

Management letter

Gemeente Rheden

Boekjaar 2023

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

ONDERWERP:
Management letter 2023

DATUM:
22 december 2023

Geachte college,

Als onderdeel van de controle van de jaarrekening 2023 van gemeente Rheden hebben wij de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing beoordeeld, teneinde onze controlewerkzaamheden in overeenstemming met Nederlands recht waaronder de controlestandaarden te kunnen bepalen.

De opzet, het bestaan en in voorkomende gevallen de werking van de interne beheersingsmaatregelen van de belangrijkste bedrijfsprocessen, inclusief de geautomatiseerde gegevensverwerking, in uw organisatie zijn beoordeeld en getoetst zodat we een terugkoppeling kunnen geven over de betrouwbaarheid van de interne informatievoorziening en de jaarrekening.

Onze bevindingen zijn gebaseerd op de normale werkzaamheden in het kader van de jaarrekeningcontrole. Deze brief bevat daardoor niet alle onvolkomenheden in uw organisatie die bij een eventueel uitgebreid en hierop specifiek gericht onderzoek naar voren zouden kunnen komen. Zoals u zult begrijpen is de management letter van nature kritisch. Wij rapporteren over de eventuele leemtes of mogelijkheden ter verbetering van de financiële en administratieve processen, de administratieve organisatie daarvan en de daarin opgenomen maatregelen van interne beheersing.

Op uw verzoek geven wij in deze management letter aan op welke wijze verbeteringen van de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing kunnen worden gerealiseerd. De aanbevelingen en oplossingsrichtingen zoals beschreven in deze management letter bieden u handvatten voor deze uitwerking. Wij hebben de concept management letter toegelicht en besproken met een afvaardiging van de ambtelijke 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.



M.C.J.M. Bekker RA

Inhoudsopgave

CONTACT

M.C.J.M. Bekker RA
Extern accountant
m.bekker@bakertilly.nl

L.F. (Lisanne) van Goor MSc RA
Junior manager
l.vangoor@bakertilly.nl

KANTOORGEGEVENS
Baker Tilly (Netherlands) N.V.
Burgemeester Roelenweg 14-18
8021 EV Zwolle
Postbus 508
8000 AM Zwolle
+31 38 425 86 00



Bestuurlijke samenvatting



Bevindingen en aandachtspunten



Bevindingen IT beheersing



Bijlage 1



Bijlage 2



Bijlage 3

Bestuurlijke samenvatting



1. Bestuurlijke samenvatting

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 2023.



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.

De gemeente Rheden hecht belang aan een goede interne beheersing en heeft de ambitie om de interne beheersing naar een hoger niveau te tillen. Hoewel in 2023 slechts 1 bevinding geheel is opgelost (zie ook pagina 10) als gevolg van prioritering op onder andere de invoering van de rechtmatigheidsverantwoording, constateren wij ook dat de gemeente een aantal punten onderhanden heeft en daarop vooruitgang laat zien. De vakafdelingen hebben ons inziens, mede vanuit integraal managementperspectief op zijn minst een medeverantwoordelijkheid voor het verbeteren van de interne beheersing naar een hoger niveau. Daarnaast zijn goede stappen gezet richting de aanstaande rechtmatigheidsverantwoording. 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.

De jaarrekening 2023 en de controle daarvan zullen in het teken staan van de rechtmatigheidsverantwoording. De gemeente Rheden is de afgelopen periode bezig geweest met de verdere voorbereidingen op de rechtmatigheidsverantwoording. Diverse technische zaken zijn reeds opgepakt. Voor de onderbouwing van de rechtmatigheidsverantwoording ligt de lat hoog en moeten nog stappen gezet worden.

Bevindingen en aandachtspunten



© Baker Tilly

2. Bevindingen en aandachtspunten

2.1 Algemeen

Doel en reikwijdte

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

Risicoanalyse

Onze risicoanalyse richt zich op een betrouwbare totstandkoming van de jaarrekening. Dit betekent dat wij niet alle risico's die voor u als 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:

- Invoering van de rechtmatigheidsverantwoording (en de daarbij horende verantwoordelijkheden voor u);
- Waardering van uw grondexploitatie;
- Prestatielevering inkopen;
- Handmatige c.q. spoedbetalingen;
- Uitkeringen (lasten Participatiewet, WMO, Jeugd)
- Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels en ziet met name toe op schattingsposten.
- Corruptierisico ten aanzien van de Europese aanbestedingsrichtlijnen met het risico op belangenverstrengeling en kickbacks.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten. In 2023 is het risico inzake de getrouwheid van de rechtmatigheidsverantwoording (als onderdeel van de jaarrekening) toegevoegd. Het in voorgaande jaren onderkende belangrijk risico met betrekking tot de rechtmatigheid van de inkopen (aanbestedingsrechtmatigheid) is geherformuleerd als corruptierisico.

2. Bevindingen en aandachtspunten

2.1 Algemeen

Algemeen beeld	De gemeente Rheden hecht waarde aan een goede interne beheersing. We constateren dat de gemeente belang hecht aan voldoende functiescheiding binnen de primaire processen en de ambitie heeft om de interne beheersing naar een hoger niveau te tillen. Wij hebben vastgesteld dat een aantal bevindingen uit de voorgaande management letter is opgepakt waarmee vooruitgang wordt gerealiseerd. De opvolging daarvan wordt onder meer bekrachtigd door middel van een verbeterplan of memo. Echter constateren we ook dat enkele bevindingen niet binnen de geplande tijd zijn afgewikkeld als gevolg van prioritering op onder andere de invoering van de rechtmatigheidsverantwoording. Wij adviseren u om planmatig hierin te werk te gaan vanuit een visie op planning en control. Bijvoorbeeld het memo inzake 10-punten verbeterplan voor de subsidieverwerving is daarmee een voorbeeld hoe planvorming ook over de nog niet opgepakt bevindingen kan worden uitgerold. Aandachtpunt daarbij is om dit SMART te formuleren. Wij adviseren u om de verantwoordelijkheid van het opvolgen van de openstaande bevindingen ook neer te leggen bij de vakafdelingen om de aanbevelingen in samenspraak met controlling gezamenlijk en doelgericht uit te voeren. De vakafdelingen hebben namelijk vanuit ingetraal managementperspectief daarin ook zeker een mede-verantwoordelijkheid.
Zichtbaarheid interne beheersmaatregelen	De rechtmatigheidsverantwoording door het college stelt hogere eisen aan het interne beheersingssysteem. De aanwezigheid van een adequaat intern (financieel) beheersingssysteem is immers een essentiële randvoorwaarde om te kunnen bijsturen en de betrouwbaarheid van financiële informatie en verslaglegging is van groot belang om dit tijdig en goed te kunnen doen. Het voorgaande laat onverlet dat op onderdelen de interne beheersingsmaatregelen in het proces nog onvoldoende verankerd dan wel onvoldoende zichtbaar zijn. In die laatste situatie kan achteraf niet vastgesteld worden of de afgesproken procedures en interne controles wel hebben bestaan en gewerkt. De verbijzonderde interne controlefunctie kan in beide gevallen niet systeemgericht controleren en wij als accountant ook niet. Dat laatste betekent dat een controle meer tijd kost voor zowel de gemeente als voor ons. Daarnaast neemt hierdoor ook het risico op fouten en onrechtmatigheden toe. Bovendien ontbreekt, doordat geen systeemgerichte controle kan plaatsvinden, een automatisch mechanisme waarbij de efficiency, doelmatigheid en effectiviteit van de processen en daarin opgenomen interne beheersingsmaatregelen tegen het licht wordt gehouden.
Procesbeschrijvingen	Tot slot is het van belang dat de gemeente beschikt over procesbeschrijvingen, waaruit blijkt hoe interne controles er precies uitzien. De gemeente Rheden beschikt over een ruim aantal procesbeschrijvingen. De procesbeschrijvingen voor betalingsverkeer, inkopen en aanbestedingen, wet maatschappelijke ondersteuning, jeugd, personeel, belastingen heffingen, uitkeringen, en subsidieverstrekkingen zijn aanwezig. Er moeten nog procesbeschrijvingen opgesteld worden voor de processen subsidiebaten, omgevingsvergunningen, grondexploitatie, algemene uitkering en administratie en verslaglegging. Wij adviseren u hierin een uniforme werkwijze toe te passen en de mogelijkheden te onderzoeken van softwarematige tooling ter ondersteuning hierbij. Voor de aanwezige beschrijvingen adviseren wij om deze te verfijnen voor de “key-controls”. Belangrijk hierbij is om de "key-controls" zo scherp mogelijk te beschrijven aan de hand van de 6W's (wie, wat, waarom, wanneer, met welke informatie en wat wordt vastgelegd) zodat iedere betrokken functionaris weet wat er van hem of haar verwacht wordt en welke verantwoordelijkheden daarbij horen. Bijvoorbeeld bij de processtap jeugd inzake collegiale toetsing wordt een werkafspraak aangehaald als maatregel, waarbij de 6W’s onvoldoende naar voren komen. Een adequate beschrijving en toereikende inrichting en werking van de interne beheersing vormt de basis voor de verbijzonderde interne controle en voor ons als accountant om over te kunnen gaan van een gegevensgerichte naar een organisatiegerichte controlestrategie.

2. Bevindingen en aandachtspunten

2.1 Algemeen

Rechtmatigheidsverantwoording

Hierdoor kan een belangrijke randvoorwaarde gerealiseerd worden om te kunnen steunen op de maatregelen van interne beheersing waardoor minder gegevensgerichte detailcontroles hoeven te worden uitgevoerd. Daarnaast biedt een toereikende inrichting en werking van de interne beheersing ook een goede grondslag voor de rechtmatigheidsverantwoording door het college.

Tot en met boekjaar 2022 vormde de accountant een oordeel over de rechtmatigheid en bracht hierover verslag uit in de controleverklaring en het accountantsverslag. Met ingang van boekjaar 2023 wordt het een verplichting voor het college van burgemeester & wethouders om verantwoording af te leggen over de rechtmatigheid middels de rechtmatigheidsverantwoording. De verantwoording is gebaseerd op een standaard model dat bij wet is vastgelegd en dient te worden aangevuld met;

- Datum vaststelling normenkader
- Het door de raad vastgestelde grensbedrag;
- Wel of niet voldoen aan de rechtmatigheid criteria;
- Geconstateerde afwijkingen boven de verantwoordingsgrens.

De rechtmatigheidsverantwoording maakt deel uit van de jaarrekening. Wij geven als accountant een getrouwheidsoordeel af over de jaarrekening. Hierdoor blijft de aandacht voor en de controle op de rechtmatigheid minimaal op het huidige kwaliteitsniveau, ons afzonderlijk rechtmatigheidsoordeel komt echter te vervallen. Om op een effectieve en efficiënte wijze te kunnen controleren is dossiervorming van groot belang. Het college dient ter onderbouwing van haar oordeel een controledossier te vormen op de 3 aspecten van de rechtmatigheidsverantwoording;

- Voorwaardencriterium
- Begrotingscriterium
- M&O (Misbruik & Oneigenlijk gebruik) –criterium

Dit dossier dient door de gemeente expliciet aan ons als accountant gerapporteerd te worden, zodat wij dit als onafhankelijke derde zelfstandig kunnen reviewen en beoordelen. Daarbij geldt dat de gestelde eisen aan de dossiers hoger zijn dan wat u gewend was in voorgaande jaren als gevolg van nieuwe werkzaamheden voor de gemeente zoals het begrotingscriterium. Ook vragen wij uw aandacht om in het VIC plan duidelijk aan te geven hoe het M&O beleid wordt uitgevoerd. Overigens vragen wij uw aandacht voor een overkoepelend M&O-beleid om inzichtelijk te maken hoe het M&O criterium is ingebed in de diverse verordeningen en gemeentelijke regelgeving.

Overigens adviseren wij u om nader te onderzoeken in hoeverre de rechtmatigheid van uitbestede taken wordt vastgesteld, ten minste voor de uitbestede taken aan de Connectie.

De gemeente Rheden is de afgelopen periode bezig geweest met de verdere voorbereidingen op de rechtmatigheidsverantwoording. Het normenkader 2023 is reeds vastgesteld. De financiële verordening (ex artikel 212), de controleverordening (ex artikel 213) en het controleprotocol 2023 zullen op korte termijn ter vaststelling worden aangeboden aan de raad. Vanuit de VIC is voorgesorteerd op de aanstaande rechtmatigheidsverantwoording en het uitvoeren van de interne controleonderzoeken is reeds onderhanden, waarvan de afwikkeling over de resterende periode gepland staat in de eerste maanden van 2024.

2. Overige bevindingen en aandachtspunten

2.2 Bedrijfsprocessen

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

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

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

In de tabel rechts is een totaal overzicht opgenomen van de detailbevindingen. De bevindingen en onze aanbevelingen worden in bijlage 1 van deze management letter nader toegelicht.

	aandachtspunten
Aantal nieuwe aanbevelingen	***0***
Aantal aanbevelingen uit voorgaande jaren	17
Waarvan opgelost in 2023	1
Resterende aanbevelingen	**16**

#	Proces	Bevinding
2021	Aanbestedingen	Startformulier niet gehanteerd
2021	Betalingen	Zelfstandig verrichten van betalingen door de Burgemeester
2020	Sociaal Domein	Signaleringslijsten onvoldoende gecontroleerd
2020	Sociaal Domein	Bevoegdheden per functionaris onlogisch
2020	Inkopen	Bij het autoriseren van inkoopfacturen wordt de prijs en prestatie onvoldoende onderbouwd
2020	Inkopen	Geen zicht op naleving aanbestedingsrichtlijn
2020	Leges	Geen zichtbare toets op heffingsgrondslag bij leges voor omgevingsvergunningen
2020	Subsidieverstrekkingen	Onvoldoende structuur en documentatie bij subsidieverstrekkingen en –vaststellingen
2020	Administratie & verslaglegging	Onvoldoende controle op verwerking van begrotingswijzigingen
2020	Treasury	Onduidelijke afspraken over treasurybeheer
2020	Treasury	Het treasurystatuut is verouderd
2019	Sociaal Domein	Geen functiescheiding bij aanmaken en muteren van stamgegevens crediteuren
2019	Sociaal Domein	Onvoldoende documentatie en collegiale toetsing in dossiers
2018	Administratie & Verslaglegging	Onvoldoende functiescheiding tussen maken, verwerken en controleren van memoriaalboekingen
2018	Subsidiebaten	Geen geformaliseerde procedure voor het aanvragen, registreren en monitoren van subsidiebaten en de daarbij horende verplichtingen.
2016	Grondexploitatie	Geen zichtbare interne beheersing bij actualisaties grondexploitaties

2. Interne beheersing

2.3 Frauderisicoanalyse en frauderisico's

Fraude- en corruptierisico's

Sinds 2022 zijn de onderwerpen fraude en continuïteit opgenomen in de controleverklaring. In de verklaring is uiteengezet hoe de accountant bij de controleaanpak inspeelt op risico's ten aanzien van fraude en continuïteit en worden de uitgevoerde werkzaamheden toegelicht. Als aanvulling kan de accountant ook de uitkomsten van deze werkzaamheden of belangrijke waarnemingen met betrekking tot het onderwerp toelichten. De beide secties worden in alle controleverklaringen (verplicht) opgenomen; ook in situaties waar geen sprake is van ernstige continuïteitsonzekerheid of spraakmakende fraudecasuïstiek.

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 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 frauderisicoanalyse laten opstellen door een externe partij. Actualisering van deze frauderisico-analyse heeft echter tot op heden nog niet plaatsgevonden. U geeft aan dit voor de 1e helft van 2024 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.

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. We hebben vastgesteld dat binnen uw gemeente facturen door twee verschillende functionarissen (een prestatie akkoord verklaarder en een budgethouder) worden gecontroleerd. Wel is de documentatie ter onderbouwing van de prijs en prestatielevering een aandachtspunt om te voorkomen dat facturen mogelijk worden goedgekeurd waar geen prestatie voor uw gemeente tegenover staat, zie hiertoe de detailbevinding in bijlage 1.

2. Overige bevindingen en aandachtspunten

2.3 Frauderisicoanalyse en frauderisico's

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

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

Frauderisicoanalyse (extern)

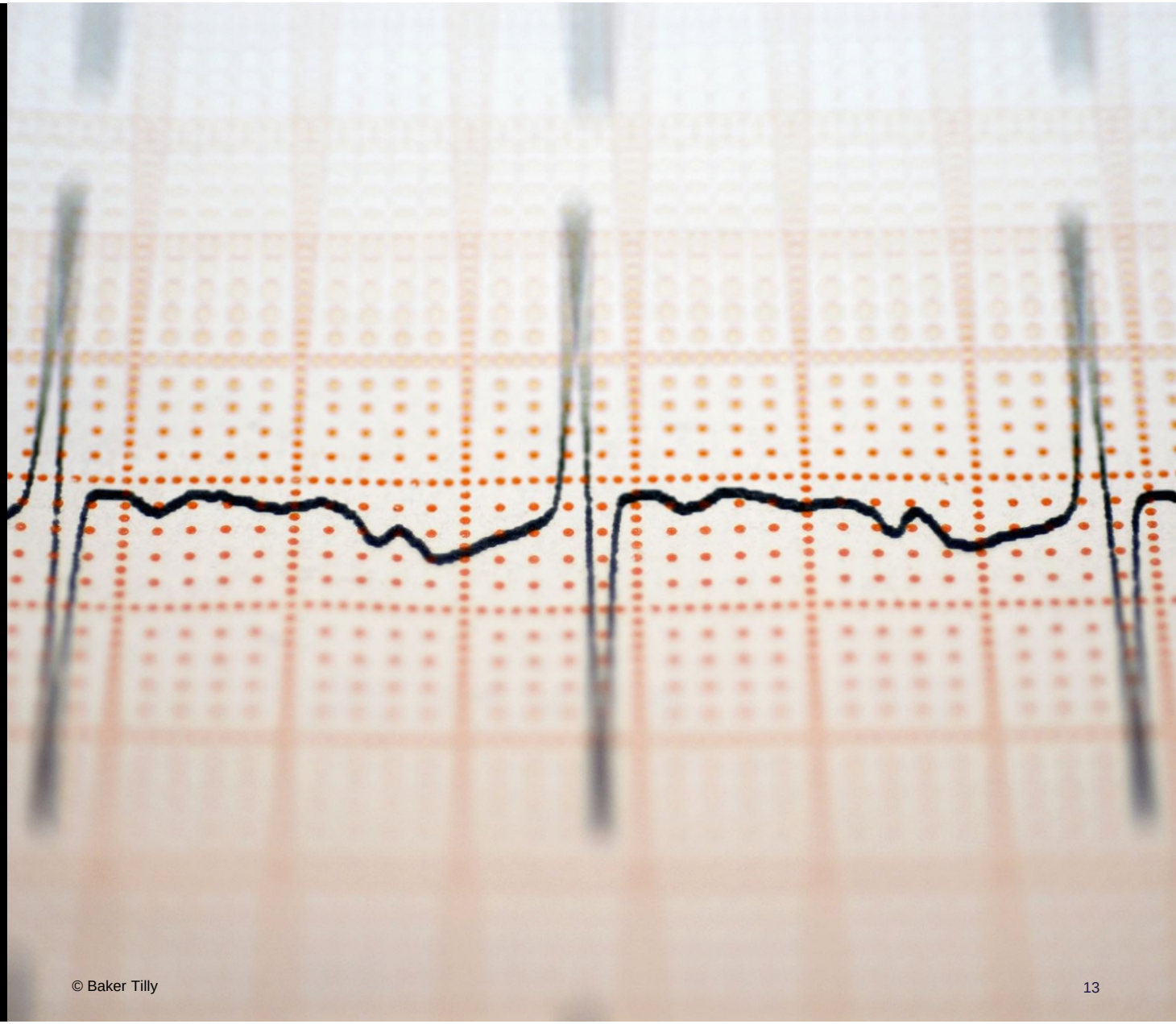
Het onderwerp fraude wordt door ons al accountant ook meegenomen in onze risico inschatting bij de jaarrekeningcontrole. Wij zullen dan ook in het accountantsverslag en de controleverklaring een passage opnemen over de geconstateerde frauderisico's en de door ons uitgevoerde werkzaamheden ten aanzien van deze risico's.

De belangrijkste onderkende risico's als gevolg van fraude 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;
- Het risico dat handmatige betalingen uitgevoerd worden aan niet-rechthebbenden;
- Risico dat het management van de gemeente de procesafspraken doorbreekt, hetgeen een standaard risico is vanuit onze beroepsregels en ziet met name toe op schattingsposten.
- Corruptierisico ten aanzien van de Europese aanbestedingsrichtlijnen met het risico op belangenverstrengeling en kickbacks.

De passages in relatie tot bovenstaande fraude-risico's die wij voornemens zijn op te nemen in de controleverklaring stemmen wij met u af en zullen wij bij de bespreking van het accountantsverslag met u doornemen.

Bevindingen IT-beheersing



© Baker Tilly

3. Bevindingen IT-beheersing

3.1 Algemeen

IT General Controls
Veel handelingen die binnen organisaties plaatsvinden, worden geregistreerd door middel van automatisering. Daarbij zijn diverse interne beheersingsmaatregelen steeds vaker geautomatiseerd in softwarepakketten. Wij onderzoeken daarom de beheersing van uw IT omgeving en rapporteren daarover in deze management letter.

Op basis van de door ons uitgevoerde werkzaamheden d.d. 02-11-2023 hebben wij onze inschatting van de kwaliteit van uw IT systeem en/of applicaties opgenomen. Hierbij hebben wij de volgende onderverdeling gemaakt om de kwaliteit weer te geven:

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

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

Categorie	Onderwerp
	Toegangsbeveiliging Bij het toetsen van 'toegangsbeveiliging' wordt onderzocht of de inrichting van de IT-omgeving de authenticiteit van de gebruiker van een gebruikersaccount borgt. Vervolgens onderzoeken wij de mogelijkheden voor het 'steunen' op autorisaties en de processen rondom het verstrekken, muteren en ontnemen van autorisaties binnen de omgeving. Wanneer de randvoorwaarden hiervoor voldoende aanwezig zijn, kunnen wij in de controle gebruik maken van ingerichte functiescheiding in het systeem. Een adequate inrichting kan preventief risico's voor uw organisaties beperken en tegelijkertijd efficiency voordelen opleveren in de controle. In paragraaf 3.2 is dit uitgewerkt.
	Wijzigingsbeheer (Change management) Bij het toetsen van 'wijzigingsbeheer' wordt vastgesteld dat wijzigingen in de applicatie op gestructureerde en gecontroleerde wijze worden doorgevoerd. Voor uw organisatie heeft wijzigingsbeheer het 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. De conclusies omtrent wijzigingsbeheer zijn uitgewerkt in paragraaf 3.3.
	Continuïteitsmaatregelen en beveiliging Onder de noemer continuïteit en beveiliging krijgen wij inzicht in uw beheersing van risico's gericht op continuïteit van uw bedrijfsvoering. Hierbij kan discontinuïteit worden veroorzaakt door menselijk of technisch falen, maar ook door interne of externe kwaadwillenden. Voor continuïteit zijn met name het punt in de tijd aan tot waar u gegevens bij discontinuïteit kunt herstellen en de tijd die het kost om tot een normale bedrijfsvoering te komen bij discontinuïteit van belang. Hiernaast schatten wij uw beheersing van cyber risico's in. Zie verdere uitwerking in paragraaf 3.4.
	Adviespunten zonder directe impact Het is ons van belang om inzicht te krijgen in de verantwoordelijkheden die binnen de organisatie zijn ingericht – of met andere organisaties overeen zijn gekomen (uitbesteding) – ten aanzien van de beheersing van de IT omgeving. Hierbij kijken wij naar beleidsstukken ten aanzien van IT strategie, beveiliging en functiescheiding. Ook de interne beheersingsmaatregelen die al dan niet zijn ingericht binnen de IT omgevingen zijn onderdeel van onze scope. Indien maatregelen periodiek worden uitgevoerd kunnen wij hier gebruik van maken in de jaarrekeningcontrole. Deze adviespunten hebben niet een directe impact op onze controlewerkzaamheden, maar zijn wel wenselijk. In paragraaf 3.5 is dit nader uitgewerkt.

3. Bevindingen IT-beheersing

3.2 Toegangsbeveiliging en wijzigingsbeheer netwerk (active directory)

De conclusies die wij op basis van onze werkzaamheden trekken over de algemene inrichting van het netwerk bij uw organisatie, delen wij op deze pagina met u.

Authenticatie
Door middel van authenticatie wordt geborgd dat een gebruiker zichzelf kan identificeren binnen een geautomatiseerde omgeving. Kort gezegd: de gebruiker toont aan dat hij/zij inlogt met een eigen persoonsgebonden account en daarmee is wie hij/zij claimt te zijn. Wij scharen onder dit onderwerp m.n. de wachtwoordvereisten.

Autorisatie
Op het gebied van autorisatie zijn verschillende vormen van diepgang te definiëren. Wat wij onderzoeken en aan u rapporteren als het gaat om de randvoorwaarden rondom autorisatie, zijn de rechten die de mogelijkheid bieden om autorisatie-structuren te wijzigen en of deze rechten belegd zijn bij functionarissen met een onafhankelijke positie ten opzichte van de jaarrekening. Dit geldt voor zowel voor rechten op applicatie- als databaseniveau voor applicaties in scope van onze controle. Daarnaast is een effectieve vaste werkwijze voor het toekennen van rechten noodzakelijk om gedurende een periode te kunnen steunen op het feit dat rechten adequaat beperkt zijn.

Wijzigingsbeheer (Change management)
Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat het proces voor wijzigingen een proces doorloopt, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden.

Authenticatie	Autorisatie	Wijzigings-beheer	Omgeving
Netwerk 		N.v.t.	**Authenticatie** De ingestelde wachtwoordeisen van het netwerk zijn van onvoldoende niveau om op de authenticatie van gebruikers te kunnen steunen. Wachtwoordrestricties binnen het netwerk wijken af van het eigen beleid. Het wachtwoordbeleid schrijft een minimale lengte van 12 voor, terwijl dit is ingesteld op 8. Daarnaast is het aantal foutieve inlogpogingen niet ingesteld, terwijl het beleid 10 pogingen voorschrijft. Tevens hebben wij beperkingen geconstateerd ten aanzien van de periodieke controle op het wachtwoordbeleid, wachtwoordinstellingen en actieve gebruikers. **Autorisatie** 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 het eigen beleid heeft plaatsgevonden, maar slechts eenmalig per jaareinde. Wij achten dit voldoende gezien de impact op de jaarrekening. **Wijzigingsbeheer** In relatie tot de jaarrekeningcontrole is wijzigingsbeheer omtrent de Windows Active Directory minder relevant, en hebben wij hiervoor geen werkzaamheden uitgevoerd. Wel hebben wij aandacht voor patch management in het kader van mogelijke cyber security risico's.

3. Bevindingen IT-beheersing

3.2 Toegangsbeveiliging en wijzigingsbeheer Unit4 Financials

De conclusies die wij op basis van onze werkzaamheden trekken over de algemene inrichting van de applicatie iFinanciën bij uw organisatie, delen wij op deze pagina met u.

Authenticatie
Door middel van authenticatie wordt geborgd dat een gebruiker zichzelf kan identificeren binnen een geautomatiseerde omgeving. Kort gezegd: de gebruiker toont aan dat hij/zij inlogt met een eigen persoonsgebonden account en daarmee is wie hij/zij claimt te zijn. Wij scharen onder dit onderwerp m.n. de wachtwoordvereisten.

Autorisatie
Op het gebied van autorisatie zijn verschillende vormen van diepgang te definiëren. Wat wij onderzoeken en aan u rapporteren als het gaat om de randvoorwaarden rondom autorisatie, zijn de rechten die de mogelijkheid bieden om autorisatie-structuren te wijzigen en of deze rechten belegd zijn bij functionarissen met een onafhankelijke positie ten opzichte van de jaarrekening. Dit geldt voor zowel voor rechten op applicatie- als databaseniveau voor applicaties in scope van onze controle. Daarnaast is een effectieve vaste werkwijze voor het toekennen van rechten noodzakelijk om gedurende een periode te kunnen steunen op het feit dat rechten adequaat beperkt zijn.

Wijzigingsbeheer (Change management)
Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat het proces voor wijzigingen een proces doorloopt, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden.

Authenticatie	Autorisatie	Wijzigings-beheer	Omgeving
Unit4 Financials 			**Authenticatie** 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 is 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 het wachtwoordbeleid. **Autorisatie** Er is sprake van een autorisatieprocedure en deze dient jaarlijks te worden gereviewd. Deze heeft echter niet tijdig plaatsgevonden. Er zijn verder geen uitzonderingen vastgesteld in het aanmaken van gebruikersaccounts. De controle op indiensttredingen, uitdiensttredingen en functiewijzigingen zijn niet conform de autorisatieprocedure doorlopen, doordat deze slechts eenmalig heeft plaatsgevonden per jaareinde. Voor accounts met hoge rechten is deze controle wel uitgevoerd conform beleid. De hoge rechten (rechten om gebruikers(rechten) te muteren) in de applicatie zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole, en zijn niet betrokken bij processen die relevant zijn voor de jaarrekening. Hoge rechten worden enkel toegekend volgens de opgestelde procedure. **Wijzigingsbeheer** 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 de controle in Q1 en Q2 niet tijdig zijn uitgevoerd. Daarnaast is in de Q1 controle een item uit 2021 opgenomen in de steekproef. Verder is er sprake van een gescheiden test- en productie omgeving.

3. Bevindingen IT-beheersing

3.3 Wijzigingsbeheer – Civision Samenlevingszaken

Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat het proces voor wijzigingen een proces doorloopt, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden.

Wij hebben in de tabel aangegeven wat wij verwachten per fase en wat wij hebben geconstateerd tijdens onze controle (deels op basis van interview) en of dit overeen komt met de verwachting.

Proces	Onze bevindingen
Risico inschatting	Wij hebben vernomen dat de risico-inschatting voor Civision Samenlevingszaken niet wordt vastgelegd. Wij adviseren u om deze werkstap te documenteren.
Opstellen testplan en aanpak	Wij hebben vernomen dat er voor Civision Samenlevingszaken nog geen gebruik wordt gemaakt van een testplan voor het uitvoeren van testwerkzaamheden. Wel is er sprake van een vaste werkwijze voor het doorvoeren van wijzigingen. Deze werkwijze is niet vastgelegd in een procedure. Wij adviseren u om vooraf een testplan op te stellen voor het uitvoeren van de testwerkzaamheden.
Testen en documenteren	Wij hebben vernomen dat er omtrent Civision Samenlevingszaken testwerkzaamheden worden uitgevoerd. Deze testwerkzaamheden (controles op functionaliteiten) worden niet gedocumenteerd. Wij adviseren u om de testwerkzaamheden vast te leggen in een testplan.
Gebruikers acceptatie	Wij hebben vernomen dat het testen voor Civision Samenlevingszaken in de huidige situatie met name plaatsvindt door een technisch applicatiebeheerder. Hierbij wordt in mindere mate de gebruikersorganisatie betrokken. Wij adviseren 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. Hierdoor is het akkoord vanuit de gebruikersorganisatie voldoende zichtbaar.

3. Bevindingen IT-beheersing

3.4 Continuïteitsmaatregelen en beveiliging

De weergave op deze sheet volgt uit de gesprekken en interviews die wij hebben uitgevoerd bij u op locatie. Het is een momentopname.

Continuïteitsmaatregelen

Recovery Point objective (RPO): De RPO is het punt in de tijd tot waar men minimaal de gegevens moet kunnen herstellen. Het is dus de acceptabele hoeveelheid aan dataverlies uitgedrukt in tijd.

Back-ups: 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 Time Objective (RTO): Een RTO is de tijd waarna een proces/middel na een onderbreking moet teruggebracht zijn op een aanvaardbaar niveau, om een onacceptabele impact op de organisatie te vermijden.

Vervolg RTO

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.

Beveiliging

Beveiliging

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

Vervolg Beveiliging

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 access: 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.

Preventie: De Connectie heeft op het Windows domein een virusscanner en firewall actief van Safepoint. De firewall stuurt ook actief pushberichten nar de beheerders als zich ongebruikelijk verkeer vertoont.

Monitoring: Cybersecurity wordt actief gemonitord door de firewall en opvolging te geven aan de meldingen van de IBD. Beheerders krijgen notificaties om bij calamiteiten actie te ondernemen. Periodiek worden er kwetsbaarheidsscans (door De Connectie) en pentesten (door externe partij) uitgevoerd. Hier wordt eventueel opvolging aan gegeven.

3. Bevindingen IT-beheersing

3.5 Adviespunten zonder directe impact

De weergave op deze sheet volgt uit de gesprekken en interviews die wij hebben uitgevoerd bij u op locatie. Het is een momentopname.

Beleid en Plannen

Beleid
Gemeente Rheden heeft een informatie-beveiligingsbeleid voor 2022-2024. Voor IT beheersing is het beleid van de Connectie van toepassing. Binnen de Connectie zijn processen in kader van IT beheersing beschreven. Deze beleidsstukken zijn recent en hierin worden relevante processen beschreven. Wij adviseren de naleving van IT beheersing te monitoren door middel van periodieke interne controles. De gemeente Rheden blijft eindverantwoordelijk.

Verantwoordelijkheden en regiefunctie
De gemeente heeft het beheer van IT-infrastructuur (maar ook technisch beheer van applicaties) belegd bij de Connectie. Daarom is het is voor gemeente Rheden belangrijk om regie te houden op de uitbestede diensten. Wij hebben begrepen dat er sprake is van een Service Level Agreement (SLA) en dat maandelijks een service level rapportage (SLR) wordt uitgebracht. Tevens rapporteert de Connectie jaarlijks op basis van een ISAE rapport. Hierin zijn het voorgaande jaar bevindingen geconstateerd. Wij adviseren u om dit rapport te analyseren en na te gaan in hoeverre deze bevindingen impact hebben op uw organisatie.

Uitvoering

Beheersing van incidenten
Om de performance van uw IT systemen en eventueel de performance van uw IT dienstverlener te monitoren, is registratie van de incidenten en problemen van belang. Hierdoor verkrijgt u inzicht in de performance van uw systemen, maar ook van uw IT organisatie en kunt u waar nodig uw beleidsplan corrigeren.

Incidenten en problemen worden op basis van een adequate procedure en middels de applicatie Topdesk geïdentificeerd, geregistreerd en opgevolgd.

Uitvoering beheersingsmaatregelen IT
Op verschillende vlakken worden (nog) geen toetsbare beheersingsmaatregelen uitgevoerd binnen uw organisatie. Denk aan:

- Procedure voor wijzigingsbeheer t.b.v. de gebruikersorganisatie/applicaties (zie ook punt ‘Wijzigingsbeheer’ Civision Samenlevings-zaken);
- Periodieke controle op inrichting van rechten in het systeem conform beleid (middels functie-autorisatie matrix);
- Monitoring van de diensten van de Connectie.

Deze procedures en daaruit volgende controlemaatregelen zorgen ervoor dat uw organisatie grip houdt op de IT-omgeving en faciliteren dat de randvoorwaarden, die de effectiviteit van ingerichte beheersings-maatregelen beïnvloeden, van voldoende niveau zijn.

Wij raden aan om bovenstaande procedures in te richten en (toetsbaar) periodiek te beheersen in de organisatie.

Bijlage 1: detailbevindingen



© Baker Tilly

Bijlage 1: Detailbevindingen interne beheersing

Uitleg opbouw management letter

In deze bijlage zijn de detailbevindingen opgenomen. Per bladzijde van deze bijlage is een bevinding opgenomen met daarbij het risico en een aanbeveling. Bij elke bevinding staat het boekjaar van de eerste vermelding aangegeven samen met de gradatie van de constatering. Bij de impact staat de mate van belangrijkheid en urgentie (hoog, gemiddeld, laag).

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.	*Risico* Hierbij geven wij aan wat de risico's zijn van de bevinding en wat de gevolgen voor uw gemeente kunnen zijn.	*Aanbeveling* Hier geven wij u Aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.	*Gevolgen controle* Hier geven wij aan wat de gevolgen zijn van de bevinding in relatie tot de verdere werkzaamheden voor de jaarrekeningcontrole.	*Impact* Urgentie en belang van de bevinding in het kader van de jaarrekening-controle en strekking van de verklaring

Bijlage 1:

Detailbevindingen interne beheersing - Follow-up overige bevindingen voorgaande jaren (1/3)

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 in alle gevallen separaat in dit hoofdstuk.

Het symbool geeft de status van de constatering aan.

- ✓ Opgelost
- ◑ Actie ondernomen, maar nog niet afgerond
- ✗ Geen actie ondernomen

Jaar	Proces	Bevinding	Ontwikkelingen	Status 2023
2021	Aanbestedingen	Startformulier niet gehanteerd	Geen wijzigingen.	✗
2021	Betalingen	Zelfstandig verrichten van betalingen door de Burgemeester	Geen wijzigingen.	✗
2020	Sociaal Domein	Signaleringslijsten onvoldoende gecontroleerd	Geen wijzigingen.	✗
2020	Sociaal Domein	Hoge wachttijden en hoge werkdruk die kunnen leiden tot ongewenste situaties	U geeft aan dat dit niet bij Jeugd speelt en dat de wachtlijst WMO is weggewerkt door inzet van het kenniscentrum WMO.	✓
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 rolinvulling van de teamleider in het proces vorm te geven en te overwegen of het mandaat daarop aansluit.	✗
2020	Inkopen	Bij het autoriseren van inkoopfacturen wordt de prijs en prestatie onvoldoende onderbouwd	Geen wijzigingen.	✗
2020	Inkopen	Geen zicht op naleving aanbestedingsrichtlijn	Ten behoeve van de rechtmatigheidsverantwoording vragen wij u een spendanalyse over de periode 2020-2023 op te stellen en alle crediteuren > EUR 214k over de 4 jaren en crediteuren 2023 > EUR 53k te motiveren of is voldaan aan de aanbestedingsrichtlijnen.	◑

Bijlage 1:

Detailbevindingen interne beheersing - Follow-up overige bevindingen voorgaande jaren (2/3)

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 in alle gevallen separaat in dit hoofdstuk.

Het symbool geeft de status van de constatering aan.

- ✓ Opgelost
- ◑ Actie ondernomen, maar nog niet afgerond
- ✗ Geen actie ondernomen

Jaar	Proces	Bevinding	Ontwikkelingen	Status 2023
2020	Leges	Geen zichtbare toets op heffingsgrondslag bij leges voor omgevingsvergunningen	Geen wijzigingen. Wij bevelen aan om een bouwkostentoets te implementeren om de volledigheid van de opbrengsten uit omgevingsvergunningen te bewaken.	✗
2020	Subsidieverstrekkingen	Onvoldoende structuur en documentatie bij subsidieverstrekkingen en –vaststellingen	Geen wijzigingen. U geeft aan dit mee te nemen in de controleplanning voor 2024.	✗
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 vervat in een memo.	◑
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. Wij vragen uw aandacht voor het opstellen van liquiditeitsprognoses.	◑
2020	Treasury	Het treasurystatuut is verouderd	Geen wijzigingen.	✗
2019	Sociaal Domein	Onvoldoende documentatie en collegiale toetsing in dossiers	U geeft aan in ieder dossier een onderzoeksverslag te hebben toegevoegd. Op basis van gegevensgerichte werkzaamheden zullen wij dit vaststellen. Bij jeugd dient altijd een collegiale toets en een kwaliteitstoets plaats te vinden. Bij WMO vindt toetsing bij 'risico' dossiers plaats. Volgens de werkinstructies vinden ook steekproeven WMO plaats. Wij vragen uw aandacht voor het zichtbaar en herleidbaar maken van de collegiale toetsingen en de steekproefbepaling.	◑

Bijlage 1:

Detailbevindingen interne beheersing - Follow-up overige bevindingen voorgaande jaren (3/3)

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 in alle gevallen separaat in dit hoofdstuk.

Het symbool geeft de status van de constatering aan.

- Opgelost
- Actie ondernomen, maar nog niet afgerond
- Geen actie ondernomen

Jaar	Proces	Bevinding	Ontwikkelingen	Status 2023
2019	Sociaal Domein	Geen functiescheiding bij aanmaken en muteren van stamgegevens crediteuren	Geen wijzigingen tot op heden. U geeft aan dat functioneel beheer dit binnenkort oppakt.	⊗
2018	Administratie & Verslaglegging	Onvoldoende functiescheiding tussen maken, verwerken en controleren van memoriaalboekingen	Geen wijzigingen.	⊗
2018	Subsidiebaten	Geen geformaliseerde procedure voor het aanvragen, registreren en monitoren van subsidiebaten en de daarbij horende verplichtingen.	Een verslag van de evaluatie is in een 10-punten verbeterplan verwoord.	◑
2016	Grondexploitatie	Geen zichtbare interne beheersing bij actualisaties grondexploitaties	Geen wijzigingen.	⊗

Bijlage 2: actuele ontwikkelingen in het kader van onze natuurlijke adviesfunctie



© Baker Tilly

Bijlage 2: Actualiteiten

Aankomende wetswijzigingen in BBV en Bado

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

Aanpassing Bado

Mogelijk veranderen met ingang van boekjaar 2024 de goedkeuringstoleranties voor de jaarrekeningcontrole. Op dit moment wordt voor fouten uitgegaan van 1% van de totale lasten inclusief dotaties aan de reserves en voor onzekerheden 3%. Vanaf 2025 worden fouten en onzekerheden mogelijk samengevoegd en wordt de goedkeuringsgrens gesteld op 2% van de totale lasten (dus zonder toevoeging reserves).
De accountant hanteert volgende tabel t.a.v. het oordeel:

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

Deze wijziging kan een belangrijke impact hebben. Indien de uitkomsten van de jaarrekeningcontrole 2022 worden afgezet tegen de gewijzigde goedkeuringstolerantie dan ontstaat het volgende beeld:

	Getrouwheid 2021	Getrouwheid 2022
	Fouten en onzekerheden	Fouten en onzekerheden
Totaal	€ 2.643.620	€ 2.749.160
% omvangsbasis (excl. toev. reserves)	2,0%	1,9%
Oordeel accountant	**Goedkeurend**	**Goedkeurend**

Hoewel met de voorgenomen wijziging, de lat hoger komt te liggen, leidt dit voor uw gemeente niet tot een andersluidende verklaring.

Controleverklaring bij de jaarrekening

Het is in het publiek belang dat de jaarstukken altijd met inbegrip van de controleverklaring toegankelijk worden voor het maatschappelijk verkeer, zoals raadsleden, burgers en andere belanghebbenden. In het BBV is nu niet expliciet opgenomen dat deze verklaring onlosmakelijk deel uitmaakt van de jaarrekening en dat de definitieve jaarrekening en / of de jaarstukken noch de controleverklaring separaat gepubliceerd mogen worden. Hierdoor komt het voor dat jaarstukken van decentrale overheden worden gepubliceerd zonder de daarbij afgegeven controleverklaring.

Om dit te borgen heeft onze beroepsvereniging suggesties opgenomen ter aanpassing van artikel 24 lid 3 van het BBV, door daarin ‘overige gegevens’ toe te voegen waarin de controleverklaring wordt opgenomen. In 2022 heeft u de jaarstukken gepubliceerd zonder de controleverklaring.

Wij adviseren u om vooruitlopend op deze aanpassing deze werkwijze alvast toe te passen voor de jaarrekening 2023.

Bijlage 2: Actualiteiten

Aankomende wetswijzigingen in BBV en Bado

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

Uitbreiding inhoud jaarrekening

De voorgeschreven inhoud van de jaarrekening wordt uitgebreid met de rechtmatigheidsverantwoording. De jaarrekening dient te bestaan uit:

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

De volgende eisen worden gesteld aan de rechtmatigheidsverantwoording:

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

De commissie BBV stelt een modeltekst voor de rechtmatigheids-verantwoording op.

Notitie Overhead

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

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

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

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

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

Bijlage 2: Actualiteiten

Aankomende wetswijzigingen in BBV en Bado

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

Paragraaf Openbaarheid

Met ingang van boekjaar 2022 is een verplichte paragraaf toegevoegd aan het jaarverslag. Dit betreft de Paragraaf Openbaarheid, deze paragraaf geeft ten minste inzicht in:

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

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

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

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

Paragraaf Bedrijfsvoering

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

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

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

De paragraaf betreffende de bedrijfsvoering bevat ten minste:

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

Bijlage 3: actuele ontwikkelingen ten aanzien van IT



Bijlage 3: Actualiteiten IT

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

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

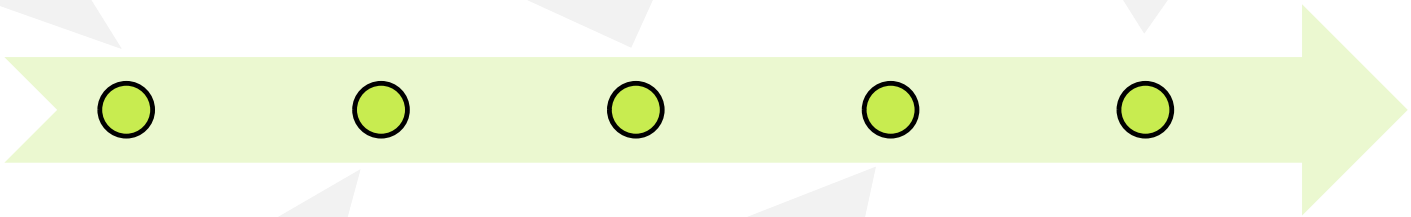
Van gemeentelijke colleges wordt verwacht dat de ambtelijke organisatie wordt gefaciliteerd bij de implementatie van deze richtlijnen en wetten. Doel van deze wetten en richtlijnen is dat uw gemeente weerbaarder wordt op het gebied van informatieveiligheid. Daarnaast zal de toezichthoudende rol van de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

Wij adviseren u in beeld te brengen in hoeverre deze ontwikkelingen voor uw ambtelijke organisatie zijn gefaciliteerd en of de gemeenteraad daarmee voldoende geëquipeerd is om zijn toezichthoudende rol te vervullen.

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

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

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



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

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

Bijlage 3: Actualiteiten IT

De implementatie van NIS2 vraagt aandacht

Onderwerp	
	**NIS2 als relevante ontwikkeling** De nieuwe Network and Information Systems Directive (NIS2-richtlijn) heeft belangrijke implicaties voor gemeenten als het gaat om toezicht op informatiebeveiliging. Lokale overheidsinstanties vallen nu ook onder de NIS2. Tegelijkertijd is de uitwerking van de NIS2 nog niet geheel helder. Denk hierbij aan vragen rondom de toepasselijkheid van de richtlijn op de Nederlandse gemeenten en wijze waarop dit zich verhoudt met bestaande structureren als de BIO (Baseline Informatiebeveiliging Overheid) en bijvoorbeeld ENSIA (de jaarlijks terugkerende audit ten behoeve van de collegeverklaring over Suwinet en DigiD).
	**Welke impact heeft de NIS2 op gemeenten in het algemeen?** Gezien het feit dat gemeenten nu al een zorgplicht (BIO), een meldplicht (Informatiebeveiligingsdienst, IBD) en toezicht (Eenduidige Normatiek Single Information Audit, ENSIA) hebben zal de impact van NIS2 voor gemeenten afhankelijk zijn van de mate waarin nu al gedocumenteerd voldaan wordt aan de BIO. De VNG zet zich onder andere in om gemeenten het zo makkelijk mogelijk te maken en heeft de impact van de wetgeving opgenomen in een overzichtelijke rapportage.
	**Wat kunt u doen?** Informatiebeveiliging is een proces wat continu aandacht blijft vragen. Daarom adviseren wij om door te blijven gaan met de cyclus van plannen, uitvoeren, controleren en bijstellen rondom de complete BIO. De BIO is een set van richtlijnen en best practices die specifiek is ontwikkeld voor de Nederlandse overheid. Door aandacht te geven aan de BIO kan in grote lijnen al een belangrijke stap gezet kan worden ter voorbereiding van de NIS2-richtlijn. Daarnaast kunnen wij uw organisatie adviseren in welke stappen u nog dient te ondernemen.

