



Aan de leden van de auditcommissie van
de gemeente Zuidplas
T.a.v. mevrouw M. Engelsman, Griffier
Postbus 100
2910 AC NIEUWERKERK AD IJSSEL

Onderwerp
Boardletter 2022

Behandeld door
M.F.B. Heuer MSc
088 288 0708

Datum
12 december 2022

Ons kenmerk
22127B14F0.02/CP

Geachte leden van de auditcommissie,

Wij hebben, conform onze opdrachtbevestiging d.d. 18 november 2022, als onderdeel van de controle van de jaarrekening 2022, de interim-controle voor de gemeente Zuidplas uitgevoerd. Deze controle is primair gericht op de analyse en evaluatie van de interne-beheersingsomgeving en de daarin opgenomen maatregelen van interne controle. In onze boardletter zijn onze bevindingen en aanbevelingen ter zake opgenomen. Tevens heeft deze controle als doelstelling om de aandachtspunten voor de jaarrekening 2022 te signaleren en onder uw aandacht te brengen. In onze managementletter die wij hebben uitgebracht aan het college van burgemeester en wethouders zijn onze bevindingen en aanbevelingen ter zake opgenomen. Een afschrift van de belangrijkste bevindingen ontvangt u als auditcommissie via deze boardletter.

Volledigheidshalve merken wij op dat onze analyse en evaluatie is uitgevoerd in het kader van de door u verstrekte opdracht tot controle van de jaarrekening. De geselecteerde werkzaamheden zijn afhankelijk van de door de accountant toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de jaarrekening een afwijking van materieel belang bevat als gevolg van fraude of fouten. Bij het maken van deze risico-inschattingen neemt de accountant de interne beheersing in aanmerking die relevant is voor het opmaken en het getrouwe beeld van de jaarrekening en de rechtmatige totstandkoming van de baten, lasten en balansmutaties, gericht op het opzetten van controlewerkzaamheden die passend zijn in de omstandigheden.

De risico-inschattingen hebben niet tot doel een oordeel tot uitdrukking te brengen over de effectiviteit van de interne beheersing, de opzet, het bestaan, de effectiviteit en de efficiency van de interne beheersing als geheel van uw organisatie, maar slechts die delen die ten grondslag liggen aan financiële mutaties in uw organisatie.

Wij merken op dat deze brief is opgesteld ten behoeve van de auditcommissie en gemeenteraad van de gemeente Zuidplas en niet zonder onze toestemming aan derden mag worden verstrekt.

Graag willen wij deze rapportage en de daarin opgenomen bevindingen en aanbevelingen nader met u bespreken tijdens de auditcommissie d.d. 23 januari 2023.

Hoogachtend,

Deloitte Accountants B.V.

drs. R.M.J. van Vugt RA

01 Management-samenvatting





Managementsamenvatting

1.1. Interne beheersing

In toenemende mate komen gemeenten voor uitdagingen te staan, die elkaar in een rap tempo opvolgen. Hierbij kunt u onder andere denken aan de opvangproblematiek, de woningbouwopgave, de klimaattransitie (verduurzaming), maar ook aan de toename van de wet- en regelgeving als gevolg van onder andere het sterk groeiende aantal SiSa-regelingen waar gemeenten verantwoording over moeten afleggen. Dit alles in een tijd waarin, als gevolg van de oorlog, de prijzen sterker stijgen en het tekort aan (bouw)materialen toeneemt, met als gevolg een sterk oplopende inflatie. Dit alles heeft uiteraard effect op het uitgavenniveau van de reguliere begroting. Mede als gevolg van deze elementen worden ook de prognoses van de woningbouwproductie onzekerder en neemt het risicoprofiel van de grondexploitatie of faciliterende projecten, mede door de stijgende rente, toe. Gelijktijdig is er sprake van een krapte op de arbeidsmarkt waardoor vacatures minder snel worden ingevuld en er mogelijk meer inhuurkrachten ingezet moeten worden.

Wij hebben bij de interim-controle de primaire bedrijfsprocessen in kaart gebracht die wij relevant achten voor de jaarrekeningcontrole. De bevindingen en onderwerpen zoals deze in de boardletter opgenomen zijn, dienen ter ondersteuning van het management bij zijn taken in het opzetten en verbeteren van de interne-beheersingsomgeving van de gemeente Zuidplas.

Wij hebben bij deze processen vastgesteld dat de randvoorwaardelijke interne-beheersingsmaatregelen, zoals bevoegdheden en functiescheiding, primair aanwezig zijn. Ten aanzien van meerdere processen hebben wij echter ook nieuwe tekortkomingen geconstateerd, welke nader toegelicht zijn in deze boardletter.

Onze belangrijkste bevindingen naar aanleiding van de interim-controle 2022 hebben betrekking op de processen inzake frauderisicomanagement en de IT-omgeving. Per proces hebben wij tevens aandacht besteed aan de huidige economische ontwikkelingen met betrekking tot de hoge inflatie.

Daarnaast hebben wij gekeken naar de impact die de personele wisselingen binnen de organisatie teweeg hebben gebracht. Wij constateren dat verschillende sleutelposities binnen de gemeente Zuidplas, mede als gevolg van de moeilijke c.q. veranderende omstandigheden op de arbeidsmarkt, tijdelijk zijn ingevuld. Hoewel uw organisatie voldoende inspanning levert om dit aan te pakken, is in onze optiek de continuïteit van uw beheersmaatregelen en beheersomgeving hierdoor kwetsbaar.

Dit is in onze optiek mede terug te zien in de beperkte voortgang c.q. opvolging van de aanbevelingen die wij in eerdere jaren hebben gedaan. Wij concluderen daarmee dat de positieve ontwikkeling ten aanzien van de kwaliteitsverbeteringen in de interne beheersing, op dit moment afvlakt. Wij gaan hierover dan ook graag met u in gesprek.

1.2 Inflatie, energietoeslag en opvang vluchtelingen

In het voorjaar van 2022 werd de wereld verrast door het conflict tussen Rusland en Oekraïne. De oorlog in Oekraïne heeft veel gevolgen, waaronder de (uitzonderlijk) hoge inflatie, stijgende energieprijzen en de toestroom van Oekraïense vluchtelingen. De rijksoverheid heeft verschillende steunmaatregelen in het leven geroepen, waarvoor gemeenten (deels) verantwoordelijk zijn. Dit betreft taken met een financiële impact op de jaarrekening 2022. Gemeenten zijn (deels) verantwoordelijk geworden voor de opvang van vluchtelingen uit Oekraïne en de uitkering van leefgeld. Deze aanvullende taken zetten extra druk op de ambtelijke organisatie, zowel qua werkdruk als op het gebied van financiële middelen. Wij hebben in het kader van onze interim-controle de, voor de jaarrekening relevante, processen beoordeeld. Wij vragen (blijvend) uw aandacht voor de tijdige signalering van de (zowel financiële als procesmatige) gevolgen van deze aanvullende taken.





Managementsamenvatting

1.3. Follow-up aanbevelingen

Onze boardletter 2021 en eerdere rapportages bevatten diverse aanbevelingen. Tijdens de interim-controle 2022 is de follow-up van deze adviezen inzichtelijk gemaakt. Samengevat geeft dit het volgende beeld:

Follow-up	Bevinding eerdere rapportages
Niet opgelost	4
Gedeeltelijk opgelost	5
Opgelost	1
Totaal	10

Wij merken op dat een grote hoeveelheid aan ambities en verbeterinitiatieven ertoe leidt dat de organisatie niet volledig is toegekomen aan een adequate opvolging van al onze bevindingen. Dit wordt mede veroorzaakt door het feit dat de organisatie te maken heeft met relatief veel personele wisselingen, waardoor een structurele borging en opvolging van onze bevindingen niet altijd gerealiseerd kan worden.

1.4. Aandachtspunten voor de jaarrekeningcontrole

Voor het opstellen van de jaarrekening 2022 en onze controle daarop identificeren wij op basis van de interim-controle en de relevante ontwikkelingen de volgende belangrijke aandachtspunten:

- Het uitvoeren van aanvullende (verbijzonderde) interne controles.
- Het beschikbaar hebben van een toereikende onderbouwing voor de waardering van het onderhanden werk (voorraad bouwgronden in exploitatie). Specifieke aandachtspunten hierbij zijn een actuele onderbouwing van de voor 2023 e.v. verwachte kosten en opbrengstenindexatie, alsmede de effecten van de stikstofuitspraak door de Raad van State en de, mede hierdoor, potentiële vertragingen in de uitvoering van de grondexploitaties.

- Het aantal regelingen dat uw gemeente moet verantwoorden in de SiSa-bijlage, alsmede het aantal overige inkomende subsidiebatens, neemt in 2022 verder toe. Het is belangrijk de interne controle op de getrouwe verantwoording in de SiSa-bijlage, overige inkomende subsidies en de rechtmatigheid van de bestedingen ervan tijdig uit te voeren en adequaat te documenteren. Tevens is het van belang dat de rollen in het verantwoordingsproces helder benoemd zijn (inhoudelijk en financieel-technisch verantwoordelijk). Wij hebben met uw organisatie afspraken gemaakt over het verder optimaliseren van het verantwoordingsproces.
- Met ingang van 1 januari 2022 kunnen medewerkers op grond van de Cao gemeenten bovenwettelijke vakantie-uren opsparen, zonder dat deze vervallen. Hierdoor ontstaat de mogelijkheid dat medewerkers 'stuwmeren' van verlof opbouwen om bijvoorbeeld een sabbatical te nemen of vervroegd met pensioen te gaan. Voor deze verlofstuwmeren dient (mogelijk) een voorziening te worden gevormd, op het moment dat de lasten niet jaarlijks van een vergelijkbare volume zijn. Het is hierbij van belang, om ten aanzien van het opstellen van de jaarrekening 2022, inzichtelijk te maken in hoeverre medewerkers gebruikmaken van deze nieuwe regeling en wat de hiermee gemoeide financiële omvang is. Wij gaan hierover graag met u in gesprek.
- Het vast laten stellen van het normenkader 2022 ten behoeve van de accountantscontrole.

Wij zullen nog nadere afspraken met u maken over het uitvoeren van de werkzaamheden. Deze afspraken zullen gaan over het moment waarop de controles uitgevoerd worden en in hoeverre de gemeente de controles kan voorbereiden ten behoeve van de jaarrekeningcontrole.





Managementsamenvatting

2.1 Frauderisicomanagement

Fraude is en blijft op basis van de actualiteit een belangrijk thema. Wij informeren u daarom jaarlijks over uw aandacht voor het thema 'fraude', en over onze zienswijze en evaluatie daarbij.

De beoordeling door het college van burgemeester en wethouders van het risico van (o.a. materiële) fouten in de jaarrekening als gevolg van fraude of van een overtreding van de wet- en regelgeving

Als onderdeel van onze interim-controle vragen wij uw organisatie jaarlijks om inzicht te geven in de eigen inschatting van het risico dat de jaarrekening een materiële afwijking zou kunnen bevatten als gevolg van fraude of van het overtreden van wet- en regelgeving (corporate compliance), inclusief de aard, omvang en frequentie van deze inschattingen, het proces dat u daarbij hanteert, alsook de communicatie daarover met het personeel en met de gemeenteraad. Interne procedures en processen moeten periodiek worden geanalyseerd op de risico's van fraude en integriteit. Het uitvoeren van een frauderisicoanalyse speelt een cruciale rol bij het ontwikkelen en in stand houden van een effectieve interne beheersing. Dergelijke risicoanalyses maken inzichtelijk op welke plaatsen wellicht niet-integer gedrag kan plaatsvinden, en wat de kwetsbare functies, processen en activiteiten zijn. Bovendien dragen deze bij aan het risicobewustzijn en aan het vermogen om snel te reageren in het geval van signalen van fraude. U bent als college – tezamen met de gemeenteraad – primair verantwoordelijk voor het beoordelen van het risico van materiële fouten in de jaarrekening als gevolg van fraude en/of het overtreden van wet- en regelgeving.

Fraudesignalen

Van de accountant wordt op grond van de regels van de beroepsorganisatie NBA een professioneel-kritische houding verwacht ten aanzien van afwijkingen van materieel belang als gevolg van fraude. Ter invulling van deze professioneel-kritische houding zal de accountant een inschatting moeten maken van de frauderisico's, zich een beeld moeten vormen van de maatregelen van interne beheersing die de organisatie heeft getroffen om mogelijke fraudes van materieel belang te voorkomen, en moeten bezien of deze maatregelen effectief zijn.

Wanneer sprake is van een aanwijzing voor fraude, zal de accountant dit moeten communiceren met, afhankelijk van de aard van de fraude, de direct leidinggevende, het college en, in sommige gevallen (fraude in de top van de organisatie) en wanneer onvoldoende herstelwerkzaamheden worden ondernomen, de gemeenteraad.

Om invulling te geven aan de eerdergenoemde verplichting hebben wij een fraudediscussie gevoerd binnen het controleteam, en hebben wij de proceseigenaren van de voor de accountantscontrole relevante processen tijdens de interim-controle gesproken over frauderisico's. Hierbij hebben wij de nadruk gelegd op de eventuele mogelijkheden van materiële onjuistheden als gevolg van fraude in relatie tot de jaarstukken, en op de preventieve maatregelen daarbij. Daarnaast hebben wij conform onze beroepsregels zelfstandig werkzaamheden uitgevoerd die erop waren gericht om het risico van het 'omzeilen' van de interne-beheersingsmaatregelen door het management te detecteren. Hoewel wij, zoals hiervoor beschreven, een kritische houding hebben ten opzichte van risico's van fraude, merken wij op dat onze controle niet specifiek gericht is op het ontdekken van fraude.

Frauderisico's bij de jaarrekeningcontrole

De primaire verantwoordelijkheid voor het voorkomen en detecteren van fraude berust bij de gemeenteraad en het college van de gemeente. Deze verantwoordelijkheid omvat ook het onderhouden van een zodanige interne beheersing als nodig is om het opmaken van de jaarrekening mogelijk te maken zonder dat deze afwijkingen van materieel belang bevat als gevolg van fraude of fouten. Onze controle is opgezet om een redelijke mate van zekerheid te verkrijgen dat de jaarrekening als geheel geen afwijkingen van materieel belang bevat als gevolg van fraude of fouten, maar richt zich niet specifiek op het ontdekken van fraude. Op basis van de door ons uitgevoerde interim-werkzaamheden hebben wij geen aanpassingen aangebracht in onze initiële frauderisicoanalyse die is opgenomen in onze controleaanpak.





Managementsamenvatting

Ons advies

Wij hebben, als onderdeel van onze controle, de meest recente frauderisicoanalyse beoordeeld. Over de wijze waarop de frauderisicoanalyse tot stand komt, zijn wij positief. Wij hebben hier eerder over gerapporteerd in onze boardletter 2021. Wel zien wij nog enkele punten waarmee u de frauderisicoanalyse kunt versterken, mede met het oog op de implementatie van de rechtmatigheidsverantwoording en de verdere professionalisering van de verbijzonderde interne-controle-functie. Wij noemen in dit kader:

- Uw interne frauderisicoanalyse is gericht op de geïdentificeerde risico's op basis van de eigen kernprocessen. Naast de focus op de risico's die worden geïdentificeerd via het perspectief en de processen van iedere afdeling, adviseren wij u om het gehele fraudelandschap bij de analyse te betrekken, om zo de kans te verkleinen dat er risico's worden gemist of weggelaten. Hierbij kunnen bijvoorbeeld aspecten worden meegenomen als: de waarschijnlijkheid van omkoping en corruptie, mogelijkheden van fraude(sturing) in de financiële overzichten, en het risico op het doorbreken van de interne beheersing door het management.
- In de frauderisicoanalyse ontbreekt nog een beschrijving van de restrisico's en van de wijze waarop hiermee wordt omgegaan (bijv. accepteren/mitigeren/ vermijden). Het verdient aanbeveling om in te gaan op de risicobereidheid ten aanzien van fraude- en compliancerisico's.
- Het is belangrijk dat de organisatie, mede in relatie tot de aankomende rechtmatigheidsverantwoording, het bestaan en de werking van de (huidige en aanvullende) beheersingsmaatregelen zoals genoemd in de frauderisicoanalyse ook gaat toetsen. Dit element is reeds opgenomen in het interne-controleplan. Hierin ontbreekt echter nog de concrete opzet van de interne-beheersingsmaatregelen die getoetst zullen worden.

2.2 Materiele vaste activa -investeringen – afschrijvingstermijnen

De gemeenteraad van de gemeente Zuidplas heeft in de financiële verordening een afschrijvingsbeleid vastgesteld waarin bandbreedtes zijn opgenomen voor de economische levensduur per activacategorie. Deze bandbreedtes zijn de spelregels waaraan de organisatie zich dient te houden bij het activeren van investeringen en de bepaling van de hierbij behorende afschrijvingstermijn.

Bij het uitvoeren van onze interim-controle hebben wij bij de door ons verrichte lijncontrole, waarmee wij het bestaan van de beheersmaatregelen beoordelen, vastgesteld dat een andere afschrijvingstermijn is gehanteerd dan vanuit de financiële verordening staat voorgeschreven. Ten aanzien van deze afwijking van het afschrijvingsbeleid heeft geen formele besluitvorming plaatsgevonden door de gemeenteraad over de afwijking die hierdoor plaatsvindt van de financiële verordening. Wel had de organisatie in het meerjarig investeringsplan de verkorte afschrijvingstermijn weergegeven achter het desbetreffende krediet. Dit is echter gebeurd zonder nadere toelichting of beschrijving dat het hier ging om een alternatieve afschrijvingstermijn of dat er sprake zou zijn van een afwijking van de financiële verordening.

In formele zin is er naar onze mening hierbij sprake van onrechtmatige afschrijvingslasten als gevolg van het onjuist toepassen van de door de Raad vastgestelde termijnen.

Wij verzoeken uw organisatie om voorafgaand aan de jaarrekeningcontrole 2022 de afwijkingen van de voorgeschreven afschrijvingstermijnen inzichtelijk te maken en om in deze specifieke situaties de afwijkende afschrijvingstermijnen expliciet door de Raad te laten autoriseren. Daarnaast adviseren wij de gemeente Zuidplas om de interne beheersing van het proces op een passende wijze aan te passen, waardoor geborgd wordt dat afwijkingen door de juiste gremia gefiatteerd worden alvorens deze in de financiële systemen doorgevoerd worden.

Wij hebben vernomen dat de hierboven beschreven wijzigingen ten aanzien van de afschrijvingstermijnen zijn meegenomen in de actualisatie van de financiële verordening die is vastgesteld door het college en vanaf boekjaar 2023 in werking zou moeten treden.





Managementsamenvatting

2.3 Materiele vaste activa - kredietbewaking

De investeringsbegroting wordt organisatiebreed opgesteld, waarbij de verschillende individuele investeringen worden samengebracht tot een totaal. De kredietbewaking wordt momenteel decentraal belegd bij de individuele budgethouder, waarbij iedere budgethouder verantwoordelijk is voor zijn eigen krediet. Een aantal keer per jaar worden er gesprekken gevoerd met de budgethouders. Er worden hiervan echter geen zichtbare notulen vastgelegd. Daarnaast hebben wij tijdens onze interim-controle vastgesteld dat er geen sprake is van een centrale vorm van kredietbewaking. Uw gemeente beschikt daarentegen echter wel over de technische ondersteuning (middels uw activamodule) om deze kredietbewaking op een centraal niveau in te richten.

Het ontbreken van deze combinatie van kredietbeheersing, leidt tot het risico dat uw organisatie onvoldoende tijdig zicht heeft in eventuele kredietoverschrijdingen (of onderschrijdingen). Wij bevelen dan ook aan om, naast de decentrale kredietbewaking, de kredietbewaking centraal in te regelen binnen uw organisatie.

2.4 Prestatielevering inhuur personeel

Tijdens onze interim-controle hebben wij met uw organisatie gesproken over de wijze waarop de verwerking van facturen van inhuurkrachten plaatsvindt. Wij hebben vernomen dat voor de inhuur van medewerkers een 'broker' (Yacht) is ingeschakeld, waarlangs een deel van de beheersmaatregelen met betrekking tot de in rekening gebrachte kosten verloopt.

Tijdens de gesprekken die zijn gevoerd, hebben wij begrepen dat de inhuurkrachten hun uren per week declareren via de applicatie MijnYacht. De inhousemedewerker van Yacht verwerkt de ingediende declaraties eens per 4 weken, waarna deze worden doorgezonden naar de kredietbeheerder en vervolgens worden uitbetaald. De toetsing van de prestatielevering is primair belegd bij de betreffende Clustermanager onder wiens leiding de inhuurkracht werkzaam is. Deze controlerende functie gaat echter uit van een negatieve controle, waarbij er geen expliciet akkoord gegeven dient te worden op de daadwerkelijk gerealiseerde urenbesteding. In plaats daarvan wordt slechts een melding ontvangen wanneer er uren zijn gedeclareerd. Indien hierop niet tijdig actie ondernomen wordt, gaat de clustermanager impliciet akkoord met hetgeen wordt gedeclareerd.

Hierdoor ontbreekt een zichtbare inhoudelijke (afgedwongen) toets ten aanzien van de levering van de onderliggende prestatie (vermeld dient te worden dat de factuur van Yacht nog het reguliere autorisatieproces doorloopt, zodra deze is ontvangen).

Daarnaast hebben wij tijdens de gesprekken vernomen dat er dit boekjaar kosten gedeclareerd werden door een inhuurkracht die geen werkzaamheden verricht had voor de gemeente, waarbij de Clustermanager hiervoor (stilzwijgend) akkoord had gegeven. Door een kritische blik van de kredietbeheerder is deze transactie (terecht) voorkomen.

Op basis van het bovenstaande bevelen wij aan om in overleg te treden met Yacht om een (afgedwongen) systeemtechnische beheersmaatregel te implementeren, waarbij een inhoudelijke toets uitgevoerd wordt ten aanzien van de prestatielevering.

2.5 Personeel - zichtbare controle personeelsmutaties

Uw gemeente maakt al meerdere jaren gebruik van de diensten van ADP voor de verloning van uw medewerkers. Voordat mutaties doorgevoerd worden (door ADP) in de salarisadministratie, worden deze door uw salarisadministratie getoetst. Na verwerking door ADP ontvangt uw organisatie een zogenoemd 'mutatierapport' waarop de daadwerkelijk doorgevoerde wijzigingen zichtbaar zijn. Op basis van de door ons uitgevoerde werkzaamheden tijdens onze interim-controle, hebben wij vastgesteld dat er geen zichtbare controle wordt uitgevoerd op het mutatierapport en daardoor niet op de definitief doorgevoerde mutaties. Hierdoor ontstaat het risico dat de personeelslasten onjuist geregistreerd en/of uitbetaald worden. Wij bevelen dan ook aan om een zichtbare controlemaatregel te implementeren aan de hand van het mutatierapport.





Managementsamenvatting

2.6 IT-audit

De toepassing van informatietechnologie (IT) en de IT-governance (veiligheid, cybersecurity etc.) spelen een steeds grotere rol. IT is een van de kernelementen van onze controleaanpak. Niet alleen ter waarborging van de betrouwbaarheid en continuïteit van de transactieverwerking, maar vooral ook ten behoeve van de efficiency en het genereren van relevante en tijdige informatievoorziening op grond waarvan u als raad kunt sturen respectievelijk bijsturen.

Proces- en beleidsmatig

In het kader van de interim-controle hebben wij specifiek aandacht besteed aan de algehele interne-beheersingsmaatregelen die uw organisatie procesmatig heeft ingericht binnen de verschillende applicaties, alsmede de algemene gebruiksomgeving. Hierbij hebben wij specifiek gekeken naar de onderstaande zaken:

- Wijzigingsbeheer: beheersingsmaatregelen die verzekeren dat enkel geautoriseerde wijzigingen worden doorgevoerd en dat deze wijzigingen op een adequate wijze zijn getest voordat deze naar productie worden gebracht.
- Logische toegang: beheersingsmaatregelen die verzekeren dat enkel geautoriseerde personen toegang hebben tot de IT-systemen en enkel voor zover dat benodigd is uit hoofde van de functie.

Uw gemeente heeft voor de bovenstaande zaken de afgelopen jaren beleid, alsmede een procesgang opgesteld. Wij stellen dat deze elementen essentieel zijn voor een solide IT-basis van de interne beheersing. Wel moeten wij constateren dat de opvolging van adviezen uit eerdere jaren nog niet volledig is, als gevolg van personele wisselingen en onderbezetting van uw IT-afdeling. Tevens merken wij dat uw IT-afdeling c.q. afdeling Informatievoorziening, als gevolg van de plaats binnen uw organisatiestructuur, onvoldoende in de positie wordt gebracht om optimaal haar bijdrage te kunnen leveren aan procesverbeteringen/het realiseren van de doelstellingen van de organisatie. Hierbij valt te denken aan:

- Het niet tijdig signaleren van ontwikkelingen op het gebied van vakspecifieke regelgeving die ingebed dienen te worden binnen de verschillende applicaties.

- Wijzigingen die doorgevoerd moeten worden in de IT-omgeving.
- Het onvoldoende tijdig kunnen signaleren van procesoptimalisatie mogelijkheden.

Wat betreft het bovenstaande gaan wij graag met uw organisatie in gesprek.

Database controls

De verschillende applicaties binnen uw organisatie worden gehost op de databases bij de gemeente Gouda. Wij vernamen dat voor een enkele applicatie de functioneel beheerder vanuit de gemeente Zuidplas eveneens rechten heeft om direct op de database in te loggen en waar nodig aanpassingen te doen. Deze rechten zijn verstrekt om rapportages direct vanuit de database te kunnen genereren, om enkele grootschalige invoeracties (zoals wijziging van tarieven) direct op de database te kunnen uitvoeren, alsmede om foutmeldingen c.q. problemen (bijvoorbeeld uit conversies) vanuit het systeem op te lossen. Wij vernamen dat hiervoor vanuit de proceseigenaar een akkoord is gegeven.

Wij adviseren uw organisatie echter wel logging en monitoring uit te voeren op de mutaties die direct in de database worden uitgevoerd. Hiermee kunnen eventuele foutieve mutaties in de database worden gesignaleerd en gecorrigeerd.

Third-party memorandum

Uw organisatie heeft het systeembeheer c.q. de hosting van de geautomatiseerde omgeving grotendeels uitbesteed aan de gemeente Gouda. In voorgaande jaren hebben wij reeds gerapporteerd dat de gemeente Zuidplas onvoldoende inzicht heeft in de algehele beheersing bij deze serviceprovider. U heeft afspraken gemaakt met de gemeente Gouda in de vorm van een herzien Service Level Agreement, waarbij u tevens met de gemeente Gouda bent overeengekomen dat zij haar stelsel van internal control door een onafhankelijke auditor laat toetsen. In 2019 is als gevolg hiervan een nulmeting (geen assurance) uitgevoerd. In 2021 is een uitgebreidere IT-audit uitgevoerd door een onafhankelijke auditor, waarbij getoetst is in hoeverre de interne-beheersingsmaatregelen overeenkomstig de Baseline Informatiebeveiliging Overheid (BIO) opgezet zijn en of deze in de praktijk bestaan.





Managementsamenvatting

In dit boekjaar wordt wederom een IT-audit uitgevoerd om na te gaan in hoeverre de bevindingen uit voorgaande jaren zijn opgevolgd en of de beheersomgeving daarmee voldoende klaar is, zodat tevens de werking van de beheersmaatregelen zullen worden getoetst zullen. Het toetsen van de effectieve werking van de interne-beheersingsmaatregelen is essentieel om voldoende zekerheid te verkrijgen over het feit of de opgezette interne-beheersingsmaatregelen van ICT Gouwe-IJssel (ten behoeve van de gemeente Zuidplas) in de praktijk ook daadwerkelijk werken en of deze de verschillende risico's in voldoende mate mitigeren. Wij adviseren dit aspect mee te nemen in de overleggen met ICT Gouwe-IJssel.

Autorisaties

Binnen de applicaties van de gemeente zijn standaard gebruikersrollen ingericht. Wij hebben vastgesteld dat de gemeente voor een aantal processen een formeel vastgestelde en geautoriseerde autorisatiematrix heeft opgesteld, waarin gewenste rollen en rechten in opzet zijn omschreven. Echter, het inzicht ontbreekt wat betreft welke kritische proceshandelingen niet in een hand mogen liggen (om bijvoorbeeld controletechnische functiescheidingen conflicten te voorkomen). Beleidsmatig heeft uw organisatie het proces omtrent het beheer van de rollen en autorisaties binnen de verschillende applicaties dusdanig ingericht dat eens per halfjaar een review wordt uitgevoerd, zodat deze overeen blijven komen met de intenties van het management en de minimaal benodigde functiescheiding niet doorbroken is.

Wij hebben vastgesteld dat deze reviews niet structureel hebben plaatsgevonden op de daadwerkelijke inrichting van de autorisaties binnen de verschillende applicaties. Hierdoor ontstaat het risico dat de functiescheiding binnen de applicaties op een onvoldoende adequate wijze is ingericht en dat zodoende ongeautoriseerd mutaties zouden kunnen worden doorgevoerd.

Tevens hebben wij vastgesteld dat, indien medewerkers binnen de organisatie van functie veranderen en zodoende ook andere rechten zouden moeten hebben in de verschillende applicaties, de afdeling ICT niet structureel wordt betrokken bij het wijzigen van de rechten. Hierdoor ontstaat het risico dat de functiescheiding binnen de applicaties op een onvoldoende adequate wijze is ingericht en dat zodoende ongeautoriseerd mutaties zouden kunnen worden doorgevoerd.

Wij adviseren u nadrukkelijk om de periodieke review ten aanzien van de gebruikersrechten en autorisaties binnen de verschillende applicaties uit te voeren en deze controle expliciet vast te leggen. Daarnaast dient gevolg gegeven te worden aan de ontwikkeling van de autorisatiematrixen, alsmede aan de formalisering daarvan voor de belangrijkste applicaties binnen de gemeente.

Wijzigingsbeheer

Wijzigingen in uw IT-omgeving worden binnen uw organisatie op verschillende wijzen doorgevoerd. Afhankelijk van de applicatie bestaan er formele of informele procedures voor het doorvoeren van wijzigingen. Wijzigingen van beperkte omvang worden direct in de productieomgeving doorgevoerd. Wijzigingen van grotere omvang, zoals grote patches, worden in een separate testomgeving doorgevoerd en getest in samenwerking met de systeembeheerders van de hostingorganisatie (Gouda). De keuze of een wijziging doorgevoerd wordt in de live-omgeving of productieomgeving, vindt plaats op basis van de professionele oordeelsvorming van de functioneel beheerder en wordt niet altijd gedocumenteerd. De wijzigingen worden door de functioneel beheerders getest en beoordeeld. Hierbij wordt bij sommige applicaties gebruikgemaakt van een standaard testformulier. Bij deze beoordeling wordt de clustermanager betrokken, die feitelijk proces- en applicatie-eigenaar is. De applicatie-eigenaar is degene die uiteindelijk eindverantwoordelijk is voor het proces en de applicatie, en zou daarom ook moeten besluiten of wijzigingen, gegeven eventuele resterende bevindingen uit testwerkzaamheden, in productie genomen zouden moeten worden. Binnen dit proces dient tevens de controletechnische functiescheiding geborgd te blijven, waarbij het klaarzetten, testen en in productie nemen van een wijziging in voldoende mate geborgd is. Wij hebben vernomen dat, mede als gevolg van de organisatorische plaats binnen de organisatie, niet altijd uw centrale IT-afdeling c.q. de afdeling Informatievoorziening, wordt betrokken bij dergelijke wijzigingen/projecten.





Managementsamenvatting

Wij adviseren u dan ook om een zogenoemde Change Advisory Board te implementeren, bestaande uit de functioneel beheerders, de clustermanager en eventuele overige gebruikers vanuit de vakafdelingen. Dit orgaan kan bij grote aanpassingen in de IT-omgeving de beoogde effecten beoordelen en waar nodig verder adviseren. Daarnaast adviseren wij u om een formeel proces op te stellen omtrent het doorvoeren van grote wijzigingen in uw IT-omgeving. Tevens dienen richtlijnen opgesteld te worden om te bepalen welke typen wijzigingen direct doorgevoerd kunnen worden in de productieomgeving en welke eerst via een testomgeving dienen te verlopen. Deze richtlijnen dienen te worden opgesteld op basis van de door de gemeente opgestelde risicoanalyse.

3.1 Disclaimer en beperking in het gebruik

Volledigheidshalve merken wij op dat onze analyse en evaluatie is uitgevoerd in het kader van de door u verstrekte opdracht tot controle van de jaarrekening. De geselecteerde werkzaamheden zijn afhankelijk van de door de accountant toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de jaarrekening een afwijking van materieel belang bevat als gevolg van fraude of fouten. Bij het maken van deze risico-inschattingen neemt de accountant de interne beheersing in aanmerking die relevant is voor het opmaken van de jaarrekening en voor het getrouwe beeld daarvan, gericht op het opzetten van controlewerkzaamheden die passend zijn in de omstandigheden. Deze risico-inschattingen hebben echter niet tot doel een oordeel tot uitdrukking te brengen over de effectiviteit van de interne beheersing.

Hierdoor is onze analyse en evaluatie beperkter dan dat deze zou zijn geweest in het kader van een opdracht tot het geven van een oordeel omtrent de opzet, het bestaan, de effectiviteit en de efficiency van de interne beheersing als geheel en deze bestrijkt daarom niet noodzakelijkerwijze alle in de interne organisatie vervatte tekortkomingen.

Wij attenderen u erop dat deze brief is opgesteld ten behoeve van het management van de gemeente Zuidplas en daarom niet zonder onze toestemming aan derden mag worden verstrekt.





Onder Deloitte wordt verstaan één of meer van Deloitte Touche Tohmatsu Limited ("DTTL"), haar wereldwijde netwerk van member firms en aan hen verbonden entiteiten (tezamen, de "Deloitte organisatie"). DTTL (hierna ook te noemen "Deloitte Global") haar wereldwijde netwerk van member firms en aan hen verbonden entiteiten zijn juridisch gescheiden en onafhankelijke entiteiten, die elkaar niet kunnen verplichtingen of binden ten aanzien van derden. DTTL en iedere DTTL member firm en aan hen verbonden entiteit is aansprakelijk voor hun eigen handelen en nalaten, en niet voor het handelen of nalaten van een andere entiteit. DTTL verleent geen diensten aan cliënten. Raadpleeg www.deloitte.com/about voor meer informatie.

Deloitte levert toonaangevende audit- en assurance-, belasting- en juridische diensten, consulting, financial advisory, and risk advisory diensten aan bijna 90% van de Fortune Global 500® en duizenden particuliere bedrijven. Onze professionals leveren meetbare en blijvende resultaten die het vertrouwen van het publiek in kapitaalmarkten helpen versterken, klanten in staat stellen te transformeren en bloeien, en de weg wijzen naar een sterkere economie, een meer rechtvaardige samenleving en een duurzame wereld. Voortbouwend op zijn meer dan 175-jarige geschiedenis, omvat het bereik van Deloitte meer dan 150 landen en gebieden. Ontdek hoe de meer dan 345.000 mensen van Deloitte wereldwijd een impact maken die ertoe doet op www.deloitte.com.

Deze communicatie bevat louter algemene informatie en noch DTTL, noch haar wereldwijde netwerk van member firms of aan hen verbonden entiteiten verleent door middel van deze communicatie professioneel advies of diensten. Voordat u een beslissing neemt of actie onderneemt die van invloed kan zijn op uw financiën of uw bedrijf, dient u een gekwalificeerde professionele adviseur te raadplegen. Geen enkele entiteit in de Deloitte organisatie is verantwoordelijk voor enig verlies dat wordt geleden door een persoon die op deze communicatie vertrouwt.

© 2022. Neem voor informatie contact op met Deloitte Nederland.