

Managementletter

Gemeente Oss

Boekjaar 2023

Aan het college van burgemeester en
wethouders van de gemeente Oss
Postbus 5
5340 BA Oss

ONDERWERP:
Concept managementletter 2023

Geacht college,

Als onderdeel van de controle van de jaarrekening 2023 van gemeente Oss 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 onderneming 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 managementletter 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 managementletter 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 managementletter bieden u handvatten voor deze uitwerking. Wij hebben de concept managementletter toegelicht en besproken met de wethouder financiën en een afvaardiging van de ambtelijke organisatie.

Deze managementletter is door ons opgesteld voor uw informatie en mag niet zonder onze uitdrukkelijke toestemming geheel of gedeeltelijk aan derden ter beschikking worden gesteld.

Wij danken u en uw medewerkers voor de samenwerking en zijn graag bereid tot het verstrekken van nadere toelichting.

Met vriendelijke groet,
Baker Tilly (Netherlands) N.V.



drs. B. (Barry) Smeenk RA

Inhoudsopgave

CONTACT

drs. B. (Barry) Smeenck RA
Eindverantwoordelijk accountant
+ 31 (0)6 15 59 17 58
b.smeenck@bakertilly.nl

drs. R. (Rik) Opendorp RA
Partner
+ 31 (0)6 10 09 04 64
r.opendorp@bakertilly.nl

R. (Rianne) van Uden-Olders MSc RA
Senior Manager
+ 31 (0)6 55 22 02 48
r.vanuden@bakertilly.nl

1. Bestuurlijke samenvatting	4
2. Bevindingen en aandachtspunten	7
3. Bevindingen IT-beheersing	18
Bijlage 1: Detailbevindingen	26
Bijlage 2: Actuele ontwikkelingen	30
Bijlage 3: Actuele ontwikkelingen IT	35

Bestuurlijke samenvatting

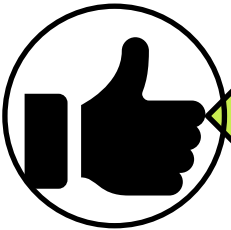
10/10/2023



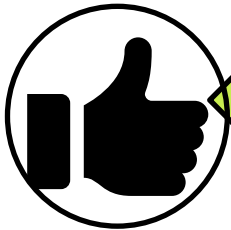
1. Bestuurlijke samenvatting



Deze managementletter bevat onze bevindingen die zijn gebaseerd op onze werkzaamheden in het kader van de jaarrekeningcontrole voor het jaar eindigend op 31 december 2023.



Uw interne beheersing is op orde. We hebben geen significante tekortkomingen in uw AO/IC geconstateerd. In deze managementletter geven we u een aantal aanbevelingen mee om de interne beheersing verder te optimaliseren. Wij constateren dat de managementletterpunten van voorgaand jaar opvolging hebben gehad.



In het kader van onze jaarrekeningcontrole hebben we de interne beheersing rondom uw IT onderzocht. Wij hebben in dat kader de netwerkomgeving onderzocht, de financiële applicatie K2F, Suites (uitkeringsadministratie) en Motion (salarisadministratie). Met betrekking tot de IT-beheersing constateren we dat onze aanbevelingen onderhanden zijn en ten opzichte van voorgaand jaar ook deels zijn opgevolgd.

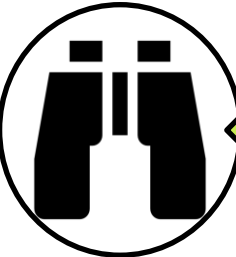


De onzekerheden vanuit macro-economisch perspectief blijft impact hebben op de lokale overheden en raakt ook de gemeente Oss. De hoge inflatie en energiecrisis hebben niet alleen impact gehad op de jaarrekening 2022, ook op de jaarrekening 2023 hebben deze elementen een belangrijke invloed op uw gemeente. In het verlengde van de inflatie en energiecrisis neemt de rente fors toe wat zal leiden tot uitdagingen om de ambitieuze investeringsagenda te kunnen realiseren.

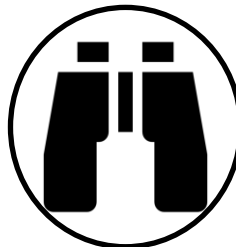
1. Bestuurlijke samenvatting



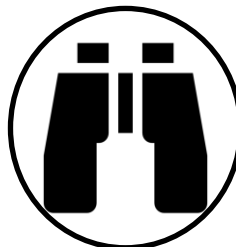
Onze samenwerking. De samenwerking met de gemeente Oss verloopt op een effectieve wijze. Naar aanleiding van de evaluatie van de controle over het boekjaar 2022 zijn op enkele aandachtspunten nadere afspraken gemaakt om de samenwerking nog soepeler te laten verlopen. Er is sprake van proactieve communicatie vanuit beide partijen en er zijn duidelijke afspraken welke worden nagekomen. Wel constateren we dat de doorlooptijd van de IT audit lang is doordat bepaalde stukken vanuit de gemeente Oss lang op zich laten wachten.



Vanaf 2023 dient het college van burgemeester en wethouders zelfstandig verantwoording af te leggen over de **rechtmatigheid**. Om tot een goede verantwoording te komen speelt de Verbijzonderde Interne Controle (VIC) een belangrijke rol. Op basis van de informatie welke wij van u hebben ontvangen is het controleplan dat de VIC in het systeem Checkpoint borgt (tezamen met de documenten die lokaal worden bewaard) toereikend ingericht in het kader van de rechtmatigheidsverantwoording. Wij zijn voornemens om te steunen op de VIC als beheersmaatregel.



Vooruitblik richting jaarrekeningcontrole 2023. We hebben met uw gemeente goede afspraken over de planning van de jaarrekeningcontrole gemaakt. Op voorhand identificeren we een aantal aandachtsgebieden met verhoogde aandacht in onze controle. Niet zozeer vanwege het feit dat de gemeente de beheersing hieromtrent niet op orde heeft, maar meer vanwege het feit dat bepaalde gebieden een verhoogd risico op fouten kennen. Dit betreffen met name de controle op de waardering van de grondexploitatie, de waardering van langlopende leningen en de controle op de toereikendheid van uw (onderhouds)voorzieningen. Daarnaast is de rechtmatigheidsverantwoording een belangrijk aspect in onze controlewerkzaamheden.



Tot slot hebben we vanuit het oogpunt van onze **natuurlijke adviesfunctie** in deze managementletter een bijlage opgenomen met actuele ontwikkelingen. Belangrijke elementen zijn hier onder andere de (aankomende) wijzigingen in de jaarverslaggevingsregels en in het Besluit accountantscontrole decentrale overheden. Ook hebben wij de ontwikkelingen ten aanzien van IT opgenomen in deze managementletter.

Bevindingen en aandachtspunten



2. Bevindingen en aandachtspunten

2.1 Algemeen

Doel en reikwijdte

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 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, 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 u als gemeente relevant zijn in onze controle meenemen. In ons auditplan hebben we onze risicoanalyse in detail aan u toegelicht. 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 (inclusief waardering complex Heesch-West);
- Risico dat het management van de gemeente de procesafspraken doorbreekt (management override of controls), hetgeen een standaard risico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de schattingsposten in de grondexploitatie en voorzieningen.

In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten. In 2023 is het risico inzake de rechtmatigheidsverantwoording toegevoegd. Daarnaast is het risico op controle van de rechtmatigheid van de inkopen/aanbestedingsrechtmatigheid niet meer van toepassing, deze verantwoordelijkheid ligt nu bij het college.

Algemeen beeld

We hebben geen significante tekortkomingen in uw AO/IC geconstateerd. Ten opzichte van voorgaand jaar constateren we dat de organisatie bezig is de inrichting van de interne beheersing verder te optimaliseren. Wij constateren dat onze eerdere aanbevelingen aandacht hebben en acties zijn ondernomen. Daarin benoemen we onder andere dat de gemeente nadere instructies heeft ontwikkeld voor de factuurafwikkeling gericht op de controle van prijs en prestatie. Daarnaast hebben wij vastgesteld dat het proces ten aanzien van de monitoring op de subsidievoorwaarden van professionele organisaties beter is ingericht. Tot slot merken we ook op dat het grondbedrijf, ondanks de krapte op de arbeidsmarkt versterkt is in de bezetting van de planeconomen.

2. Bevindingen en aandachtspunten

2.2 Beeld interne beheersing

Is de gemeente Oss klaar voor de rechtmatigheidsverantwoording?

Per 1 januari 2023 moet de gemeente Oss zelf een rechtmatigheidsverantwoording in de jaarrekening opnemen. Voorheen vormde de accountant een oordeel en bracht hierover verslag uit. Met ingang van boekjaar 2023 wordt het een verplichting voor het college van burgemeester & wethouders. De van toepassing zijnde wet- en regelgeving (Besluit begroting en verantwoording en Besluit Accountantscontrole Decentrale overheden) is op dit moment in revisie/in consultatie. De verwachting is dat de deze formalisatie de komende tijd gaat plaatsvinden.

De rechtmatigheidsverantwoording zien primair toe op de volgende aspecten:

- Begrotingscriterium
 - Begrotingsrechtmatigheid
 - Kredietrechtmatigheid
- Voorwaardencriterium
 - Aanbestedingsrechtmatigheid
 - Overige aspecten (treasury, subsidies, uitkeringen)
- M&O (Misbruik & Oneigenlijk) – gebruik criterium
 - Vaststellen dat college M&O-beleid heeft nageleefd

Op deze drie dossiers dient het college in het jaarrekeningdossier rekening te houden dat op deze aspecten er een toereikend onderbouwd oordeel beschikbaar dient te zijn inclusief het onderliggende interne controledossier. Dit dossier dient door de gemeente dusdanig aan ons als accountant gerapporteerd te worden, zodat wij dit als onafhankelijke derde zelfstandig moeten kunnen reviewen en beoordelen. De eisen die aan deze dossiers gesteld worden zijn dus hoger dan voorgaande jaren.

De gemeente is enkele jaren geleden ten behoeve van een planmatige aanpak van de verbijzonderde interne controle (VIC) Checkpoint gaan gebruiken en heeft inmiddels alle processen ingebed in Checkpoint. Het interne controleplan van de gemeente is opgenomen binnen de applicatie Checkpoint. Daarmee heeft de gemeente een duidelijk kader van aanpak en een gestructureerde aanpak geborgd. Ten opzichte van voorgaand jaar constateren we ook een verdere verduidelijking van de algehele aanpak en vastlegging.

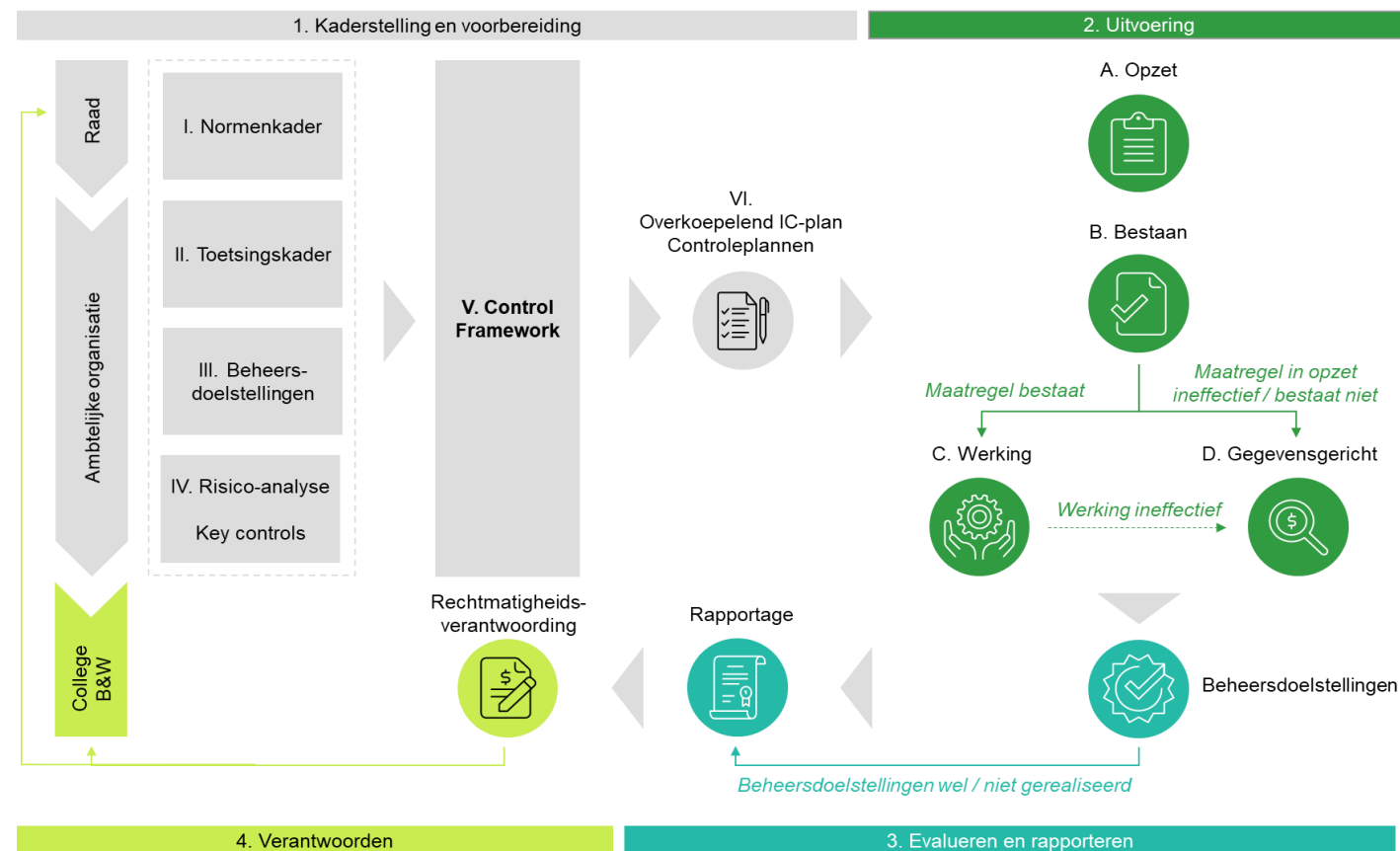
2. Bevindingen en aandachtspunten

2.2 Beeld interne beheersing

Inrichting en kwaliteit VIC

Een belangrijk onderdeel van de interne beheersing is de (verbijzonderde) interne controlefunctie (VIC). In het kader van de implementatie van de rechtmatigheidsverantwoording besteden wij hier extra aandacht aan.

In het kader van de rechtmatigheidsverantwoording is het voor uw gemeente van groot belang om alle stappen van onderliggende afbeelding goed in te richten. Dit betreffen (i) de kaderstelling en voorbereiding, (ii) de uitvoering, (iii) het evalueren en rapporteren en (iv) het verantwoorden van de uitgevoerde werkzaamheden in het kader van de rechtmatigheid. Zoals ook blijkt uit onderstaand proces heeft de VIC een prominente rol ten aanzien van de rechtmatigheidsverantwoording.



2. Bevindingen en aandachtspunten

2.2 Beeld interne beheersing

Inrichting en kwaliteit VIC

Op basis van de NBA handreiking 1152 zijn er voor de werkzaamheden van de accountant vier onderdelen waarop wij de VIC kunnen inzetten voor onze controlewerkzaamheden in het kader van de rechtmatigheidsverantwoording. Dit betreffen de volgende 'lagen':

1. VIC-functie als instrument om de aanlevering van stukken aan de accountant te verbeteren;
2. VIC-functie als onderdeel van het interne beheersingskader om toezicht te houden op de uitvoering van de interne beheersingsmaatregelen in de lijncontrole;
3. VIC-functie als interne beheersmaatregel voor de onderbouwing van de toelichting van de rechtmatigheidsverantwoording, waarop de accountant kan steunen bij de organisatie- en procesgerichte (test of control) werkzaamheden; en
4. VIC-functie als interne auditfunctie.

Wij zijn voornemens om in onze aanpak voor te sorteren op situatie 3, dit is de verwachting bij de meeste (grotere) gemeenten. Hierbij is het echter van belang dat het proces, zoals weergegeven op de vorige pagina, goed is ingeregeld. Voor 2023 geldt het volgende:

- Wij constateren dat de gemeente Oss een intern controleprotocol heeft geïmplementeerd. Hierin ligt vast hoe binnen de gemeente de VIC-controles worden uitgevoerd ten aanzien van de rechtmatigheid, getrouwheid en interne beheersing. Dit protocol omvat ook een stappenplan hoe een VIC-medewerker zijn werkzaamheden dient uit te voeren en hoe de selecties (voor de controlewerkzaamheden) gemaakt kunnen worden.
- Daarnaast hebben we in de voorgaande managementletter aanbevelingen gegeven om de kwaliteit en diepgang van de vastlegging in Checkpoint verder te verhogen. We zien dat in de vastlegging in Checkpoint ten opzichte van voorgaand jaar verdere vooruitgang is geboekt. De conclusies zijn uitgebreider verwoord. Hierbij wordt gebruik gemaakt van controlevragen waar in de reactievelden antwoord op wordt gegeven.
- Qua vastleggingen concludeert de gemeente dat Checkpoint zich niet altijd leent om onderliggende documentatie en controlewerkzaamheden op te nemen. De documentatie waarop de conclusies zijn gebaseerd is dan ook opgenomen in afzonderlijke mappen op de schijf. We vragen derhalve uw aandacht voor de onderlinge samenhang en leesbaarheid van het totale dossier per jaareinde.
- Gezien dit het eerste jaar is van de controle inzake de rechtmatigheidsverantwoording is het wenselijk vroegtijdig afstemming te hebben over de wijze waarop de onderbouwing van rechtmatigheidsverantwoording bij ons gaat worden aangeleverd en hoe u daarbij komt tot uw bevindingen in het kader van de rechtmatigheid.

Concluderend zien wij dat ten opzichte van voorgaand jaar stappen zijn gemaakt om het proces inzake de rechtmatigheidsverantwoording beter in te regelen. We zien dat in basis de vastlegging in Checkpoint (tezamen met de documenten welke lokaal zijn opgeslagen) voldoende is voor de werkzaamheden en zijn voornemens om op uw VIC als beheersmaatregel te steunen.

2. Bevindingen en aandachtspunten

2.3 Bedrijfsprocessen

Deze managementletter bevat onze bevindingen die zijn gebaseerd op de onze werkzaamheden in het kader van de jaar-rekeningcontrole 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 managementletter geven wij u een schriftelijke update van onze bevindingen.

In het overzicht hiernaast zijn de bevindingen inclusief prioriteit opgenomen. Een totaaloverzicht van de detailbevindingen is opgenomen in bijlage 1.

In de tabel rechts is een totaal overzicht opgenomen van het totaal aantal detailbevindingen. De bevindingen en onze aanbevelingen worden in bijlage 1 van deze managementletter uitgebreider toegelicht.

De kleur van de het symbool geeft de status van de constatering aan.

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

aandachtspunten	
Aantal nieuwe aanbevelingen	0
Aantal aanbevelingen uit voorgaande jaren	2
Waarvan opgelost in 2023	2
Resterende aanbevelingen uit voorgaande jaren	0
Waarvan reeds acties zijn ondernomen, maar nog niet zijn afgerond	0
Waarvan nog geen acties zijn ondernomen	0
Aantal openstaande aanbevelingen	0

#	Proces	Bevinding	Status	Prioriteit 2023	Prioriteit 2022
1	Verstrekke subsidies	Monitoring op naleving subsidievoorwaarden	●	-	Laag
2	Inkopen	Inrichting van het proces	●	-	Middel

2. Bevindingen en aandachtspunten

2.4 Three lines model

Wij rapporteren via het 3 lines model. Dat wil zeggen dat wij binnen de processen nagaan op welk niveau in de organisatie de interne beheersmaatregelen worden ondervangen. De volgende niveaus worden hierbij onderkend:

- 1^e lijn: in het primaire proces, onder verantwoordelijkheid van de proceseigenaar.
- 2^e lijn: in de ondersteunende processen zoals financiën en control, waar checks and balances ingericht zijn om fouten te signaleren.
- 3^e lijn: in uw verbijzonderde interne controle achteraf.

Indien de beheersmaatregelen in de 1^e en/of 2^e lijn adequaat zijn ingericht dan is de organisatie optimaal in control en is een voornamelijk systeemgerichte controleaanpak mogelijk. Indien dit niet het geval is kan dit gecompenseerd worden door de gegevensgerichte werkzaamheden van de VIC. In het kader van de rechtmatigheidsverantwoording dient in ieder geval de 3^e lijn (VIC) toereikend te zijn. Onderstaand overzicht geeft zodoende een beeld over de mate van beheersing en controle van uw gemeente.

Nr.	Proces	1 ^e lijn	2 ^e lijn	3 ^e lijn	Opmerking / toelichting
1	Inkopen en betalingen	●	●	●	Zie bijlage 1 detailbevinding 2 'inkopen- inrichting van het proces. Deze bevinding is in 2023 opgevolgd en om deze reden is eerste lijn aangepast naar groen.
2	Aanbestedingen	●	●	●	
3	Lonen en salarissen	●	●	●	
4	Subsidies	●	●	●	Zie bijlage 1 detailbevinding 1 'verstrekke subsidies - Monitoring op naleving subsidievoorwaarden'. Deze bevinding is in 2023 opgevolgd en om deze reden is eerste lijn aangepast naar groen.
5	Grondexploitatie	●	●	●	Zie paragraaf 2.5 in deze managementletter
7	Participatiewet	●	●	●	
8	Jeugdwet	●	●	●	
9	WMO	●	●	●	
10	Omgevingsvergunningen	●	●	●	
11	Huren en pachten	●	●	●	
12	IT	●	●	-	Zie hoofdstuk 3 bevindingen IT-beheersing

Uit bovenstaand beeld komt naar voren dat wij nog niet optimaal op alle processen kunnen steunen, maar wel een mogelijkheid zien om meer op uw interne beheersing te kunnen steunen. In lijn met voorgaande jaren hanteert de VIC nog grotendeels een gegevensgerichte aanpak. Wij bespreken uiteraard graag met u de mate van beheersing en uw gewenste ambitieniveau en op welke vlakken .

Legenda status:

- = geen bevindingen met kans op materiële fouten, enkel aanbeveling ter verdere optimalisatie
- = één of enkele bevindingen met geringe impact reteren

● = meerdere bevindingen en aanbevelingen met mogelijk grote impact

2. Bevindingen en aandachtspunten

2.5 Belangrijke macro-economische ontwikkelingen

Grondexploitaties

In het kader van onze tussentijdse controle hebben wij met uw planeconomen gesproken. Wij hebben het concept najaarsbericht besproken en daarnaast hebben wij gesproken over de opzet van het proces om te komen tot een juiste waardering van de grondexploitaties.

Allereerst constateren wij dat uw bezetting van de planeconomen qua kwaliteit en kwantiteit versterkt zijn. Deze afdeling fungeert inmiddels op volle kracht en is proactief bezig om de beheersing rondom de grondexploitaties verder aan te scherpen. Wij achten dit een goede ontwikkeling.

Met uw planeconomen hebben wij gesproken over twee belangrijke aanbevelingen ten aanzien van de juistheid en waardering van de grondexploitaties. Deze aanbevelingen hebben wij gerapporteerd in het accountantsverslag 2022. Wij vragen u hier nogmaals de aandacht voor in het kader van de jaarrekeningcontrole 2023. Dit betreffen de volgende aanbevelingen:

- De optimistische inschattingen qua timing ten aanzien van de kosten en opbrengsten;
- Aandacht voor de actualiteit van de kostenramingen.

Wij constateren dat op vlakken al actiepunten door de organisatie geïdentificeerd zijn en onze adviezen worden volgens de afdeling meegenomen bij het opstellen van het Meerjaren Perspectief Grondexploitaties (MPG) voor de jaarrekening 2023.

Tevens hebben wij de volgende adviezen besproken:

- Maak een overkoepelende analyse van het totaal van uw grondexploitaties zodat u op totaalniveau weet wanneer kosten/opbrengsten ongeveer gerealiseerd gaan worden. Op deze wijze kunt u ook op macroniveau een analyse maken of de realisatie van (toekomstige) plannen ook past binnen de capaciteit van de ambtelijke organisatie.
- Breng tijdens het actualiseren van de grondexploitatie (zowel bij het najaarsbericht als bij het opstellen van het MPG) specifiek in beeld of de noodzakelijke aanpassingen in schattingen reeds eerder geïdentificeerd hadden kunnen worden en ga na welke redenen hieraan ten grondslag liggen. Dit zodat in de toekomst de kwaliteit van de schattingsnauwkeurigheid verder verbeterd kan worden.

Tot slot merken we op dat er (conform voorgaand jaar) momenteel diverse onzekere factoren zijn die impact hebben op de ontwikkeling van grondexploitaties, denk hierbij onder andere aan de stijgende rente. De onzekerheid over de toekomstige ontwikkelingen betekent een zeer grote schattingsonzekerheid op de verwachte realisatie van uw complexen. Wij verzoeken u bij het opstellen van de jaarrekening wederom om na te gaan in welke mate bovenstaande elementen impact hebben op uw specifieke situatie en deze op een vergelijkbare wijze toe te lichten in de jaarrekening. Op deze wijze heeft de raad ook een goed inzicht in de schattingsgevoeligheid van de grondexploitatie.

2. Bevindingen en aandachtspunten

2.5 Belangrijke macro-economische ontwikkelingen

Aandachtspunten voor de
jaarrekeningcontrole 2023

Nederland heeft op dit moment nog steeds te maken met enkele extreme omstandigheden: enorm oplopende inflatie en rente, 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 2023. Deze aandachtspunten zijn op hoofdlijnen ongewijzigd aan voorgaand jaar (zowel managementletter als accountantsverslag). Wij noemen ze hier puntsgewijs.

- Actualisatie van uw grondexploitaties zoals op de voorgaande pagina benoemd.
- Inbaarheid van de langlopende vorderingen (in het bijzonder aandacht voor de vorderingen richting gesubsidieerde instellingen en de leningen Wachtmeester en Pivot Park).
- Actualiteit van uw onderhoudsvoorzieningen als gevolg van stijgende bouwkosten en inflatie. De jaarlijkse analyse op de onderhoudsvoorzieningen kan aan kwaliteit winnen. Hierbij is het van belang om de verwachte kosten te actualiseren naar het prijspeil 2023. Tevens is het van belang om een juiste en volledige analyse op te stellen inzake doorgeschoven onderhoud.
- Indien het negatieve vermogen van de gemeenschappelijke regeling Heesch-West verder op loopt dient hiervoor een risicovoorziening te worden gevormd.
- Gezien de hoeveelheid SiSa-regelingen vragen wij u voldoende kritisch door de interne oplevering heen te gaan alvorens dit wordt aangeleverd aan ons. Afgelopen jaar was de aanlevering niet in alle gevallen volledig c.q. nauwkeurig.

2. Bevindingen en aandachtspunten

2.6 Fraudeanalyse

Verantwoordelijkheid college/
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.

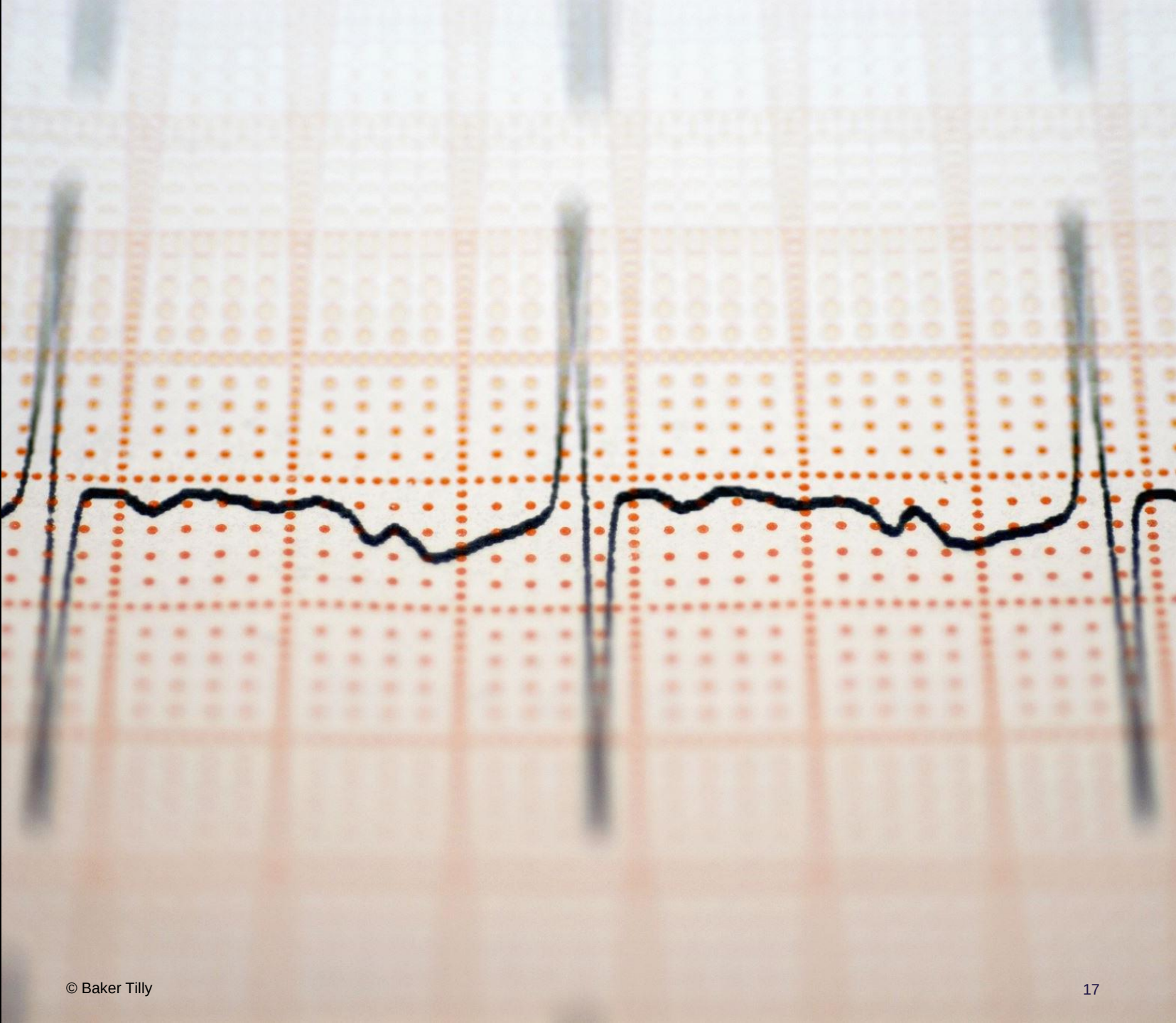
Wij hebben in voorgaand jaar reeds vastgesteld dat er binnen de gemeente aandacht is voor frauderisico's en de preventie daarvan. Wel zijn wij van mening dat hier een verbeterslag in te maken is en dat de risicoanalyse meer moet toezien op deze tijd. Inmiddels is de gemeente bezig om een nieuwe frauderisicoanalyse op te stellen. De voorgaande frauderisicoanalyse dateerde uit 2015 en was derhalve toe aan actualisatie. Recentelijk hebben wij de concept frauderisicoanalyse beoordeeld en van aanbevelingen voorzien. Wij adviseren u onze aanbevelingen te verwerken in de frauderisicoanalyse zodat deze vervolgens geïmplementeerd kan worden.

De verbijzonderde interne controle kan ook aan waarde winnen als de opdracht hiervoor wordt ingegeven vanuit een interne frauderisicoanalyse, waardoor de werkzaamheden beter aansluiten op de risico's binnen de organisatie. Op deze wijze wordt de verbijzonderde interne controle volwaardiger en volwassener. Het is van belang dit door te vertalen in Checkpoint.

Nota misbruik en oneigenlijk gebruik

De huidige nota Misbruik en Oneigenlijk gebruik is in werking getreden in 2015. Wij hebben uit diverse besprekingen vernomen dat vernieuwing van deze nota onder de aandacht is. Wij adviseren om deze nota te actualiseren, dan wel te integreren in de onder handen zijnde frauderisicoanalyse (ook in het oogpunt van de rechtmatigheidsverantwoording).

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 managementletter.

Op basis van de door ons uitgevoerde werkzaamheden in september 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 zullen wij onze bevindingen rapporteren.

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.
 Wijzigingsbeheer	Bij het toetsen van 'wijzigingsbeheer' ofwel change management wordt vastgesteld dat wijzigingen aan de applicatie op gestructureerde en gecontroleerde wijze worden doorgevoerd. Voor uw organisatie heeft wijzigingsbeheer ten doel om te voorkomen dat applicaties zich niet gedragen zoals u verwacht na een wijziging in de software, resulterend in, wellicht niet opgemerkte, (financiële) gevolgen.
 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	Het is van 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.

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.

Authenticatie	Autorisatie	Wijzigings-beheer	Omgeving
Netwerk n.v.t			De ingestelde wachtwoordeisen van het netwerk zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen. We constateerden dat 213 actieve accounts een niet verlopend wachtwoord hebben, waarvan 144 accounts ook een inlogdatum in dit jaar hebben. Gezien de aard van deze accounts (service-accounts, mailboxen, tv-schermen), achten wij het risico daarvan laag. De accounts hebben geen impact op de relevante applicaties voor de jaarrekeningcontrole. De hoge rechten in de Active Directory zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole. Wij hebben gezien dat het aantal accounts ten opzichte van het voorgaande boekjaar flink is afgenomen (vorig jaar 341 accounts met 189 ingelogd in 2022), wij adviseren u om na te gaan of het terecht is dat 213 accounts een niet verlopend wachtwoord dienen te hebben.
Suites voor het Sociaal Domein 			De ingestelde wachtwoordeisen van de applicatie zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen. Suites voor het Sociaal Domein kent een vaste set wachtwoordvereisten waaraan de gebruikersorganisatie in basis geen aanpassingen aan kan doen. Wel kan er, per gebruiker, een afwijkende geldigheidsduur voor het wachtwoord worden ingesteld. Wij hebben verschillende accounts aangetroffen welke actief zijn, maar sinds 2022 of eerder niet hebben ingelogd, dit kan een indicatie zijn dat de accounts niet meer noodzakelijk zijn. Wij hebben geconstateerd dat 2 relevante accounts uitgezonderd zijn van de wachtwoordperiodiciteit en langere wachtwoordduur hanteren. Wij raden aan wachtwoorden minimaal twee keer per jaar te wijzigen, mede gegeven de gevoeligheid van de processen die daarin plaatsvinden. Wij hebben vastgesteld dat 7 persoonsgebonden gebruikers rechten hebben tot het wijzigen van autorisaties per gebruiker en autorisaties per rol. Deze personen zijn niet actief in de uitvoering. Wij adviseren u ten aanzien van de beheerprocessen om de rechten voor het aanmaken en verwijderen van gebruikers en het muteren van gebruikersrechten te registreren en hiervoor een matrix te hanteren voor de SOLL-positie en rollen en rechten in te richten en beheersen conform deze matrix met geformaliseerde procedures.

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.

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

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 vervolg   			Softwarewijzigingen worden getest alvorens deze worden doorgevoerd. Deze testwerkzaamheden zijn op dit moment nog niet altijd te herleiden. Voor wijzigingsbeheer geldt dat de stappen, zoals beschreven in bijlage 3, slechts deels en veelal zonder uitgebreide vastlegging, worden doorlopen. Wij raden aan het wijzigingsproces te formaliseren en alle stappen zichtbaar vast te leggen. Dit zodat u als organisatie aantoonbaar grip houdt op alle wijzigingen die zijn doorgevoerd. Tevens kunt zich er op deze manier van verzekeren dat er geen onvoorziene mutaties in de applicatie worden doorgevoerd. Wij hebben tijdens ons interview vernomen dat gemeente Oss bezig is met de implementatie van testsoftware die de vastleggingen in dit proces meer zal gaan faciliteren.

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

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

Wijzigingsbeheer

Omgeving

Key2

Financiën



Er wordt ingelogd in de applicatie middels Single Sign On (SSO). Hierdoor zijn de wachtwoordinstellingen van het netwerk leidend. De ingestelde wachtwoordeisen van het netwerk zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen.

De hoge rechten in de applicatie zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole. Hierin hebben wij een verbetering gezien ten opzichte van de interim-controle van voorgaand jaar.

Wij adviseren u om de rechten voor het aanmaken en verwijderen van gebruikers en het muteren van gebruikersrechten te registreren en hiervoor een matrix te hanteren voor de SOLL-positie en rollen en rechten in te richten en beheersen conform deze matrix met geformaliseerde procedures. De huidige inrichting waarbij afdoende functiescheiding is aangebracht kan voor deze functieautorisatiematrix als sjabloon dienen.

Met betrekking tot het proces wijzigingsbeheer hebben wij voor een doorgevoerde wijziging kunnen vaststellen dat de functionaliteiten in de applicatie worden getest voor live-gang en dat door de verantwoordelijke voor de applicatie akkoord wordt gegeven op de testwerkzaamheden en live-gang naar productie. De risicoanalyse op de wijziging zien wij impliciet terug in de uitgevoerde werkzaamheden. Daarmee wordt invulling gegeven aan de relevante stappen in het wijzigingsbeheerproces. Wij hebben tijdens ons interview vernomen dat gemeente Oss bezig is met de implementatie van testsoftware die de vastleggingen in dit proces meer zal gaan faciliteren.

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

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

Wijzigingsbeheer

Omgeving

Motion



Er wordt ingelogd in deze applicatie ten behoeve van de salarisadministratie middels Single Sign-On (SSO). Hierdoor zijn de wachtwoordinstellingen van het netwerk leidend. De ingestelde wachtwoordeisen van het netwerk zijn van voldoende niveau om op de authenticatie van gebruikers te kunnen steunen.

De hoge rechten in de applicatie zijn niet beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole. Er zijn meerdere gebruikers, buiten de applicatiebeheerder, met administratorrechten. Deze gebruikers met hoge rechten kunnen zichzelf of anderen rechten toe kennen die niet aan de functie zijn toebedeeld. Hierdoor is het risico aanwezig dat functiescheiding kan worden doorbroken. Wij raden aan de scheiding tussen beheer en processen aan te houden binnen Motion.

Wij adviseren u om de rechten voor het aanmaken en verwijderen van gebruikers en het muteren van gebruikersrechten te registreren en hiervoor een matrix te hanteren voor de SOLL-positie en rollen en rechten in te richten en beheersen conform deze matrix met geformaliseerde procedures.

Het proces m.b.t. wijzigingsbeheer hebben wij niet inhoudelijk kunnen toetsen. In opzet achten wij dit proces voldoende. Motion betreft een SaaS-applicatie en daarom is een deel van het wijzigingsproces belegd bij de leverancier. Dit houdt echter niet in dat uw organisatie geen verantwoordelijkheden meer kent binnen het wijzigingsproces. Wij verwijzen graag naar bijlage 3 en raden aan ook in de toekomst de relevante stappen binnen het wijzigingsproces te blijven uitvoeren. Wij hebben tijdens ons interview vernomen dat gemeente Oss bezig is met de implementatie van testsoftware die de vastleggingen in dit proces meer zal gaan faciliteren.

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: U heeft aangegeven dat back-ups periodiek en incrementeel worden gemaakt en extern worden opgeslagen. Er wordt een dagelijkse back-up gemaakt, waardoor het dataverlies beperkt wordt. Tevens wordt u geïnformeerd of de back-up naar behoren is uitgevoerd.

Voor de aanstaande beweging richting de gehoste Microsoft-oplossing is het afgelopen jaar gewerkt aan een wijze van back-up van de gebruikersgegevens, zodat het Recovery Point gehandhaafd kan worden in de nieuwe omgeving.

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.

Recovery: U heeft aangegeven dat er periodiek (disaster) recovery test wordt uitgevoerd. Dit wordt uitgevoerd als onderdeel van de uitwijktest. Zie ook hieronder.

Uitwijk: U heeft aangegeven dat er periodiek een uitwijktest wordt uitgevoerd. Dit wordt opgenomen in een rapport en eventuele bevindingen zijn opgevolgd.

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 aparte ruimte. De serverruimte wordt niet gebruikt voor andere doeleinden. Naast toegang zijn er maatregelen getroffen omtrent klimaatbeheersing en branddetectie. Voor Cloud-applicaties zijn afspraken gemaakt met leveranciers over de beveiliging van de fysieke servers.

Vervolg Beveiliging

Remote access: Voor extern inloggen wordt gebruik gemaakt van een VPN verbinding, waarbij met een combinatie van gebruikersnaam en wachtwoord ingelogd wordt en aanvullend gebruik wordt gemaakt van Two-factor Authenticatie. Het risico dat externen zich toegang verschaffen tot uw geautomatiseerde omgeving is hierdoor beperkt.

Preventie: Een firewall en virusscanner is aanwezig en wordt actief beheerd. Hiernaast vindt een periodieke awareness training plaats, waarmee het risico op fouten door menselijk handelen verminderd wordt.

Monitoring: Intern vindt monitoring plaats ten aanzien van cyber risico's. Wij hebben begrepen dat sinds eind 2022 een Cyber monitoring en response dienst afgenomen wordt bij een daarin gespecialiseerde partij.

Naast deze ontwikkeling is er in het boekjaar een onderzoek door een externe organisatie een kwetsbaarheidsscan uitgevoerd en zijn verschillende initiatieven ontplooid, zoals het bezoek van een mystery guest.

Hiermee laat de gemeente Oss zien aandacht te besteden aan de zowel de technische beveiliging van de omgeving als het menselijke component daarin.

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 ontlenen aan de door ons beschreven aandachtspunten.

Beleid en Plannen

Beleid

Binnen uw organisatie is een overkoepelend informatiebeveiligingsbeleid aanwezig. In dit beleid staan de uitgangspunten voor informatiebeveiligingsbeleid beschreven. Op basis van dit beleidsplan is monitoring mogelijk aan de hand van een plan-do-check-act cyclus. Wij hebben begrepen dat het nieuwe informatiebeveiligingsbeleid geformaliseerd is ter vervanging van het beleid uit 2018.

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. De verantwoordelijkheden binnen uw gemeente zijn belegd.

Verantwoordelijkheden en regiefunctie (vervolg)

Bij het uitbesteden van taken en verantwoordelijkheden aan externe partijen, zoals bij SaaS-applicaties gebruikelijk is, is het in gevallen waar het toezicht op deze organisaties belegd is. Wij hebben begrepen dat voor de relevante applicaties wel verantwoordelijkheden toegewezen en regelmatig overleg plaats vindt. Het is aan te bevelen dit een meer integraal onderdeel van de organisatie te maken.

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.

U heeft een ticketsysteem, waar incidenten in gemeld worden en via waar ook verschillende procedures zijn ingericht.

Uitvoering beheersingsmaatregelen IT

Op verschillende vlakken worden (nog) geen toetsbare beheersingsmaatregelen uitgevoerd binnen uw organisatie.

Denk daarbij aan vastgelegde periodieke controles op actieve gebruikers & een periodieke controle op inrichting van wachtwoordbeleid conform de daarvoor gestelde normen door uw organisatie.

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

Bij de uitvoering van onze interim-werkzaamheden zijn wij, zoals gemeld, niet tegen materiële bijzonderheden aangelopen.

Bijlage 1: detailbevindingen

Detailbevindingen

1. Uitleg opbouw

In dit hoofdstuk zijn de significante bevindingen opgenomen.

Per bladzijde van deze managementletter is een bevinding opgenomen met daarbij het risico en een aanbeveling. Bij elke bevinding staat de datum van de eerste vermelding aangegeven te samen met de gradatie van de constatering. Bij de prioriteit staat de mate van belangrijkheid en urgentie.

Per bevinding zullen wij aangeven welke alternatieve werkzaamheden wij zullen uitvoeren om het geconstateerde risico (gegevensgericht) te ondervangen.

Voor bestaande bevindingen geven wij tevens een update van de status van deze bevinding in het huidige boekjaar.

Bevinding

In dit blok wordt aangegeven wat gedurende de accountantscontrole is geconstateerd en waarvan wij u graag op de hoogte willen brengen.

Prioriteit	Boekjaar bevinding	Status
Urgentie en belang van de bevinding	Boekjaar eerste vermelding	   
	Risico Hierbij geven wij aan wat de risico's zijn van de bevinding en wat de gevolgen voor uw organisatie kunnen zijn.	
	Aanbeveling Hier geven wij u aanbevelingen met betrekking tot de bevinding. Deze aanbeveling is een mogelijke oplossing voor de bevinding.	
	Update boekjaar / Gevolgen jaarrekeningcontrole Hier geven wij een update van de bevinding wanneer deze in een eerder boekjaar is geconstateerd. Tevens kan de bevinding gevolgen hebben voor de controleaanpak / omvang van onze controlewerkzaamheden. Op deze plaats maken wij hier eveneens vermelding van.	

De kleur van de het symbool geeft de status van de constatering aan.

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

Detailbevindingen

2. Verstrekte subsidies - monitoring op naleving subsidievoorwaarden

Bevinding

Er vindt geen gestructureerde zichtbare evaluatie plaats of de subsidieontvanger in formele zin aan de vereisten uit de subsidieverordening heeft voldaan. Tevens is er geen gestructureerde zichtbare vastlegging of de subsidieontvanger de prestaties heeft geleverd zoals afgesproken in de beschikking. Dit geldt voor zowel professionele als vrijwillige subsidies.

Update 2023

Wij hebben geconstateerd dat gedurende boekjaar 2023 binnen de afdeling subsidiebeheer een bewakingsadministratie is opgesteld. Dit geldt enkel voor de professionele organisaties. Wij begrijpen van u dat vrijwillige subsidies een waarde per jaar kennen van circa € 1,8 miljoen. Gezien de relatief geringe waarde van deze vrijwillige subsidies ten opzichte van professionele subsidies (circa € 20 miljoen) (en ook in relatie tot onze materialiteit) zijn wij van mening dat dit punt in het kader van de jaarrekeningcontrole is opgevolgd en daarmee afgerond.

Prioriteit	Boekjaar bevinding	Status
Laag	2020	
	Risico Deze bevinding is opgevolgd.	
	Aanbeveling Deze bevinding is opgevolgd.	
	Gevolgen jaarrekeningcontrole Deze bevinding is opgevolgd.	

Detailbevindingen

3. Inkopen – inrichting van het proces

Bevinding

We constateren dat er geen geformaliseerde vastlegging wat de codeerder (prestatieverklaarder) noch een budgethouder moet controleren voordat een factuur wordt geautoriseerd. Voor zover ons nu bekend geeft men akkoord naar eigen invulling. Dit leidt er toe dat de mate van diepgang van de controle door de codeerder dan wel budgethouder kan verschillen. Tevens kan het zijn dat aspecten niet gecontroleerd worden doordat de codeerder dan wel budgethouder onvoldoende op de hoogte zijn wat hun verantwoordelijkheid is.

Tevens is niet duidelijk in welke mate eventuele de onderliggende documenten ter onderbouwing van de prestatielevering in Key2Financien opgeslagen moeten worden.

Achteraf wordt steekproefsgewijs een controle uitgevoerd door de VIC medewerkers of de medewerkers terecht akkoord hebben gegeven.

Update 2023

Wij constateren dat er een presentatie factuurafhandeling en kredietbewaking is opgesteld en is gedeeld via intranet. Daarnaast zijn er trainingen gegeven waarbij uitleg wordt gegeven welke rollen er zijn bij een facturatieproces en wat er bij welke rol wordt verwacht. Echter hebben we de controle vanuit VIC (of medewerkers terecht akkoord hebben gegeven) nog niet kunnen toetsen. Mochten we hierbij bevindingen constateren zullen wij dit rapporteren in het accountantsverslag.

Prioriteit	Boekjaar bevinding	Status
Middel	2022	
	Risico Deze bevinding is opgevolgd.	
	Aanbeveling Deze bevinding is opgevolgd.	
	Gevolgen jaarrekeningcontrole Deze bevinding is opgevolgd.	

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



Notitie overhead

Notitie overhead

De Notitie Overhead van de commissie BBV is in het voorjaar 2023 geactualiseerd en ter consultatie 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.

Wetswijzigingen BBV en Bado (1)

Wetswijzigingen BBV en Bado (1/3)

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 onderstaand de belangrijkste voorgestelde wijzigingen opgenomen:

Er wordt een nieuwe 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.

Wetswijzigingen BBV en Bado (2)

Wetswijziging BBV en Bado (2/3)

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.

Daarnaast worden de eisen ten aanzien van 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:

- 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.

Wetswijzigingen BBV en Bado (3)

Wetswijzigingen BBV en Bado (3/3):

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 verantwoordinggrens.
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 van de reserves.
4. Indien het eindbedrag hoger is dan de verantwoordingsgrens licht het college van burgemeesters en wethouders of gedeputeerde staten deze afwijking toe in de rechtmatigheidsverantwoording.

De commissie BBV stelt een modeltekst voor de rechtmatigheidsverantwoording op.

Besluit accountantscontrole decentrale overheden

Besluit accountantscontrole decentrale overheden

Er ligt op dit moment een consultatie voor inzake de wijziging van het besluit accountantscontrole decentrale overheden. De verwachting is dat de voorgestelde wijzigingen vanaf boekjaar 2025 van kracht zullen zijn. De belangrijkste wijzigingen zijn het feit dat de goedkeuringstolerantie wijzigt van 1% voor fouten en 3% voor onzekerheden met als omvangsbasis de totale lasten (inclusief dotaties aan reserves) naar 2% voor het totaal aan fouten en onzekerheden met als omvangsbasis de totale lasten (exclusief dotaties aan reserves).

Ten aanzien van de SiSa-bijlage houdt de accountant de verantwoordelijkheid om ook de rechtmatigheid vast te stellen.

Materialiteit	Goedkeurende verklaring	Verklaring met beperking	Verklaring van oordeelonthouding/ Afkeurende verklaring
Fouten in de jaarrekening en onzekerheden in de controle	$\leq 2\%$	$> 2\% - \leq 4\%$	$> 4\%$

Deze wijziging kan een belangrijke impact hebben. Wij adviseren u te evalueren wat dit voor uw situatie betekent en welke stappen gezet dienen te worden ter waarborging dat de fouten en onzekerheden binnen de goedkeuringstoleranties blijven.

Kadernota rechtmatigheid 2023

De Kadernota rechtmatigheid is per 29 september 2023 geactualiseerd. Belangrijke wijzigingen ten opzichte van de versie van augustus 2021 zijn als volgt:

- SiSa is onderdeel van de rechtmatigheidsverantwoording. Fouten en onduidelijkheden ten aanzien van de regelingen dienen betrokken te worden bij de rechtmatigheidsverantwoording.
- Er is nadere verduidelijking gegeven aan de begrotingsonrechtmatigheid en wanneer hier sprake van is;
- Er is een beslisboom opgenomen waarin wordt ingegaan op de samenloop van getrouw- en rechtmatigheidsbevindingen.

Bijlage 3: actuele ontwikkelingen ten aanzien van IT



Logische toegangsbeveiliging

Wij onderscheiden vijf bouwstenen ten aanzien van toegangsbeveiliging, waarbij bouwstenen gestapeld, naast een sterke IT beheersing, ook de meeste controlezekerheid oplevert. Beperkingen in de onderliggende steen, zorgt voor een verzwakking van de bovenliggende stenen. In het onderstaande figuur zijn de bouwstenen schematisch weergegeven, op de volgende slides geven wij per applicatie weer welke bevindingen wij per applicatie hebben:

Authenticatie



Databases: Basis voor toegangsbeveiliging van een applicatie is dat de applicatie de enige toegangspoort is en dat niet rechtstreeks op de database gemuteerd kan worden.



Wachtwoorden: Sterke, regelmatig wijzigende wachtwoorden voor applicaties en databases zijn de basis voor toegangsbeveiliging, samenhangend met bewustzijn bij medewerkers.

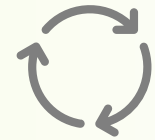
Autorisatie



Hoge rechten: Voor het beheersen van autorisaties is het cruciaal dat de rechten tot het aanpassen van rechten zijn beperkt tot medewerkers die geen belang hebben bij aanpassingen.



Gewenste situatie: Iedere organisatie zal moeten bepalen wat de "SOLL-positie" is ten aanzien van rechten, met name gericht op kritische functiescheidingen



Beheersen mutaties: Wanneer de gewenste situatie is ingericht, verwachten wij een beheerst proces ten aanzien van het toekennen, ontnemen en wijzigen van rechten inclusief monitoring en controle.

Wijzigingsbeheer

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 onderstaand aangegeven wat wij verwachten per fase. Onder wijzigingen verstaan wij niet alleen nieuwe versie updates, maar ook aanpassingen in (kritieke) systeemconfiguraties.

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

NIS2 als uitdaging voor uw gemeente?

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 Normatieve 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 adviseren wij de ontwikkelingen te blijven volgen en te anticiperen op de impact daarvan.

Wij hebben in gesprekken met de gemeente Oss begrepen dat de urgentie en relevantie van de nieuwe regelgeving bekend is en dat de gemeente Oss de impact van de nieuwe regelgeving onderzoekt.

