

Board letter

Gemeente Zutphen
Boekjaar 2022

Aan de gemeenteraad
van de gemeente Zutphen
Postbus 41
7200 AA ZUTPHEN

ONDERWERP:
Board letter 2022

DATUM:
9 februari 2023

Geachte raadsleden,

Als onderdeel van de controle van de jaarrekening 2022 van gemeente Zutphen 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 gemeente 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 de organisatie, die bij een eventueel uitgebreid en hierop specifiek gericht onderzoek naar voren zouden kunnen komen. Zoals u zult begrijpen, zijn de management letter en de board 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. Wij geven in deze board letter in hoofdlijn aan op welke wijze verbeteringen van de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing kunnen worden gerealiseerd. De gedetailleerde aanbevelingen en oplossingsrichtingen zoals beschreven in de management letter bieden het college handvatten voor de uitwerking.

Deze board 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 het college en de 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

Director Audit (Extern accountant)

+31 (0)6 15 30 36 59

m.bekker@bakertilly.nl

Drs. W.W.L.A. Wentink RA

Senior manager Audit

+31 (0)6 15 38 17 56

w.wentink@bakertilly.nl

E.R.M. Friesen MSc RA

Junior manager Audit

+31 (0)6 21 92 16 95

e.friesen@bakertilly.nl

1. Bestuurlijke samenvatting	4
2. Overige bevindingen en aandachtspunten	6
3. Bevindingen IT-beheersing	17

Bestuurlijke samenvatting

1. Bestuurlijke samenvatting

Deze board letter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2022.



Wij zien dat er binnen de gemeente veel aandacht is voor interne beheersing. Nagenoeg alle in het verleden gerapporteerde bevindingen zijn opgepakt. Het blijkt wel moeilijk te zijn om ook daadwerkelijk tot een afronding te komen. In onze optiek ligt dat niet aan de effort die er wordt ingestoken vanuit het team Control. De daadkracht bij de vakafdelingen om daadwerkelijk stappen te zetten op het gebied van interne beheersing blijft achter op de inzet van team Control.

In zowel de financiële applicatie alsook de sociale zaken administratie zijn nog verbeteringen mogelijk c.q. noodzakelijk. 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 nog te realiseren verbeteringen voor beide applicaties zien toe op het aspect autorisatie (wie mag wat?).



Nederland heeft op dit moment te maken met enkele extreme omstandigheden: fors oplopende inflatie, de energiecrisis en de capaciteitsproblemen op de arbeidsmarkt. Deze omstandigheden leiden tot financiële risico's ook voor uw gemeente op langere termijn, maar zeker ook op korte termijn in relatie tot het opstellen van de jaarrekening 2022.



2. Overige bevindingen en aandachtspunten

2. Overige bevindingen en aandachtspunten

2.1 Algemeen

Doel en reikwijdte

Inleiding

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

Risicoanalyse

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

- Waardering van uw grondexploitatie;
- Waardering van uw onderhoudsvoorzieningen;
- Rechtmatigheid aanbestedingen;
- Prestatielevering inkopen;
- 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.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten. Deze punten zijn ongewijzigd ten opzichte van voorgaand jaar.

2. Overige bevindingen en aandachtspunten

2.2 Bedrijfsprocessen

Interne beheersing

Beeld interne beheersing

In onze vorige rapportages hebben we reeds gerapporteerd dat uw gemeente op het gebied van interne beheersing nog stappen moet zetten. Immers: om alle financiële uitdagingen voor uw gemeente in de komende tijd in goede banen te leiden worden hoge eisen aan het planning- en control instrumentarium, alsmede het interne beheersingssysteem gesteld. De aanstaande invoering van de rechtmatigheidsverantwoording door het college stelt hogere eisen aan het interne beheersingssysteem. De aanwezigheid van een adequaat intern (financieel) beheersingssysteem is daarbij een essentiële randvoorwaarde om te kunnen bijsturen en de betrouwbaarheid van financiële informatie en verslaglegging is van groot belang om dit tijdig en goed te kunnen doen.

Wij constateren dat de primaire functiescheiding, met uitzondering voor de processen omtrent memoriaalboekingen en omgevingsvergunningen, is ingeregeld. Evenwel zijn op onderdelen de interne beheersingsmaatregelen in het proces nog onvoldoende verankerd dan wel onvoldoende zichtbaar. 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. Ons advies om de zichtbaarheid van de interne beheersingsmaatregelen te vergroten om het college in staat te stellen bestaan en werking van de beheersingsmaatregelen te monitoren, blijft derhalve staan.

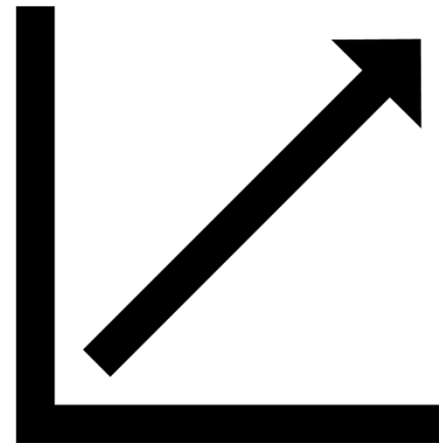
Er is binnen de gemeente Zutphen sprake van een vaste kern aan medewerkers op de afdeling Control die werken vanuit een gestructureerd intern controleplan. Wij zien dat er vanuit deze basis goede initiatieven genomen zijn om de interne beheersing van de gemeente Zutphen te verbeteren en voor te bereiden op de aanstaande rechtmatigheidsverantwoording. Evenwel is de realiteit ook dat in de afgelopen periode slechts één van de zeven bevindingen volledig is afgerond en ook werkt, maar dat de overige bevindingen nog onderhanden zijn en één bevinding nog niet is opgepakt. Illustratief is in onze optiek de implementatie van de nieuwe budgethoudersregeling en de vastlegging van de onderbouwing van de prestatielevering voor facturen > € 1.400. De afdeling control heeft hier afgelopen jaar veel tijd en energie in gestoken, waarmee in opzet een goed systeem om prestatielevering te borgen is gerealiseerd. Evenwel blijkt uit een themaonderzoek dat de interne beheersingsmaatregelen (vooralsnog) niet werken. Van de vijftien onderzochte facturen bleken er twee betaald te zijn zonder dat de prestatielevering überhaupt was onderbouwd en daarnaast bleek bij nog eens acht facturen de prijscomponent niet onderbouwd. Uiteindelijk is overigens alsnog wel vastgesteld dat prijs en hoeveelheid van alle facturen kon worden onderbouwd.

2. Overige bevindingen en aandachtspunten

2.2 Bedrijfsprocessen

Natuurlijk kunnen er technische en praktische aanloopproblemen zijn die ertoe leiden dat niet alles meteen gaat zoals het moet, maar feitelijk zouden dat soort problemen ook tijdig intern gecommuniceerd moeten worden. Uit ervaring weten wij dat om dit soort projecten te laten slagen voldoende capaciteit en zeker ook draagvlak in de organisatie essentieel is. Om voldoende draagvlak binnen de organisatie te creëren is het van belang dat het management en de overige leidinggevenden het belang van interne beheersing onderkennen en ook uitdragen binnen hun afdeling. Alleen op die manier wordt de ambitie van de gemeente Zutphen, zoals verwoord in het actieplan zoals dat inmiddels al weer drie jaar geleden is opgesteld, op het gebied van interne beheersing gerealiseerd.

Het is van belang dat de opgepakte bevindingen op korte termijn worden afgerond, alleen hiermee komt de interne beheersing van de diverse processen op het gewenste hogere niveau. Dit maakt de uitkomsten van deze processen betrouwbaarder, er is immers minder ruimte voor fouten. Daarnaast winnen ook de (financiële) rapportages aan waarde, wordt een basis gelegd voor een systeemgerichte interne controle en een fundament voor de rechtmatigheidsverantwoording door het college.



2. Overige bevindingen en aandachtspunten

2.2 Bedrijfsprocessen

Deze board letter bevat onze bevindingen die zijn gebaseerd op de onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2022. 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 diverse aanbevelingen benoemd ter verdere optimalisering van de bestaande administratieve organisatie en interne beheersing. In deze board letter geven wij u een schriftelijke update van onze bevindingen.

Hiernaast is een overzicht opgenomen van onze bevindingen met de status.

Legenda status:

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

In de tabel rechts is een totaal overzicht opgenomen van de het totaal aantal detailbevindingen.

	Aandachtspunten
Aantal nieuwe aanbevelingen	0
Aantal aanbevelingen uit voorgaande jaren	7
Waarvan opgelost in 2022	1
Resterende aanbevelingen uit voorgaande jaren	6
Waarvan reeds acties zijn ondernomen, maar nog niet zijn afgerond	5
Waarvan nog geen acties zijn ondernomen	1
Aantal openstaande aanbevelingen	6

Nr.	Proces	Bevinding/Aandachtspunt	Status	Impact
2019.01	Administratie en verslaglegging	Memoriaalboekingen	●	Hoog, want frauderisico
2019.02	GREX	Vastleggingen IB	●	Hoog, want frauderisico
2019.03	Omgevingsvergunningen	Functiescheiding	●	Gemiddeld
2019.04	Omgevingsvergunningen	Invoer tarieven	●	Gemiddeld
2019.05	Inkopen	Aanbestedingen	●	Hoog, want corruptierisico
2019.06	Inkopen	Prestatielevering	●	Hoog, want frauderisico
2019.07	Subsidies	Inhoudelijke toets	●	Gemiddeld

2. Overige bevindingen en aandachtspunten

2.3 Status rechtmatigheidsverantwoording (1/3)

Stand van zaken in verband met invoering rechtmatigheidsverantwoording

Op 27 september jl. heeft de Eerste Kamer het wetsvoorstel inzake de invoering van de rechtmatigheidsverantwoording aangenomen. Dit betekent dat met ingang van het boekjaar 2023 de accountant uitsluitend nog een oordeel over de getrouwheid van de jaarrekening afgeeft. In de jaarrekening wordt door het college een nieuwe toelichting over rechtmatigheid opgenomen ('rechtmatigheidsverantwoording'). In deze rechtmatigheidsverantwoording verantwoordt het college zich over de al dan niet rechtmatige totstandkoming van de lasten, baten en balansmutaties. De accountant stelt vervolgens de getrouwheid van deze verantwoording vast.

Op dit moment wordt gekeken naar de noodzakelijke aanpassingen van het Besluit Accountantscontrole Decentrale Overheden (BADO) en het Besluit Begroting en Verantwoording (BBV). Ook bij gemeenten moeten de noodzakelijke voorbereidingen worden getroffen. Naast de verplichting dat in de jaarstukken 2023 een rechtmatigheidsverantwoording moet worden opgenomen en het feit dat deze ook onderbouwd moet worden door (bijvoorbeeld) een verbijzonderde interne controle zijn ook een aantal operationele zaken die (in)geregeld moeten worden. Met ingang van boekjaar 2023 is het verplicht het normenkader voor de rechtmatigheid jaarlijks door de gemeenteraad te laten vaststellen. Tot en met boekjaar 2022 bestaat ook de mogelijkheid om het normenkader ter kennisgeving in de raad te brengen. Inhoudelijk krijgt de gemeenteraad ook een aanvullende verantwoordelijkheid, namelijk het bepalen van de verantwoordingsgrens die het college moet hanteren voor het opmaken van de rechtmatigheidsverantwoording:

- De gemeenteraad stelt een verantwoordingsgrens (tussen 0% en 3%) vast. Het college moet de financiële onrechtmatigheden boven dit bedrag rapporteren in de rechtmatigheidsverantwoording. Wij hebben het college geadviseerd deze verantwoordingsgrens in de financiële verordening (ex artikel 212) vast te leggen.
- De gemeenteraad kan kaders opstellen ten behoeve van de rapporteringsgrens waarboven de raad een nadere uiteenzetting verwacht in de paragraaf bedrijfsvoering. In lijn met artikel 212 lid 1 van de gemeentewet kan de gemeenteraad deze kaders vastleggen in de financiële verordening.

Naast de financiële verordening moeten ook de controleverordening (ex artikel 213) en het controleprotocol in lijn worden gebracht met de nieuwe wetgeving. De controleverordening en het controleprotocol gaan over hoe de kaders voor de toetsing van de jaarrekening inclusief de rechtmatigheidsverantwoording moet worden getoetst door de accountant. Deze moeten worden aangepast omdat het college rapporteert in de rechtmatigheidsverantwoording en de accountant de toetsing van de rechtmatigheid zal doen aan de hand van de rechtmatigheidsverantwoording van het college. De nauwkeurigheid en diepgang waarmee de accountantscontrole van de jaarrekening, met inbegrip van de rechtmatigheidsverantwoording, moet worden uitgevoerd, ofwel de materialiteit van maximaal 1%, wijzigt overigens vooralsnog niet door de invoering van de rechtmatigheidsverantwoording. De VNG heeft overigens onlangs modelverordeningen gepubliceerd waarin voorstaande zaken verwerkt zijn.

De gemeente Zutphen sorteert al voor op de aanstaande rechtmatigheidsverantwoording met het "Verbijzonderde interne controleplan 2021 en 2022 gemeente Zutphen" (hierna: VIC-plan). Daarnaast is "Plan van aanpak rechtmatigheidsverantwoording" opgesteld. In het VIC-plan wordt aangegeven dat het uitgangspunt is om zo veel mogelijk in het primaire proces te beleggen. Evenwel stellen wij vast dat op basis van onze bevindingen dit nog niet bij alle processen goed is ingericht. Hier lijken visie en praktijk dus nog uit elkaar te lopen.

2. Overige bevindingen en aandachtspunten

2.3 Status rechtmatigheidsverantwoording (2/3)

In het plan wordt verder (terecht) onderscheid gemaakt in systeemgerichte werkzaamheden (hebben de controles gewerkt?) en gegevensgerichte werkzaamheden (zijn de uitkomsten goed?). In het plan zelf wordt nog niet aangegeven voor welke aanpak wordt gekozen. Wij stemmen deze inschatting graag met het college af, om de werkzaamheden van de VIC en de werkzaamheden uit hoofde van de accountantscontrole zo goed mogelijk op elkaar te laten aansluiten.

Als vervolgstap is het belangrijk om in beeld te brengen of naar mening van het college de drie criteria voor de rechtmatigheidsverantwoording voldoende scherp zijn beschreven en geoperationaliseerd.

Voor het *begrotingscriterium* geldt dat het college en de gemeenteraad in de financiële verordening vastleggen op welke wijze zij omgaan met begrotingsoverschrijdingen. Uit de financiële verordening moet blijken hoe afwijkingen geïnterpreteerd worden in het kader van het uitoefenen van het budgetrecht door de gemeenteraad (stellige uitspraak Commissie BBV). De rechtmatigheidsverantwoording in de jaarrekening bevat belangrijke informatie voor het (politieke) verantwoordingsdebat van de gemeenteraad met het college.

Het *voorwaardencriterium* ziet toe op voorwaarden die gelden voor de uitvoering van de financiële beheershandelingen. Deze voorwaarden komen voort uit de relevante regelgeving en hebben betrekking op aspecten zoals: doelgroep, grondslag, administratieve bepalingen, normbedragen, bevoegdheden, bewijsstukken, recht, hoogte en duur voor zover deze relevant zijn voor de financiële rechtmatigheid. Het is van belang dat het college duidelijk maakt welke specifieke bepalingen van de regelgeving relevant zijn voor het financiële rechtmatigheidsbeheer en waar financiële consequenties uit kunnen voortkomen. Dit kan op verschillende wijzen worden vormgegeven:

- a) In het normenkader zelf, door per wet/regel/verordening aan te geven op welke artikelen getoetst worden en welke rechtmatigheidsaspecten daarbij relevant zijn (bijv. recht, hoogte, duur).
- b) In een apart toetsingskader of daaruit afgeleid control framework en afgeleid (interne)controleplan (zichtbaar gelinkt aan het normenkader).
- c) In de werkprogramma's waarbij per controleactiviteit wordt aangegeven welk artikel uit welke wet/regel/verordening wordt getoetst (zichtbaar gelinkt aan het normenkader).

Het laatste criterium heeft betrekking op *Misbruik en Oneigenlijk gebruik* (ook wel M&O). Het college is verantwoordelijk voor het inrichten van effectieve maatregelen ter voorkoming van misbruik en oneigenlijk gebruik van overheidsregels om overheidssubsidies en bijdragen te ontvangen dan wel een te laag bedrag aan heffingen aan de overheid te betalen. Deze maatregelen hangen veelal samen met de interne beheersing ter borging van het voorwaardencriterium. Het college gaat straks een uitspraak doen in hoeverre het M&O beleid feitelijk wordt nageleefd en of de getroffen maatregelen effectief werken. Wanneer het college concludeert dat het M&O-beleid (op onderdelen) niet actueel is en/of dat er geen M&O-beleid bestaat of het M&O-beleid feitelijk niet wordt nageleefd moet het college in de paragraaf Bedrijfsvoering melden.

2. Overige bevindingen en aandachtspunten

2.3 Status Rechtmatigheidsverantwoording (3/3)

Afwijkingen, voor zover zij niet het getrouwheidsaspect raken, moet het college in de rechtmatigheidsverantwoording rapporteren. Om aan deze verplichting te kunnen voldoen is van belang dat inzichtelijk is hoe het M&O criterium is ingebed in de diverse verordeningen en gemeentelijke regelgeving. Dit kan door een inventarisatie te doen en een nota M&O beleid op te stellen waarin de uitkomsten en afwegingen voor te treffen c.q. getroffen maatregelen in zijn opgenomen. Wij hebben het college geadviseerd daarin te voorzien.



2. Overige bevindingen en aandachtspunten

2.4 Belangrijke macro-economische ontwikkelingen

Energiecrisis en hoge inflatie

Nederland heeft op dit moment te maken met enkele extreme omstandigheden: enorm oplopende inflatie, de energiecrisis en de capaciteitsproblemen op de arbeidsmarkt. Deze omstandigheden leiden tot financiële risico's voor de gemeenten op langere termijn, maar zeker ook op korte termijn in relatie tot het opstellen van de jaarrekening 2022. Actualisatie van de grondexploitaties ligt gezien de genoemde omstandigheden voor de hand, maar ook op andere gebieden is het noodzakelijk om afdoende rekening te houden met de huidige ontwikkelingen. We vragen hier dan ook nadrukkelijk aandacht voor en verwachten van het college bij de jaarrekeningcontrole een expliciete analyse van:

- Waardering (langlopende) vorderingen. Ook partijen waar de gemeente leningen aan heeft verstrekt of vorderingen op heeft, kunnen zijn getroffen door de genoemde ontwikkelingen. Het is bij het opstellen van de jaarrekening dan ook noodzakelijk om een toereikende voorziening te treffen voor de eventuele oninbaarheid van deze vorderingen. In het bijzonder vragen we het college aandacht voor de vorderingen richting gesubsidieerde instellingen.
- Onderhoudsvoorzieningen. Gezien het feit dat bouwkosten fors toenemen, is de kans groot dat de beheerplannen waarop uw onderhoudsvoorziening is gebaseerd, niet meer actueel zijn. Het BBV heeft als een van de eisen dat er een actueel beheerplan aanwezig is. Het is dan ook noodzakelijk om de geschetste ontwikkelingen in financiële zin door te vertalen in de aanwezige beheerplannen. De gemeenteraad dient tijdig geïnformeerd te worden over eventuele benodigde bijstelling van de beheerplannen.
- Begrotings- en kredietrechtmatigheid. De genoemde ontwikkelingen leiden zowel op korte als langere termijn tot hogere lasten voor de gemeente. In het kader van de begrotingsrechtmatigheid is het van belang dat het college eventuele begrotingsafwijkingen als gevolg van deze hogere lasten tijdig meldt aan de gemeenteraad en hier begrotingsruimte voor vindt. Ook mogelijke kredietoverschrijdingen dienen tijdig in beeld te zijn en daar waar noodzakelijk tijdig met de gemeenteraad te worden gecommuniceerd.

Tot slot is het noodzakelijk om de toekomstige risico's, zoals bijvoorbeeld ten aanzien van de toenemende rente in beeld te hebben.

Er zijn momenteel naast het bovengenoemde diverse onzekere factoren die impact hebben op de ontwikkeling van grondexploitaties, denk hierbij onder andere aan:

- Een stijgende vraag naar woningen;
- Krapte aan (betaalbare) woningen op de markt;
- Krapte op de arbeidsmarkt bij bouwondernemingen;
- Verduurzamingsopgave.

Deze huidige ontwikkeling en de onzekerheid over de toekomstige ontwikkelingen betekent een grote schattingsonzekerheid op de verwachte realisatie van uw complexen. Wij hebben het college verzocht om na te gaan in welke mate bovenstaande elementen impact hebben op de gemeente Zutphen. Te meer omdat regionale verschillen en stijgingen van prijzen in specifieke kostensoorten fors van elkaar kunnen verschillen. Daarnaast dient bij een hoge mate van schattingsonzekerheid een adequate toelichting bij de verantwoording in de jaarrekening te worden opgenomen. Belangrijke elementen hierbij zijn:

- Het toelichten van de gehanteerde veronderstellingen; en
- Een toelichting (impact / scenario's) over de schattingsonzekerheid.

Wij hebben het college gevraagd na te gaan welke acties reeds zijn ondernomen en welke uitgangspunten gekozen zijn. Daarnaast gaan wij graag, net als voorgaande jaren, tijdig in overleg om de uitgevoerde analyses, de uitkomsten en de voorgestelde toelichtingen te bespreken.

Grondexploitaties

2. Overige bevindingen en aandachtspunten

2.5 Fraude en continuïteit

Fraude en continuïteit in de controleverklaring

Fraude

Als reactie op de rapporten van de Commissie Toezicht Accountancysector en Monitoring Commissie Accountancy heeft de NBA in de 2e helft van 2020 aangekondigd dat zij het beleid op de gebieden Fraude en Continuïteit meer concreet en meer zichtbaar tot uitdrukking wil brengen. Dit wordt gedaan met een aanvulling op Standaard 700.

De aanvulling in Standaard 700 komt er in hoofdlijnen op neer dat afzonderlijke secties voor de onderwerpen continuïteit en fraude in de controleverklaring worden opgenomen. Hierin wordt uiteengezet hoe de accountant bij de controle-aanpak 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.

Wij willen u erop wijzen dat wij vanaf dit boekjaar verplicht zijn om in onze controleverklaring specifiek te vermelden welke frauderisico's wij bij de controle van de jaarrekening van de gemeente Zutphen hebben geïdentificeerd en welke werkzaamheden wij ten aanzien van deze risico's hebben uitgevoerd.

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.

Frauderisicoanalyse (intern)

Op basis van onze uitgevoerde interim-controle stellen wij vast dat er binnen de gemeente aandacht is voor frauderisico's en de preventie daarvan. Wij constateren dat de gemeente een interne frauderisicoanalyse heeft opgesteld, actualisatie van deze frauderisicoanalyse heeft echter recent (sinds 2017) niet meer plaatsgevonden. Wij hebben het college geadviseerd deze frauderisicoanalyse op korte termijn te actualiseren en hierbij aandacht te besteden aan de risico inschatting (kans x impact) en binnen de gemeente Zutphen aanwezige interne beheersingsmaatregelen. Idealiter worden eerst de frauderisicofactoren ingeschat zonder rekening te houden met interne beheersing en vervolgens wordt aan de hand van de interne beheersing (en het werken daarvan) bekeken of sprake is van een daadwerkelijk frauderisico.

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

2. Overige bevindingen en aandachtspunten

2.5 Fraude en continuïteit

Fraudedriehoek

Wij raden het college aan bij het identificeren van de frauderisico's binnen uw gemeente specifiek gebruik te maken van de fraudedriehoek.

De fraudedriehoek kent de elementen 'Gelegenheid', 'Rationalisatie' en 'Druk' en is een goed hulpmiddel om frauderisicofactoren in beeld te krijgen en van daar uit te bepalen of deze frauderisicofactoren ook daadwerkelijk tot een frauderisico voor uw gemeente leiden. Belangrijk is om uw overwegingen/analyse goed te documenteren.

Wij hebben het college gevraagd als gevolg van de huidige economische ontwikkelingen (o.a. stijgende energieprijzen en indexatie) bij uw analyse nadrukkelijk aandacht te besteden aan de elementen druk en rationalisatie. Deze kunnen mogelijk leiden tot aanvullende frauderisico's. Wij hebben het college geadviseerd daarbij specifiek te kijken naar het (fraude)risico van onrechtmatige onttrekkingen van geld aan de gemeente.

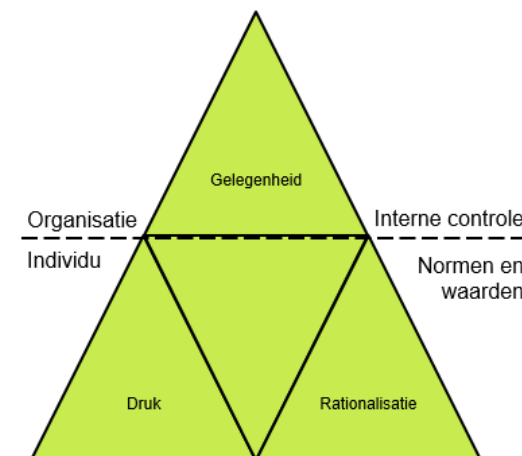
Frauderisicoanalyse vanuit de blik van de accountant

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

- Het risico dat het management maatregelen van interne beheersing doorbreekt;
- Het risico dat handmatige betalingen uitgevoerd worden aan niet-rechthebbenden;
- Het risico dat inkoopfacturen niet in overeenstemming zijn met de geleverde prestatie, omdat de prestatie niet is ontvangen.

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

Voor gemeenten geldt dat vanwege de onbegrensde leencapaciteit bij de BNG (en daardoor altijd aanwezige liquiditeit) per definitie geen onzekerheid kan bestaan over de continuïteitsveronderstelling. Evenwel stellen wij vast dat dat feit slechts zelden ook daadwerkelijk wordt benoemd in gemeentelijke jaarstukken. Dit zou bijvoorbeeld kunnen in de paragraaf weerstandsvermogen en risicobeheersing. Daarnaast is het ook raadzaam om de impliciete veronderstelling dat de gemeentelijke jaarstukken op basis van een continuïteitsveronderstelling zijn opgesteld, expliciet genoemd mogen worden in de grondslagen. Wij hebben gevraagd beide zaken mee te nemen bij het opstellen van de jaarstukken 2022. Naast feitelijke discontinuïteit is ook de mate waarin de gemeente zelfstandig en autonoom (financieel) beleid kan voeren een belangrijke veronderstelling. Derhalve is in onze optiek ook het risico op preventief provinciaal toezicht (artikel 12) een onderwerp wat daar in meegenomen moet worden.



Continuïteit

3. Bevindingen IT-beheersing

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 board letter.

Op basis van de door ons uitgevoerde werkzaamheden 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.

	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.
	Wijzigingsbeheer (Change management) Bij het doorvoeren van wijzigingen in software-omgevingen kunnen risico's ontstaan voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat er een vaste werkwijze is ingericht voor het doorvoeren van wijzigingen in de functionaliteiten van de applicatie. Daarnaast verwachten wij dat er gebruik wordt gemaakt van een test- en productie omgeving.
	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.
	Adviespunten zonder directe impact Gegeven de omvang van uw organisatie en de mate waarin de IT-beheersingsomgeving invloed heeft op de bedrijfsvoering binnen de organisatie, zijn wij met het college overeengekomen dat wij over de volgende onderwerpen wel analyseren in kader van onze controle, maar niet rapporteren: - IT-beleid; - Verantwoordelijkheden en regiefunctie; - Procedure beheersing van incidenten; - Uitvoering procedures beheersingsmaatregelen IT (reproduceerbare beheersing van o.a. toegangsbeveiliging en wijzigingsbeheer). Overigens hebben wij omtrent deze onderwerpen geen bevindingen geconstateerd die significante impact hebben voor de jaarrekeningcontrole.

3. Bevindingen IT-beheersing

3.2 Toegangsbeveiliging en wijzigingsbeheer

De conclusies die wij op basis van onze werkzaamheden trekken over de algemene inrichting van IT 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 autorisatiestructuren 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 database-niveau 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 			De ingestelde wachtwoordeisen van het netwerk zijn van voldoende niveau. De authenticiteit van gebruikers is hiermee geborgd. De hoge rechten in de Windows Active Directory zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole.
iFinanciën 			De ingestelde wachtwoordeisen van de applicatie zijn van voldoende niveau. De authenticiteit van gebruikers is hiermee geborgd. De hoge rechten voor iFinanciën voor het muteren van gebruikers zijn belegd bij onafhankelijke functionarissen. Er worden echter geen zichtbare periodieke controles uitgevoerd op gebruikers en gebruikersrechten in de applicatie door een onafhankelijke functionaris. Binnen de gemeente Zutphen wordt gebruik gemaakt van een SaaS-applicatie. Hierdoor is het proces omtrent wijzigingen belegd bij de leverancier van de applicatie, te weten Pink Roccade. Ons is niet gebleken dat er bijzonderheden hebben plaatsgevonden bij het doorvoeren van wijzigingen in het boekjaar.

3. Bevindingen IT-beheersing

3.2 Toegangsbeveiliging en wijzigingsbeheer

De conclusies die wij op basis van onze werkzaamheden trekken over de algemene inrichting van IT 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 autorisatiestructuren 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 database-niveau 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

Suites voor het Sociaal Domein



De ingestelde wachtwoordeisen van de applicatie zijn van voldoende niveau. De authenticiteit van gebruikers is hiermee geborgd.

De hoge rechten voor Suites voor het Sociaal Domein voor het muteren van gebruikers zijn niet belegd bij onafhankelijke functionarissen. Er worden geen zichtbare periodieke controles uitgevoerd op gebruikers en gebruikersrechten in de applicatie door een onafhankelijke functionaris.

Er wordt een risicoanalyse bij uw organisatie geïdentificeerd voor het doorvoeren van updates en fixes. Wijzigingen worden getest door gebruikers, dit wordt ook gedocumenteerd. Er wordt door de gebruikers akkoord gegeven voor het doorvoeren van een wijziging in de productieomgeving.

3. Bevindingen IT-beheersing

3.3 Continuïteitsmaatregelen en beveiliging

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

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: Back-ups worden dagelijks gemaakt en op meerdere locaties worden opgeslagen. Daarnaast vindt er monitoring plaats op de uitvoering van de back-ups door de afdeling ICT.

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: Recent heeft geen volledige recovery test plaatsgevonden op de gehele organisatie. Wel worden er periodiek recovery testen uitgevoerd op onderdelen van de organisatie. Hierdoor beschouwen wij het risico op dataverlies en downtime voor uw IT organisatie als laag. Wij raden wel aan om een volledige recovery test uit te voeren op de gehele organisatie.

Uitwijk: Er is een uitwijkmogelijkheid ingericht. Deze is echter niet getest in het boekjaar.

Beveiliging

Beveiliging

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

Fysieke beveiliging: De servers zijn ondergebracht in een serverruimte op locatie en op een secundaire locatie. De serverruimtes zijn voorzien van diverse beveiligingsmaatregelen ten aanzien van temperatuur, klimaat, noodstroomvoorzieningen en brandrisico's. Toegang is alleen mogelijk met een keycard.

Vervolg beveiliging

Remote access

Voor het extern inloggen wordt gebruik gemaakt van extra beveiligingsmaatregelen in de vorm van two-factor authenticatie. Hiermee wordt een extra authenticatie stap afgedwongen.

Preventie

Een firewall en virusscanner zijn aanwezig en wordt actief beheerd en gemonitord. Geen bevindingen.

Monitoring

Wij hebben vernomen dat er in 2022 een attack- en penetrationtest heeft plaatsgevonden.

Door het uitvoeren van een dergelijke test worden zwakheden in de IT-omgeving blootgelegd en kan actie ondernomen worden.

Een praktische oplossing kan zijn om elke paar jaar een diepgaande attack- en penetrationtest af te wisselen met een jaarlijkse (minder diepgaande) kwetsbaarheidsscan.

3. Bevindingen IT-beheersing

3.4 Adviespunten zonder directe impact

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

Beleid en Plannen

Beleid

Binnen uw organisatie is een uitgewerkt IT beleidsplan aanwezig, waarin de uitgangspunten voor IT beheer en ontwikkelingen zijn beschreven.

Deze beleidsstukken vormen de basis voor monitoring op basis van een plan-do-check-act cyclus toe te passen binnen uw organisatie.

Verantwoordelijkheden en regiefunctie

Wij verwachten dat binnen uw organisatie duidelijke afspraken zijn gemaakt ten aanzien van verantwoordelijkheden over uitvoering en strategie op het gebied van IT. Er is aangegeven dat dit het geval is. Uw organisatie maakt gebruik van een zelfstandige afdeling ICT. Daarnaast zijn er per applicatie personen aangesteld als verantwoordelijke.

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 wordt inzicht verkregen in de performance van de systemen, maar ook van de IT-organisatie en kan waar nodig het.

Er is aangegeven dat incidenten gemeld worden op verschillende manieren. Door de afdeling ICT wordt aan iedere melding een ticket aangemaakt in TopDesk. Indien mogelijk worden incidenten gelijk afgehandeld, anders wordt het belegd bij een specialist.

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');
- Periodieke controle op actieve gebruikers;
- Periodieke controle op inrichting van wachtwoordbeleid;
- Procedure voor het gestructureerd toekennen, wijzigen en ontnemen van rechten;
- Periodieke controle op inrichting van rechten in het systeem conform beleid (middels functie-autorisatie matrix).

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

Wij hebben het college geadviseerd om bovenstaande procedures in te richten en (toetsbaar) periodiek te beheersen in de organisatie.



KANTOORGEGEVENS

Baker Tilly (Netherlands) N.V.
Burgemeester Roelenweg 14-18
8021 EV Zwolle
Postbus 508
8000 AM Zwolle
+31 (0)38 425 86 00