratieve verwerking subsidies	Wij vragen uw aandacht om administratief meer structuur aan te brengen voor het boeken van verstrekte subsidies. Nu wordt dit veelal op dezelfde wijze als inkoopfacturen verantwoord. Door een eenduidige boekingsgang krijgt u een zuivere subsidiepopulatie in uw administratie.	
	3	2021	Aanbestedingen	Startformulier niet gehanteerd	Voor alle inkopen boven de EUR 10.000 is een zogeheten inkoopmelding verplicht gesteld (via Topdesk) zoals vastgesteld in het vigerende Rhedens inkoopbeleid. Wij hebben nog niet kunnen vaststellen of dit altijd gebeurt. Ook zien wij geen waarborg die zorgt dat altijd een formulier wordt gehanteerd	
	4	2021	Betalingen	Zelfstandig betaalbevoegdheden bij de Rabobank voor de Burgemeester	U geeft aan in overleg te zijn met de Rabobank hoe de bevoegdheden beperkt kunnen worden.	
	5	2020	Sociaal Domein	Signaleringslijsten onvoldoende gecontroleerd	Geen wijzigingen.	
	6	2020	Sociaal Domein	Bevoegdheden per functionaris onlogisch	U geeft aan dat in alle sjablonen de digitale handtekening van de teamleider standaard wordt afgedrukt conform mandaat. Het feit dat de handtekening van de teamleider wordt gebruikt zonder goedkeuring vanuit de teamleider zelf is daarin onwenselijk. Wij adviseren u om de functionarissen die de beschikking afgeven op basis van onder-mandatering tekeningsbevoegdheid te geven.	

6.1 Bijlagen



Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze managementletters 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
-  Gemeente heeft besloten bevinding niet op te volgen

Nr	Jaar	Proces	Bevinding	Ontwikkelingen	Status 2024
7	2020	Inkopen	Bij het autoriseren van inkoopfacturen wordt de prijs en prestatie onvoldoende onderbouwd	U geeft aan de beschrijving van de werkwijze op te pakken binnen het programma versterken financiële functie (VFF). Dit staat op de planning voor 2027.	
8	2020	Inkopen	Geen zicht op naleving aanbestedingsrichtlijn	Wij vragen uw aandacht voor het tussentijds monitoren van mogelijke overschrijdingen van de aanbestedingsgrenzen door middel van een periodieke spendanalyse.	
9	2020	Leges	Geen zichtbare toets op heffingsgrondslag bij leges voor omgevingsvergunningen	Wij bevelen aan om een bouwkostentoets te implementeren om de volledigheid van de opbrengsten uit omgevingsvergunningen te bewaken. De nieuwe legesverordening (onderdelen fysiek domein) is op 24 september 2024 vastgesteld in de Raad. U geeft aan dat hiermee de werkwijze is aangepast, maar dit vindt nog niet structureel plaats.	
10	2020	Subsidie-verstrekingen	Onvoldoende structuur en documentatie bij subsidieverstrekingen en -vaststellingen	In 2024 is er meer structuur gekomen in het proces. Wel vragen wij uw blijvende aandacht hiervoor omdat onderbouwing bij elke subsidieverstreking en -vaststelling belangrijk is.	
11	2020	Administratie & verslaglegging	Onvoldoende controle op verwerking van begrotingswijzigingen	De inhoudelijke toetsing wordt uitgevoerd vanuit verschillende functies binnen de vakgroep financiën. Hier zijn concrete werkafspraken voor gemaakt, die nog moeten worden vevat in een memo.	
12	2020	Treasury	Onduidelijke afspraken over treasurybeheer	U geeft aan deze verantwoordelijkheid te hebben belegd bij de financieel controller, die de rol van treasurer heeft. Daarbij wordt hij ondersteund door de Connectie.	
13	2020	Treasury	Het treasurystatuut is verouderd	Geen wijzigingen. Wij vragen uw aandacht voor het opstellen van liquiditeitsprognoses. U geeft aan dit in 2025 op te pakken binnen het programma versterken financiële functie (VFF).	

6.1 Bijlagen



Deze tabel geeft een overzicht van de follow-up van de (overige) aanbevelingen uit onze managementletters 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
-  Gemeente heeft besloten bevinding niet op te volgen

Nr	Jaar	Proces	Bevinding	Ontwikkelingen	Status 2024
14	2019	Sociaal Domein	Collegiale toetsing / toetsing kwaliteitsmedewerker	Bij jeugd dient altijd een collegiale toets en een kwaliteitstoets plaats te vinden. Bij WMO vindt collegiale toetsing bij 'risico' dossiers plaats, waaronder tenminste toekenningen groter dan EUR 50.000. Vanuit de kwaliteitsmedewerker WMO zal met terugwerkende kracht over 2024 controles plaatsvinden. Wij vragen daarbij uw aandacht voor het zichtbaar en herleidbaar maken van de wijze waarop deze selectie wordt bepaald.	
15	2019	Sociaal Domein	Geen functiescheiding bij aanmaken en muteren van stamgegevens crediteuren	U geeft aan dat medewerker interne controle dit onderhanden heeft.	
16	2018	Administratie & Verslaglegging	Onvoldoende functiescheiding tussen maken, verwerken en controleren van memoriaalboekingen	In februari 2024 is de afspraak vastgelegd dat alleen de medewerkers financieel beheer memoriaal boekingen mogen aanleveren bij de Connectie. De financieel adviseur moet de memoriaal boeking daardoor eerst ter controle aanleveren bij de medewerker financieel beheer. De controle is echter niet zichtbaar. U geeft aan de beschrijving van de werkwijze op te pakken binnen het programma versterken financiële functie (VFF). Daarnaast vragen wij u de boekingen die door de Connectie zijn verwerkt, zichtbaar te controleren.	
17	2018	Subsidiebaton	Geen geformaliseerde procedure voor het aanvragen, registreren en monitoren van subsidiebaton	Het borgen van de verantwoording op ontvangen subsidies wordt opgepakt in het programma versterken financiële functie (VFF). De planning hiervan is 2028.	
18	2016	Grondexploitatie	Geen zichtbare interne beheersing bij actualisaties grondexploitaties	Wij vragen uw aandacht om de controles op de calculatie zichtbaar te maken. De controle dient door een andere functionaris te worden uitgevoerd dan de functionaris die de calculatie heeft opgesteld. U geeft aan de werkwijze op te pakken binnen het programma versterken financiële functie (VFF).	

6.1 Bijlagen



Nr	Jaar	Proces	Bevinding	Ontwikkelingen	Status 2024
19	2023	Financieel	Onderbouwing afschrijvingstermijn gemeentehuis opstellen	De levensduurverwachting ten aanzien van deze investeringen is ten tijde van de jaarrekeningcontrole 2023 besproken. Daarbij is de inschatting dat duurzaamheidsaspecten levensduur verlengend zijn ten opzichte van de oude bouwmaterialen, waarbij het afschrijvingstermijn vooralsnog wordt ingestoken op basis van 50 jaar, hetgeen nog door de gemeente onderbouwd zal moeten worden. De nota waardering en afschrijvingen zou vervolgens daarop moeten worden aangepast.	
20	2023	Financieel	Verbeteren inzicht in investeringskredieten	Het genereren van een goed overzicht van de investeringskredieten en de besteding op de kredieten is moeilijk voor de organisatie. Wij adviseren u uw administratie beter te ordenen, zodat er tijdig en adequaat inzicht is in de investeringskredieten. Tevens adviseren wij de kredieten op te schonen en af te sluiten. Het actualiseren van de nota vaste activa kan hierbij structuur bieden.	
21	2023	Financieel	Actualiseren nota reserve & voorzieningen en de bestemmingsreserves opschonen	Uw gemeente had ultimo 2023 veel bestemmingsreserves (€ 18,1 miljoen verspreid over meer dan 30 reserves). Op sommige reserves vinden geen mutaties plaats. Wij hebben geadviseerd om de nota reserve & voorzieningen te actualiseren om de bestedingsdoelen van de reserves duidelijk te hebben. De concept nota en het voorstel van opschonen hebben wij ingezien en van commentaar voorzien, waardoor dit punt ultimo 2024 afgewikkeld zal zijn.	
22	2023	Financieel	Voorzieningen adequaat onderbouwen met actueel meerjarenonderhoudsplan	Wij hebben in de controle geconstateerd dat het vormen en muteren van voorzieningen beter aangestuurd en geadmistreerd kan worden. Bovendien is voor het vormen van een voorziening belangrijk om de richtlijnen van het BBV te volgen. Zo dient de voorziening voor groot onderhoud aan te sluiten op het beheersplan en een actueel meerjarenonderhoudsplan. Om deze voorziening in de jaarrekening 2024 te handhaven dient de onderbouwing aanwezig te zijn.	
23	2023	Financieel	SiSa-regelingen onvoldoende gemonitord en onderbouwd	Wij adviseren om de subsidie beschikking kritischer te lezen op de verantwoordingsverplichtingen en dit goed te registreren waardoor de verantwoording beter opgesteld kan worden. Kennis van de regelgeving is hierbij een vereiste. Daarnaast is het belangrijk de aansluiting tussen de SiSa-regeling en de jaarrekening/administratie te verbeteren.	
24	2022	Baten	Tijdig opboeken opbrengsten	Bij voorgaande jaarrekeningcontroles bleek dat gedurende het jaar meerdere geldbedragen worden ontvangen per bank die niet zijn toe te wijzen aan een opgeboekte vordering of factuur. De onvolledige opboeking/verantwoording van de vorderingen en de daarbij behorende opbrengst in de financiële administratie leidt tot onvoldoende inzicht en het mislopen van gelden. Wij adviseren u dit nader te analyseren en acties uit te zetten dat de financiële administratie volledig en tijdig actueel is.	
25	2022	Baten	Debiteurenposities strakker monitoren	Wij merken dat veel vorderingen en transitorische balansposten verouderde vorderingen bevatten. Wij vragen u de overzichten op te schonen en af te letteren om een beter inzicht te hebben in de saldo's. Daarnaast worden de invorderings-procedures niet gevolgd wat leidt tot een groot debiteurenrisico en te nemen verliezen omdat debiteuren niet betalen. Tevens is het belangrijk jaarlijks de voorziening oninbaarheid te actualiseren. In 2023 was de onderbouwing van de debiteuren beter dan 2022.	



6.2 Bijlage IT-omgeving

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.



6.2 Bijlage IT-omgeving

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.

discontinuïteit van belang. Hiernaast schatten wij uw beheersing van cyber risico's in.

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

6.2 Bijlage IT-omgeving

Detailbevindingen interne beheersing – Toegangsbeveiliging netwerk

	Authenticatie 	Autorisatie 
Constatering	<i>De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 31-12-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.</i> De ingestelde wachtwoordeisen van het netwerk zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen. Wachtwoordrestricties binnen het netwerk wijken echter af van het beleid. Het wachtwoordbeleid schrijft een minimale lengte van 12 voor, terwijl dit is ingesteld op 8. Tevens hebben wij beperkingen geconstateerd ten aanzien van de periodieke controle op actieve gebruikers.	<i>De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 31-12-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.</i> In relatie tot de jaarrekeningcontrole is het van belang dat de hoge rechten op het netwerk beperkt zijn ingericht. De hoge rechten (rechten om gebruikers(rechten) te muteren) in de Windows Active Directory zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole, en zijn niet betrokken bij processen die relevant zijn voor de jaarrekening. Wel hebben wij geconstateerd dat de periodieke controle op autorisatiebeheer niet maandelijks conform beleid heeft plaatsgevonden en dat hoge rechten accounts niet zijn meegenomen in de controle.
Risico	Het risico bestaat dat personen toegang kunnen krijgen tot het netwerk terwijl deze al uit dienst zijn.	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.
Aanbeveling	Wij adviseren u om de ISAE rapportage van de Connectie jaarlijks te beoordelen op bevindingen, en hierover in gesprek te gaan met de Connectie. Tevens raden wij aan om dit proces te documenteren.	
Gevolgen voor de jaarrekeningcontrole	De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 1-1-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.	

6.2 Bijlage IT-omgeving

Detailbevindingen interne beheersing – Toegangsbeveiliging en wijzigingsbeheer Unit4 Financials



	Authenticatie 	Autorisatie 	Wijzigingsbeheer 
Constatering	<i>De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 31-12-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.</i> De ingestelde wachtwoordeisen van de applicatie zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen. Wachtwoorden dienen te voldoen aan het wachtwoordbeleid, met uitzondering van de wachtwoordlengte welke was ingesteld op 8 in plaats van 12. Hierbij voldoet het wachtwoordbeleid wel aan de best practice. Tevens hebben wij beperkingen geconstateerd ten aanzien van de periodieke controle op actieve gebruikers.	<i>De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 31-12-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.</i> De hoge rechten voor het muteren van gebruikers in Unit4 zijn op het moment van controle belegd bij onafhankelijke functionarissen. Wij hebben echter geconstateerd dat de periodieke controle op autorisatiebeheer niet maandelijks conform beleid heeft plaatsgevonden en dat hoge rechten accounts niet zijn meegenomen in de controle. Daarnaast is er geen adequate logging aanwezig op wijzigingen van gebruikersrechten waarmee vastgesteld kan worden of hoge rechten voor de gehele periode juist belegd zijn geweest.	<i>De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 31-12-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.</i> Er is sprake van een procedure omtrent het gestructureerd doorvoeren van nieuwe releases in de applicatie. Deze procedure wordt jaarlijks gereviewd. Elk kwartaal wordt er een controle uitgevoerd of alle doorgevoerde releases conform de change management procedure zijn doorlopen. Bij deze controle zijn echter beperkingen geconstateerd, doordat bij 2 doorgevoerde wijzigingen geen sprake was van een testplan. Verder is er sprake van een gescheiden test- en productie omgeving.
Risico	Het risico bestaat dat personen toegang kunnen krijgen tot de applicatie terwijl deze al uit dienst zijn.	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 een testplan 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 de ISAE rapportage van de Connectie jaarlijks te beoordelen op bevindingen, en hierover in gesprek te gaan met de Connectie. Tevens raden wij aan om dit proces te documenteren.		
Gevolgen voor de jaarrekening-controle	De bevindingen zijn afkomstig uit het meest recente ISAE 3042 type 2 rapport van de Connectie, over de periode van 1-1-2023 tot en met 1-1-2023. De nieuwe rapportage over het boekjaar 2024 wordt naar verwachting in het voorjaar van 2025 beschikbaar gesteld. Houd er rekening mee dat de bevindingen over het boekjaar 2024 anders kunnen zijn.		



6.2 Bijlage IT-omgeving

Detailbevindingen interne beheersing – Wijzigingsbeheer Civision Samenlevingszaken

Wijzigingsbeheer

Constatering

Er vindt geen zichtbare vastlegging plaats van de risicoanalyse. De testwerkzaamheden worden niet uitgevoerd aan de hand van een testplan, niet zichtbaar gedocumenteerd en er vindt geen gebruikersacceptatie plaats. Afsluitend vindt er geen formele goedkeuring plaats voor het doorvoeren van de wijzigingen in de productieomgeving.

Risico

De kans bestaat dat niet alle wijzigingen met de juiste impact worden getest, met mogelijke gevolgen voor de betrouwbare gegevensverwerking binnen de applicatie.

Aanbeveling

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. Ten slotte adviseren wij u om key-users (de gebruikers die de applicatie bij de dagelijkse werkzaamheden veel gebruiken en veel kennis hebben van de applicatie) te laten testen en deze werkstap documenteren.

Gevolgen voor de jaarrekeningcontrole

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 releasenotes te analyseren. Op basis van deze werkzaamheden zijn er geen bevindingen geconstateerd welke impact hebben op de jaarrekeningcontrole.



6.2 Bijlage 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 jaarrekeningcontrole	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.



6.2 Bijlage IT-omgeving

Detailbevindingen interne beheersing – Continuïteitsmaatregelen en beveiliging

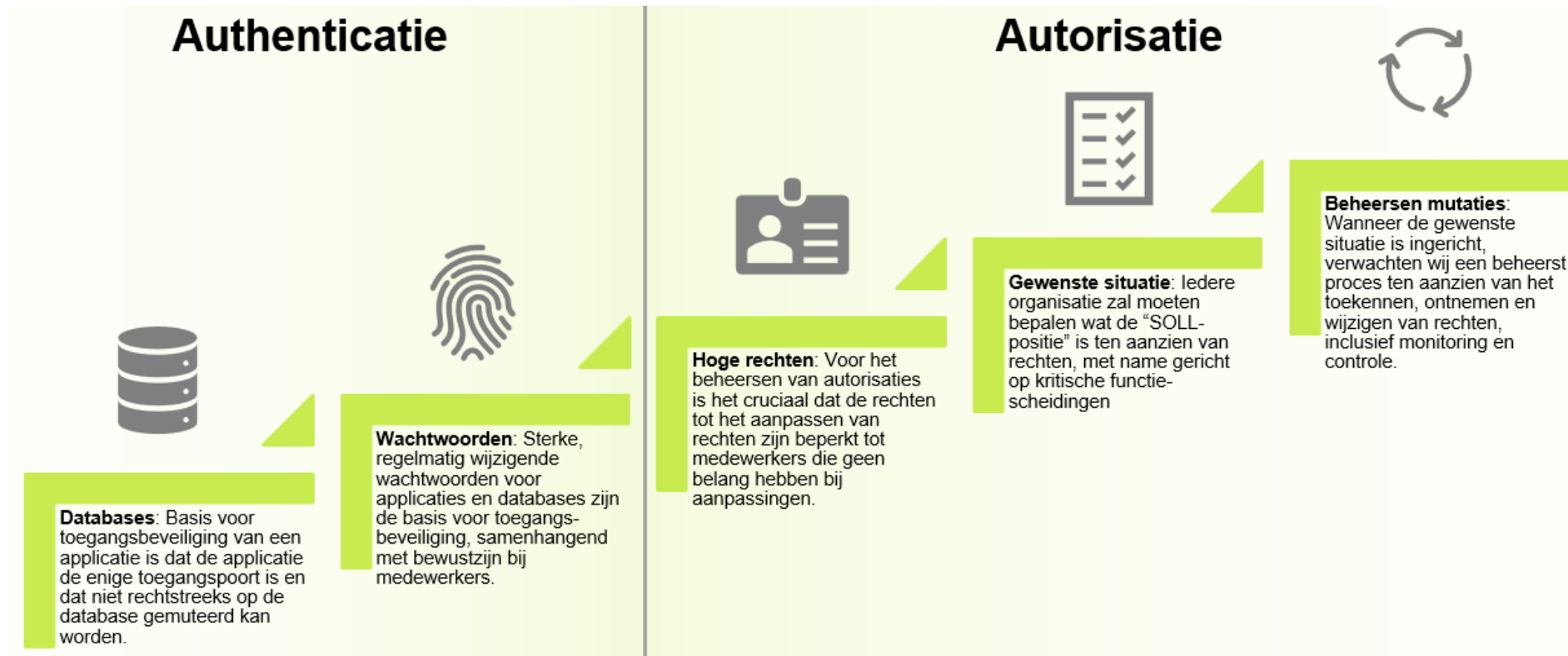
Onderstaande onderwerpen volgen uit interviews. Hierop zijn door ons over het algemeen geen testwerkzaamheden uitgevoerd om vast te stellen dat de IT-omgeving is ingericht zoals ons voorgesteld is. Dit beperkt de zekerheid die u kunt ontlenen aan de door ons beschreven aandachtspunten.

Onderwerp	Bevinding
Back-up	De gemeente heeft het operationele IT beheer uitbesteed aan de Connectie. De Connectie heeft procedures ingericht die beschrijven op welke wijze back-ups dienen plaats te vinden en omtrent het monitoren van back-ups.
Recovery	De gemeente heeft het operationele IT beheer uitbesteed aan de Connectie. De Connectie heeft een formele procedure die beschrijft op welke wijze en met welke periodiciteit recovery testen dienen plaats te vinden. Deze procedures zijn adequaat ingericht. Periodiek worden er recovery testen uitgevoerd en vindt hier terugkoppeling en eventueel opvolging op plaats. Dit wordt gedocumenteerd in Topdesk.
Uitwijk	De gemeente heeft het operationele IT beheer uitbesteed aan de Connectie. De Connectie heeft geen uitwijklocatie maar maakt gebruik van een failover configuratie met twee gespiegelde omgevingen. Elke omgeving is op een andere locatie, op die manier is er een locatie aanwezig die als back-up kan dienen. Hiervoor heeft de Connectie adequate procedures ingericht waarbij er periodiek een failover test worden uitgevoerd. Tevens vindt hier terugkoppeling en eventueel opvolging op plaats. Dit wordt gedocumenteerd in Topdesk.
Fysieke beveiliging	De servers staan fysiek op twee locaties in datacenters (met eigen toegangsprocedures). Daarnaast is het gebouw van de Connectie niet toegankelijk zonder toegangspas. De toegang is adequaat beveiligd. Monitoring ten van temperatuur e.d. zijn aanwezig en worden periodiek getest.
Remote acces	Voor remote toegang wordt gebruik gemaakt van two-factor authenticatie. Doordat de bedrijfskritische applicaties alleen bereikbaar zijn in de Citrix-omgeving waar altijd two-factor wordt afgedwongen voor de medewerkers van gemeente Rheden is het adequaat beveiligd.

6.2 Bijlage IT-omgeving

Toelichting 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.





6.2 Bijlage IT-omgeving

Toelichting 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.



6.3 Bijlage Cybersecurity en NIS2 scan

Cybersecurity NIS2 scan

1. Deze scan is bedoeld om u inzicht te geven in de staat van cyberweerbaarheid van uw organisatie. De lijst is niet uitputtend, maar betreft een focus op de belangrijkste punten.
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 ontleen aan de door ons beschreven aandachtspunten.
4. De score wordt weergegeven 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.
----------------	--

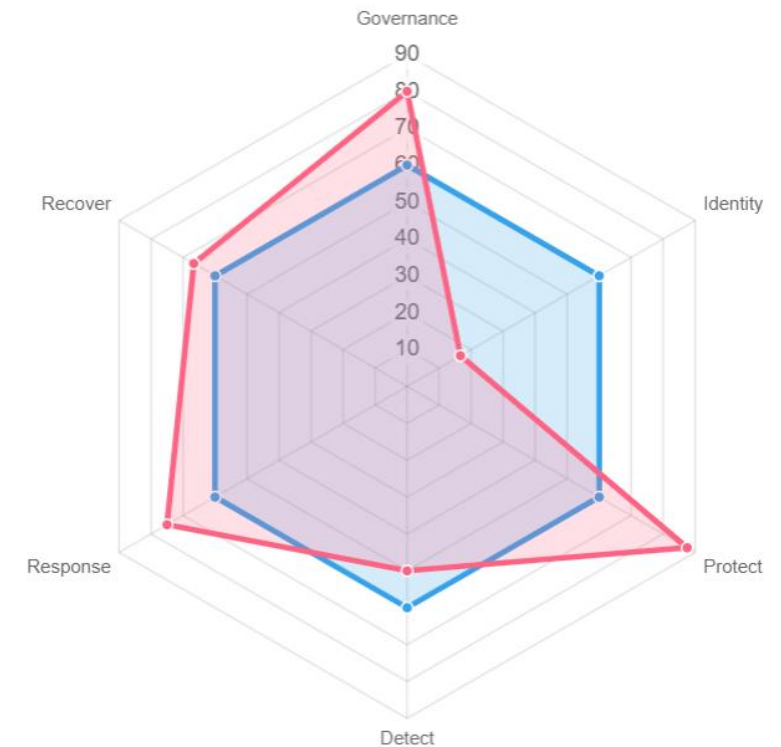
6.3 Bijlage Cybersecurity en NIS2 scan



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 en het bevoegd gezag heeft de verantwoordelijkheden en taken voor cyber-risico's in de eigen organisatie geformaliseerd. Ter verbetering valt te denken aan het creëren van een centraal overzicht van bedrijfsmiddelen en de interne en externe stakeholders / eigenaren.
Identificatie	Wij zien dat het identificeren van kroonjuwelen, risico's en maatregelen (ook bij leveranciers) directe actie vereist. 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 cyber-risico'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 opvragen van Service Level Rapportages en back-up rapportages door de Demand Managers zodat hier adequaat op gemonitord kan worden.
Detectie	Op basis van het model zien wij dat aandacht gegeven is aan monitoring en vulnerability scanning, maar dat er verbeterpotentieel ligt om de cyberweerbaarheid van uw organisatie te verhogen. Denk hierbij aan het aanscherpen van de procedures omtrent toegangsbeheer (met een bredere scope dan enkel de ENSIA), het minimaal jaarlijks uitvoeren van pentesten en het periodiek beoordelen van externe Assurance en Service Level Rapportages op beveiligingsmaatregelen van externe leveranciers.
Reactie	Reageren op incidenten en bijsturen op basis van inzichten is op orde. U heeft aangegeven dat het Business Continuity Management plan een punt van aandacht betreft, met name op het gebied van Governance. Deze zal volgend jaar worden herzien.
Herstel	Het herstellen naar normale bedrijfsvoering krijgt de nodige aandacht. Ter verdere verbetering kunt u denken aan het regelmatig oefenen met de back-up voorzieningen van systemen, operationele techniek en data binnen een uitgebreide scope, en of deze adequaat kunnen herstellen.



Contact

M.C.J.M. (Marc) Bekker RA

Extern accountant

+31 (0)6 15 30 36 59

m.bekker@bakertilly.nl

J.B. Vree-Brink MSc RA

Manager Audit

+31 (0)6 52 76 55 24

m.vree@bakertilly.nl

L.F. van Goor MSc RA

Junior Manager Audit

+31 (0)6 223 850 55

l.vangoor@bakertilly.nl

Kantoorgegevens

Baker Tilly (Netherlands) N.V.

Burg. Roelenweg 14-18

8021 EV Zwolle

Postbus 508

8000 AM Zwolle

T +31 (0)38 425 86 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.

