

Managementletter

Gemeente Oss
Boekjaar 2026

Aanbiedingsbrief



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

ONDERWERP:
Managementletter

Geacht college,

Als onderdeel van de jaarrekeningcontrole van boekjaar 2026 van de gemeente Oss rapporteren wij u onze bevindingen uit de interim-controle.

In deze managementletter rapporteren wij de bevindingen naar aanleiding van onze controle, de belangrijkste risico's, ons beeld van de interne beheersing, relevante ontwikkelingen in wet- en regelgeving en indien van toepassing andere veranderingen die voor u relevant kunnen zijn. In de bijlage hebben wij een gedetailleerd overzicht opgenomen van onze bevindingen en aanbevelingen.

De bevindingen komen voort uit onze werkzaamheden in het kader van de jaarrekeningcontrole en zijn opgenomen voor zover wij het van belang achten om deze met u te communiceren. De bevindingen en aanbevelingen dienen te worden gelezen als constructieve aanwijzingen voor het college als onderdeel van een continue proces van het veranderen en verbeteren van de beheersing van de organisatie.

Deze 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) B.V.

drs. B. (Barry) Smeenk RA

Inhoud

1. Management samenvatting
2. Kwaliteit interne beheersing & IT
3. Voorbereiding jaarrekeningcontrole
4. Actualiteiten
5. Bijlagen



1. Management samenvatting



1. Management samenvatting

Algemene conclusie over interne beheersing

Wij hebben geen significante tekortkomingen in uw AO/IC geconstateerd. Onze aanbevelingen in deze managementletter zijn dan ook, gelijk aan voorgaande jaren, gericht op het verder aanscherpen en optimaliseren van de (IT-)processen en bevatten de belangrijkste aandachtspunten richting de jaarrekeningcontrole.

Het beeld dat wij van de gemeente Oss hebben vanuit voorgaande jaren is bij de tussentijdse controle voor de jaarrekening 2026 bevestigd. Ontwikkelingen worden actief opgepakt en er is zichtbaar aandacht voor het continue verbeteren van processen.

IT

Ook de IT beheersomgeving is binnen de gemeente Oss in grote mate op orde. Er zijn nog met name aandachtspunten, zoals ook door de organisatie zelf gesignaleerd, ten aanzien van het voldaan aan de recent ingevoerde cyberbeveiligingswet. Daarbij merken we wel op dat de gemeente Oss ten opzichte van andere vergelijkbare gemeenten de compliance ten aanzien van de cyberbeveiligingswet goed oppakt. Ten aanzien van de nieuw in gebruik genomen salarisapplicatie hebben we aanvullende aandachtspunten in deze managementletter opgenomen.

Kwaliteit van Verbijzonderde Interne Controle (VIC)

De VIC binnen de gemeente Oss is op een goede en professionele wijze ingericht. We zijn van mening dat dit instrument van nog meer toegevoegde waarde kan zijn op het moment dat de VIC breder wordt ingezet op bijvoorbeeld themaonderzoeken, de beheersing van de IT-omgeving of de waardering grondexploitaties. Daarnaast moedigen we u aan de VIC te blijven doorontwikkelen door meer gebruik te maken van data-analyse.

Aandachtspunten jaarrekeningcontrole

Op basis van onze risicoanalyse hebben wij een aantal aandachtspunten geïdentificeerd die gedurende de jaarrekeningcontrole specifieke aandacht vragen. Deze aandachtspunten houden niet zozeer verband met tekortkomingen in de interne beheersing, maar vloeien met name voort uit de inherente complexiteit en het verhoogde risico op afwijkingen binnen deze posten. De risicoanalyse is een continu proces en wordt gedurende de controle waar nodig geactualiseerd.

De belangrijkste aandachtspunten zien toe op de waardering van de grondexploitaties. In het bijzonder vragen wij aandacht voor de grondexploitatie Raadhuislaan Zuid. Recente uitspraken van de Commissie BBV hebben naar verwachting gevolgen voor de financiële verwerking van dit project. Wij begrijpen dat bij de behandeling van de begroting de financiële dekking wordt herijkt en de dat de administratieve verwerking bij de jaarrekening mee wordt genomen.

Daarnaast vragen wij aandacht voor de tijdige en volledige dossiervorming ten behoeve van de SiSa-verantwoording. De controle van de specifieke uitkeringen neemt zowel voor de organisatie als voor de accountant een toenemend beslag op capaciteit. Tot slot vragen de actuele ontwikkelingen rondom de voorgenomen overdracht van de wethouderspensioenen blijvende aandacht. Wij verzoeken u de financiële gevolgen van deze ontwikkelingen tijdig te beoordelen.

Actuele ontwikkelingen

Vanuit onze natuurlijke adviesfunctie hebben wij in deze managementletter een bijlage met actuele ontwikkelingen opgenomen. Wij vragen u hiervan kennis te nemen en hier indien noodzakelijk rekening mee te houden bij de doorontwikkeling van uw organisatie dan wel bij het opstellen van de jaarrekening 2026.

Management samenvatting

Kwaliteit interne beheersing & IT

Voorbereiding Jaarrekeningcontrole

Actualiteiten

Bijlagen

2. Kwaliteit interne beheersing & IT

Dit hoofdstuk bevat onze bevindingen ten aanzien van de interne beheersing (inclusief de IT-omgeving). Vanuit onze natuurlijke adviesfunctie willen wij bijdragen aan verbetering van uw bedrijfsvoering, onder andere door het analyseren van de IT-omgeving en de bedrijfsprocessen.

Onze observaties en aanbevelingen koppelen we in dit hoofdstuk aan de gemeente terug.

2. Kwaliteit interne beheersing

2.1 Algemeen

Onderwerp	Omschrijving
Doel en reikwijdte	Het doel van onze jaarrekeningcontrole is het vormen van een oordeel over de getrouwheid van de jaarrekening als geheel, zoals bedoeld in het Besluit Accountantscontrole Decentrale Overheden (BADO). In het kader van de jaarrekeningcontrole beoordelen wij de kwaliteit van de administratieve organisatie en interne beheersing, voor zover deze relevant is voor onze oordeelsvorming. Wij geven hierover geen zelfstandig oordeel. 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.
Kernpunten in de controle	Op basis van onze kennis van de gemeente Oss worden de belangrijkste specifieke risico's in kaart gebracht, die mogelijk een afwijking van materieel belang veroorzaken in de jaarrekening van de gemeente Oss. Onze controlewerkzaamheden richten zich op de jaarrekeningposten, schattingen, processen en transacties met naar ons oordeel het grootste risico op een afwijking van materieel belang in de financiële overzichten, door fouten of fraude. We houden hierbij rekening met de effecten van de huidige risicofactoren in de sector en leggen ook de nadruk op die gebieden die door het management subjectieve beslissingen vereisen. We houden tijdens onze controle voortdurend aandacht voor wijzigingen van interne en externe factoren die onze initiële risico-inschatting kunnen beïnvloeden.

2. Kwaliteit interne beheersing

2.1 Algemeen

Onderwerp	Omschrijving
Onze risicoanalyse	De belangrijkste bij de gemeente Oss onderkende risico's / kernpunten in de controle zijn, zoals ook in ons audit plan zijn opgenomen: • Risico dat het management van de gemeente de procesafspraken doorbreekt (management override of controls), hetgeen een standaardrisico is vanuit onze beroepsregels. Dit risico ziet bij uw gemeente met name toe op de schattingsposten in de grondexploitaties en voorzieningen; • Waardering van de activa (waaronder o.a. terreinen, panden en grondexploitaties incl. strategische gronden); • Het op marktconforme wijze tot stand komen van significante grond aan- en verkopen (dit gezien de mogelijke mate van subjectiviteit bij het aangaan van dit soort overeenkomsten en wanneer dit zich voordoet bij materiële posities); • Onterechte betalingen waardoor de lasten ten onrechte zijn verantwoord; • Getrouwheid van de rechtmatigheidsverantwoording; • Nauwkeurigheid van de lasten (bedrijfskosten en lasten sociaal domein) in relatie tot het juist beoordelen van de prestatielevering. In ons verslag van bevindingen rapporteren wij naar aanleiding van de jaarrekeningcontrole over bovenstaande punten.

2. Kwaliteit interne beheersing

2.2 Algemeen beeld

Onderwerp	Omschrijving
Interne beheersing is op orde	In lijn met voorgaande jaren constateren wij dat de interne beheersing, inclusief de IT-beheersing, in belangrijke mate op orde is. Daarbij zien wij dat de organisatie blijvend investeert in het verder verbeteren en professionaliseren van haar processen. Een voorbeeld hiervan is de verdere optimalisatie van het inkoopproces, waarbij nadrukkelijker aandacht wordt besteed aan het meer aan de voorkant vastleggen van verplichtingen. Enerzijds helpt dit in het versterken van het begrotingsbeheer, anderzijds kan dit helpen de dossiervorming rondom het inkoopproces te versterken. Ten aanzien van dit laatste constateren we dat vanuit de verbijzonderde interne controle wordt geconstateerd dat documentatie ter onderbouwing van de prestatielevering nog niet in alle gevallen op een eenduidige wijze wordt vastgelegd en opgeslagen. Hierdoor kost het bij interne en externe controles relatief veel inspanning om de benodigde onderbouwing te achterhalen. Eenzelfde aandachtspunt geldt voor de gedocumenteerde vastlegging van de inkoopkeuze. Uit de interim-werkzaamheden is daarnaast gebleken dat er in 2026 een onterechte en foutieve personeelsdeclaratie is uitbetaald. De organisatie heeft dit achteraf op aangeven van de collega ontdekt. Naar aanleiding hiervan zijn acties geformuleerd om herhaling te voorkomen. Gezien de gemaakte afspraken en onze ervaringen uit het verleden, leiden deze bevindingen niet tot aanvullende aandachtspunten richting de jaarrekeningcontrole. Op het gebied van IT zien we dat gemeente Oss beheersing steeds meer vanuit een integrale blik wordt vormgegeven. Daarbij ligt met name focus op het stroomlijnen van IT en beheersing in samenhang met de digitaliseringsstrategie en het versterken van de gesignaleerde noodzakelijke verbeteringen ten aanzien van de nieuw geïntroduceerde Cyberbeveiligingswet (zie hierover ook de paragraaf Actualiteiten). Met de introductie van het nieuwe personeelssysteem AFAS kon ook een nieuwe stap gezet worden op het gebied van het beheersen van personeelsmutaties binnen de IT systemen in het Identity en Access Management. We hebben ten aanzien van de interne beheersing rondom deze applicatie beperkte aanbevelingen. Onze aanbevelingen in deze managementletter zien dan ook met name toe op het verder aanscherpen en optimaliseren van de processen.

2. Kwaliteit interne beheersing

2.3 IT General controls - Detailbevindingen

Applicatie	Toegangsbeveiliging		Wijzigingsbeheer	Continuïteit	Belangrijkste bevindingen en gevolgen voor de controle
	Authenticatie	Autorisatie			
Netwerk	O	A	N.v.t.	O	Gevolgen voor de controle zijn beperkt. Enkele aanbevelingen, waaronder periodiek beoordelen functie-autorisatiematrix blijven relevant.
Centric Financiën (voorheen Key2Financiën)	O	A	O	O	Rechten worden nog niet periodiek beoordeeld aan de hand van een functie-autorisatiematrix.
Suites voor het Sociaal Domein	O	A	O	O	Rechten worden nog niet periodiek beoordeeld aan de hand van een functie-autorisatiematrix.
AFAS	O	G	O	O	Pakket is nieuw geïntroduceerd. Rechten niet beperkt tot onafhankelijke functionarissen. Rechten worden nog niet periodiek beoordeeld aan de hand van een functie-autorisatiematrix.

Eventuele adviespunten zijn opgenomen in de bijlage. Ten opzichte van voorgaand jaar constateren we eenzelfde beeld waarbij aan de slag is gegaan met het doorvoeren van onze adviespunten.

O Op orde A Adviespunt G Verbetering nodig

2. Kwaliteit interne beheersing

2.4 Kwaliteit van Verbijzonderde interne controle

Een belangrijk onderdeel van de interne beheersing is de (verbijzonderde) interne controlefunctie (VIC). Binnen gemeente Oss is de VIC-functie op een goede wijze ingericht. Er is sprake van een gedegen controleaanpak en de controle wordt op een professionele wijze uitgevoerd.

Voor het boekjaar 2026 delen wij onze observaties en aanbevelingen aan de hand van 10 punten:

G	1. Het intern controleplan is formeel vastgesteld, actueel en afgestemd op de risico's en doelstellingen van de gemeente
T	2. Het normenkader is voor 2026 geactualiseerd en sluit aan bij relevante wet- en regelgeving
G	3. Het normenkader is uitgewerkt in een concreet werkprogramma met toetsingscriteria en controlewerkzaamheden
T	4. De VIC-werkzaamheden zijn tijdig en volgens planning uitgevoerd
T	5. De controlewerkzaamheden zijn onderbouwd met voldoende, relevante en betrouwbare informatie, inclusief een duidelijk controlespoor.
T	6. Er is sprake van een duidelijke conclusie waarbij hoor- en wederhoor is toegepast
T	7. De VIC-rapportages en bevindingen zijn besproken in het MT/directieoverleg en Auditcommissie
T	8. Er is aantoonbare opvolging van bevindingen, inclusief acties, verantwoordelijken en deadlines
T	9. Fouten worden geëvalueerd op impact (financieel en procesmatig), met waar nodig uitbreiding van controlewerkzaamheden
V	10. IT-controles zijn geïntegreerd in VIC, inclusief beoordeling van de betrouwbaarheid van lijstwerk en impact van IT-gerelateerde bevindingen

V Voor verbetering vatbaar T Toereikend G Good practice

2. Kwaliteit interne beheersing

2.5 Kwaliteit van Verbijzonderde interne controle

Wij constateren dat de verbijzonderde interne controle (VIC) binnen de gemeente Oss op een professionele en gestructureerde wijze is ingericht. We zien daarbij op een beperkt aantal vlakken kansen om de VIC nog verder te optimaliseren.

We constateren dat de werkzaamheden van de VIC momenteel worden uitgevoerd op basis van een goedkeuringstolerantie van zowel 1% als 2%. Gezien de verruiming van de verantwoordingsgrenzen in het Besluit Accountantscontrole Decentrale Overheden (BADO) voorgaand boekjaar kan worden overwogen de controleaanpak hierop aan te passen voor alle processen. Een keuze om de 1%-norm te blijven hanteren kan overigens wel leiden tot een scherpere sturing op de inrichting en naleving van processen wordt behouden en eventuele afwijkingen eerder zichtbaar worden, doordat met een grotere diepgang gecontroleerd wordt (voor bijvoorbeeld instanties als de Belastingdienst). Wij adviseren u wel om de keuze van de goedkeuringstolerantie te verankeren in het controleplan.

Voor een doelmatige inzet van de werkzaamheden van de Verbijzonderde Interne Controle (VIC) binnen de accountantscontrole is het van belang dat de samenstelling van de gecontroleerde transacties (de zogenoemde stratificatie) zoveel mogelijk aansluit bij de uitgangspunten die de accountant hanteert bij de controle van de jaarrekening. Met stratificatie wordt bedoeld dat transacties worden onderverdeeld in logisch samenhangende groepen met een vergelijkbaar karakter en risicoprofiel.

Wij constateren dat de organisatie dit aandachtspunt onderkent en dat reeds stappen worden gezet om de aansluiting tussen de VIC en de accountantscontrole verder te verbeteren. Hierbij vindt actief afstemming plaats tussen de organisatie en de accountant. Wij adviseren deze ontwikkeling

2. Kwaliteit interne beheersing

2.5 Kwaliteit van Verbijzonderde interne controle

voort te zetten, zodat de uitgevoerde VIC-werkzaamheden optimaal kunnen worden benut binnen de accountantscontrole en aanvullende werkzaamheden zoveel mogelijk kunnen worden beperkt.

De gemeente heeft de VIC in het afgelopen jaar met name ingezet op thema's zoals de toepassing van AI, verdere doorontwikkeling met betrekking tot data-analyse en andere controletechnieken zouden we toejuichen. Daarnaast is de gemeente voornemens om gerichte themaonderzoeken uit te voeren, waarmee aanvullende inzichten worden verkregen in de beheersing van risico's en processen. We kunnen ons voorstellen dat een toenemende focus op IT, waardering grondexploitaties, begrotingsbeheer en grote projecten onderwerpen zouden kunnen zijn waar de VIC een versterkende rol kan pakken.

Wij constateren dat de VIC in sommige gevallen de nodige inspanningen moet verrichten om de vereiste onderbouwingen en bewijsstukken beschikbaar te krijgen. Dit onderstreept het belang van een kritische beoordeling door de VIC van zowel de opzet als de uitvoering van de interne beheersingsmaatregelen. Indien controles onvoldoende diepgaand worden uitgevoerd of de vastlegging van de uitgevoerde werkzaamheden ontoereikend is, beperkt dit de mate waarin op de werkzaamheden van de VIC kan worden gesteund in het kader van de jaarrekeningcontrole. Wij adviseren daarom om blijvend aandacht te besteden aan zowel de kwaliteit van de documentatie als de diepgang van de uitgevoerde controles, zodat de toegevoegde waarde van de VIC optimaal kan worden benut.

2. Kwaliteit interne beheersing

2.6 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. Op basis van onze uitgevoerde interim-controle stellen wij vast dat er binnen de gemeente voldoende aandacht is voor frauderisico's en de preventie daarvan. Voor het boekjaar 2026 delen wij onze observaties en aanbevelingen aan de hand van 7 punten:

V	1. Er is een integrale fraude-risicoanalyse opgesteld waarin het misbruik- en oneigenlijk gebruikbeleid (M&O) en corruptierisico's expliciet zijn meegenomen.
T	2. Bij elk onderkend frauderisico is een inschatting gemaakt van de waarschijnlijkheid van optreden en de potentiële impact (financieel, reputatie, juridisch, externe signalen).
T	3. Er is overzichtelijk vastgelegd welke interne beheersingsmaatregelen reeds zijn getroffen om de geïdentificeerde frauderisico's te beperken.
T	4. De gemeente heeft haar risicobereidheid en wijze van omgaan met frauderisico signalen beschreven in een vastgesteld (fraude)risicobeleid.
T	5. Er is expliciete aandacht voor soft controls zoals integriteitscultuur, voorbeeldgedrag, training en bewustwording, open communicatie en ethisch leiderschap als onderdeel van fraudepreventie.
T	6. De gemeente beschikt over actueel beleid en regelingen ter bevordering van integriteit, waaronder een klokkenluidersregeling en een nota integriteit.
V	7. De gemeente beschikt over een adequaat frauderesponseplan.

V Voor verbetering vatbaar T Toereikend G Good practice

2. Kwaliteit interne beheersing

2.6 Frauderisicoanalyse

Wij constateren dat de gemeente beschikt over een interne frauderisicoanalyse. Daarbij merken wij op dat deze analyse voor het laatst in 2024 is geactualiseerd. Gezien de dynamische omgeving waarin gemeenten opereren en de toenemende dreigingen van fraude van buitenaf, achten wij het van belang dat periodiek wordt beoordeeld of de geïdentificeerde frauderisico's nog actueel en toereikend zijn. Wij adviseren u daarom om jaarlijks vast te stellen dat de frauderisicoanalyse aansluit bij de actuele ontwikkelingen, werkzaamheden en risico's van de gemeente.

Daarnaast merken wij op dat het niet de vraag is óf, maar wanneer een organisatie wordt geconfronteerd met een fraude-incident. Tegen deze achtergrond adviseren wij u nadrukkelijk om te beschikken over een overkoepelend frauderesponseplan. Hiermee wordt geborgd dat bij signalen of vermoedens van fraude tijdig en eenduidig wordt gehandeld, waarbij duidelijk is welke maatregelen moeten worden getroffen en welke verantwoordelijkheden binnen de organisatie gelden. We constateren dat de gemeente Oss ten aanzien van integriteitskwesties en cybersecurity al veel doet in het kader van frauderesponse, maar wij adviseren dit om in het verlengde van de frauderisicoanalyse specifiek op meer vlakken aandacht te geven en in bredere zin op te volgen. Voor nadere concrete handvaten verwijzen we naar de communicatie hieromtrent van de NBA.

Management samenvatting

Kwaliteit interne Beheersing & IT

Voorbereiding jaarrekeningcontrole

Actualiteiten

Bijlagen

Voorbereiding jaarrekeningcontrole

Om aan uw behoeften te kunnen voldoen en om het proces voor de jaareinde controle efficiënt te laten verlopen vinden wij het belangrijk om vooraf afspraken te maken, het proces regelmatig te evalueren en onze bevindingen met u te delen. Om achteraf verrassingen te voorkomen willen wij de volgende werkafspraken met u maken.



3. Voorbereiding jaarrekeningcontrole

3.1 Voorbereiding jaarrekeningcontrole

Wij starten met de jaarrekeningcontrole op 1 maart 2027 (week 9). In het najaar van 2026 halen wij detailwerkzaamheden naar voren, om op deze wijze de belasting voor uw organisatie en onze organisatie in het voorjaar te verminderen. Specifieke aandachtspunten die bijdragen aan een soepele controle voor 2026 hebben wij in onderstaande tabel samengevat. Dit zijn aandachtsgebieden voor de jaarrekeningcontrole, niet zo zeer dat deze onderwerpen niet bij de organisatie bekend zijn, maar meer als aandachtspunten om samen tot een soepele jaarrekeningcontrole te komen.

Onderwerp	Toelichting	Actie
Onze afspraken	In juli 2026 hebben wij gezamenlijk de jaarrekeningcontrole 2025 geëvalueerd. Behoudens enkele aandachtspunten voor beide partijen hebben wij (gelijk aan voorgaande jaren) geconcludeerd dat de controle over het boekjaar 2025 soepel en plezierig is verlopen. De gemaakte afspraken zien toe op een verdere ontwikkeling in de samenwerking.	n.v.t.
Opvolging van bevindingen	Bij de uitvoering van de verbijzonderde interne controle dient toenemende aandacht te worden besteed aan de samenstelling van de controlemassa's en de aard van de daarin opgenomen transacties. Daarbij is het van belang dat transacties met een verschillend risicoprofiel en een afwijkende controleaanpak, zoals subsidieverstrekkingen en reguliere inkoopuitgaven, op passende wijze worden onderscheiden. Een zorgvuldige afstemming van de gehanteerde indeling op de controleaanpak van de accountant draagt bij aan een betere aansluiting tussen de VIC-werkzaamheden en de accountantscontrole, waardoor de noodzaak van aanvullende controlewerkzaamheden kan worden beperkt.	We verwachten van de gemeente dat zichtbaar opvolging gegeven is aan dit advies en dat de gehanteerde populaties zichtbaar aansluiten op de jaarrekening.
SiSa-regelingen	Gezien de grote hoeveelheid SiSa-regelingen vragen wij u tijdig te inventariseren welke regelingen van toepassing zijn en welke informatie hiervoor nodig is. Tevens vragen we aandacht om voldoende kritisch door de interne oplevering heen te gaan alvorens dit wordt aangeleverd aan ons. Hierbij vragen we u ook tijdig contact te leggen met de subsidieverstrekker bij wijzigingen binnen de projecten, zodat onduidelijkheden vooraf met de belangrijkste stakeholder zijn afgestemd.	Aanleggen van consistente balansdossiers met betrekking tot de SiSa oplevering.

3. Voorbereiding jaarrekeningcontrole

Waardering activa

In het kader van onze tussentijdse controle, onze aanbevelingen vanuit voorgaande jaren en het feit dat de waardering van de grondexploitaties een significant risico voor onze jaarrekeningcontrole is, hebben wij aan de hand van het concept najaarsbericht uw planeconomen gesproken. Wij hebben enerzijds 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.

In lijn met voorgaande jaren constateren wij dat de kwaliteit van de totstandkoming van de rapportages verder is verbeterd. Daarnaast stellen wij vast dat aanbevelingen uit eerdere rapportages proactief worden opgepakt. Wel merken wij op dat de zichtbaarheid van de aanvullend uitgevoerde checks and balances nog beperkt is. Hierdoor ontstaat de indruk dat de getroffen maatregelen een relatief vrijblijvend karakter hebben.

Wij adviseren daarom om het proces rondom de totstandkoming van het najaarsbericht en het meerjarenperspectief (MJP), als onderdeel van de jaarrekeningcyclus, verder te formaliseren en te beschrijven. Daarbij verdient het aanbeveling expliciet aandacht te besteden aan de relevante interne beheersingsmaatregelen, zodat zichtbaar wordt dat deze beheersingsmaatregelen daadwerkelijk worden uitgevoerd, gemonitord en vastgelegd. De Verbijzonderde Interne Controle (VIC) kan hierbij een toetsende en signalerende rol vervullen.

Daarnaast blijven we aandacht vragen voor de optimistische inschattingen qua timing ten aanzien van de kosten en opbrengsten. We vragen u bij de actualisering van de grondexploitaties bij de jaarrekening 2026 wederom voor dit aspect extra aandacht te hebben. Met name op die projecten waar vertraging door externe factoren, zoals lopende procedures, van toepassing kan zijn.

Ook hebben we stilgestaan bij de onderbouwing van de waardering van de “warme” gronden. Dit betreffen de in het verleden strategisch aangekochte grondposities voor onder andere Amsteleind. De regelgever stelt dat deze gronden, zo ver deze nog niet zijn ingebracht in een grondexploitatie, periodiek (minimaal eens in de 2 jaar) worden getaxeerd. Deze taxatie dient tegen de waarde volgens de toekomstige bestemming, met inachtneming van de inherente onzekerheden van de ontwikkelmogelijkheden te gebeuren.

Management samenvatting

Kwaliteit interne Beheersing & IT

Voorbereiding Jaarrekeningcontrole

Actualiteiten

Bijlagen

Actualiteiten



4. Actualiteiten

Cash Compensation Model (CCM)

Het Cash Compensation Model (CCM) is een door opsporingsdiensten en toezichthouders onderkende witwasconstructie waarbij crimineel contant geld wordt omgezet in giraal geld via schijnbaar legitieme zakelijke transacties. Hierbij ontvangen ondernemingen met een behoefte aan contant geld, bijvoorbeeld voor niet-geregistreerde loonbetalingen, contanten van derden en compenseren zij dit door middel van girale betalingen op basis van gefingeerde facturen. Deze constructie kan verband houden met witwassen, belastingfraude, arbeidsuitbuiting en verstoring van eerlijke marktwerking.

Voor een gemeente is het risico doorgaans niet gelegen binnen de eigen financiële administratie of jaarrekening, maar in de leveranciers- en aannemersketen. Met name bij arbeidsintensieve activiteiten, zoals infrastructurele projecten, onderhoudswerkzaamheden en de inzet van onderaannemers, bestaat het risico dat betrokken partijen gebruikmaken van dergelijke constructies. Indien gemeentelijke middelen indirect terechtkomen bij partijen die betrokken zijn bij witwassen of fraude, kan dit leiden tot integriteitsrisico's, reputatieschade en mogelijke financiële of juridische consequenties voor de gemeente.

Wij onderkennen dat de gemeente reeds maatregelen heeft ingericht op het gebied van aanbesteding, contractbeheer en integriteitsbewaking van leveranciers.
Tegen de achtergrond van de toenemende aandacht van opsporingsdiensten en toezichthouders voor het Cash Compensation Model achten wij het echter van belang dat binnen deze bestaande processen blijvend aandacht bestaat voor signalen die kunnen wijzen op verhoogde integriteits- of witwasrisico's binnen de leveranciers- en onderaannemersketen.

In dat kader kan de gemeente periodiek beoordelen of de huidige beheersmaatregelen voldoende aansluiten bij de risico's binnen de leverancierskete ten. Daarbij kan specifiek aandacht worden besteed aan signalen van arbeidsuitbuiting, fiscale fraude of onverklaarbare geldstromen bij contractpartijen en, waar passend, gebruik worden gemaakt van het Bibob-instrumentarium. Daarnaast kunnen due diligence-maatregelen bij aanbestedingen en gedurende de contractperiode bijdragen aan het tijdig identificeren van verhoogde risico's. Op deze wijze wordt de kans beperkt dat publieke middelen direct of indirect bijdragen aan frauduleuze of criminele activiteiten.

4. Actualiteiten

Schending mededingingseis bij begrotingssubsidies

De uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 23 juli 2025 heeft belangrijke gevolgen voor de wijze waarop gemeenten begrotingssubsidies verstrekken. Uit deze uitspraak volgt dat een begrotingssubsidie onder omstandigheden kan worden aangemerkt als een schaars publiek recht. Wanneer meerdere organisaties in aanmerking kunnen komen voor het uitvoeren van een gesubsidieerde activiteit, dient de gemeente een transparante procedure te organiseren waarbij gelijke kansen worden geboden aan potentiële gegadigden. Alleen wanneer objectief en toetsbaar kan worden onderbouwd dat sprake is van slechts één serieuze gegadigde, kan van een openbare selectieprocedure worden afgezien.

Voor u betekent dit dat bestaande en toekomstige subsidierelaties kritisch moeten worden beoordeeld. Het risico bestaat dat subsidies die rechtstreeks aan één organisatie zijn verstrekt zonder voorafgaande mededinging juridisch kwetsbaar zijn. In dergelijke situaties kunnen bezwaar- en beroepsprocedures ontstaan, met mogelijke gevolgen voor de rechtmatigheid van subsidiebesluiten, financiële risico's en reputatieschade.

Het is belangrijk vooraf een expliciete schaarstetoets uit te voeren om vast te stellen of meerdere partijen de betreffende activiteit zouden kunnen uitvoeren. Op basis van deze toets moet worden bepaald of een openbare verdelingsprocedure noodzakelijk is. Daarnaast moet het juridische kader, waaronder de Algemene Subsidieverordening (ASV), beleidsregels en eventuele nadere subsidieregels, voldoende aansluiten op de eisen die voortvloeien uit de actuele jurisprudentie. Geadviseerd wordt om deze beoordeling structureel te verankeren in de planning- en controlcyclus en het reguliere subsidieproces.

Indien een mogelijke schending wordt geconstateerd, is een gestructureerde aanpak noodzakelijk. De eerste stap bestaat uit het identificeren van risicovolle subsidies en het uitvoeren van een juridische, financiële en bestuurlijke risicoanalyse. Vervolgens dient de gemeente te voorkomen dat vergelijkbare situaties zich opnieuw voordoen door nieuwe subsidiebesluiten te onderwerpen aan een expliciete toets op schaarste en mededinging. Daarnaast is het van belang bestaande subsidierelaties te inventariseren en te classificeren naar risico.

Voor subsidies waarbij een verhoogd risico wordt vastgesteld, zijn verschillende herstelstrategieën mogelijk. Indien aannemelijk kan worden gemaakt dat slechts één serieuze gegadigde bestaat, kan dit alsnog gemotiveerd en openbaar worden gemaakt. Wanneer meerdere partijen in aanmerking kunnen

4. Actualiteiten

komen, verdient een open en transparante selectieprocedure de voorkeur. In situaties waarin het oorspronkelijke besluit ernstige gebreken vertoont, kan intrekking of heroverweging van het subsidiebesluit noodzakelijk zijn. Daarbij dient aandacht te worden besteed aan een zorgvuldige overgangsregeling voor bestaande subsidieontvangers en de continuïteit van maatschappelijke voorzieningen.

Vanuit governance- en rechtmatigheidsperspectief vraagt dit onderwerp niet uitsluitend om juridische correcties, maar ook om bestuurlijke sturing en structurele procesverbetering. Het actualiseren van regelgeving, het inrichten van standaard werkprocessen, het opnemen van een verplichte schaarstetoets en het vergroten van de bewustwording binnen de organisatie zijn daarbij essentiële randvoorwaarden. Door deze maatregelen tijdig te treffen kunt u het risico op onrechtmatige subsidieverstrekking beperken en beter invulling geven aan de beginselen van transparantie, gelijke behandeling en rechtmatige besteding van publieke middelen.

We hebben begrepen dat mede naar aanleiding van deze ontwikkeling de organisatie druk doende is het subsidiebeleid te herzien en de processen te borgen in een nieuw in te richten subsidiesysteem.

Overdracht Appa-pensioenen naar ABP

Het kabinet heeft een wetsvoorstel gepubliceerd waarbij de pensioenverplichtingen van politieke ambtsdragers op grond van de Appa, waaronder wethouders, met ingang van 1 januari 2028 worden ondergebracht bij het ABP. Onderdeel van dit voorstel betreft een compensatieregeling voor politieke ambtsdragers die als gevolg van de overgang naar het nieuwe pensioenstelsel nadeel ondervinden. Op basis van de huidige inzichten geldt deze regeling naar verwachting voor ambtsdragers die op 31 december 2027 een leeftijd hebben tussen 40 en 68 jaar en op dat moment nog in functie zijn. Aangezien binnen de Appa-regeling geen collectieve buffer aanwezig is om deze compensatie te financieren, bestaat het risico dat de hiermee samenhangende lasten voor rekening komen van gemeenten en andere overheidsorganisaties.

Wij adviseren de gemeente om tijdig in overleg te treden met de actuaris die verantwoordelijk is voor de actualisatie van de Appa-voorziening, teneinde inzicht te verkrijgen in de mogelijke financiële gevolgen van de voorgestelde compensatieregeling. Op basis van deze analyse kan worden beoordeeld of en in hoeverre een aanvullende dotatie aan de Appa-voorziening in de jaarrekening 2026 noodzakelijk is. Voor zover de financiële gevolgen op balansdatum nog onvoldoende kunnen worden vastgesteld, adviseren wij de hieraan verbonden onzekerheden adequaat toe te lichten in de jaarrekening.

4. Actualiteiten

Opbrengstgenererende vastgoedinvesteringen binnen grondexploitaties
De Commissie BBV heeft in mei 2026 een nadere toelichting gepubliceerd over de verwerking van vastgoedinvesteringen binnen grondexploitaties die opbrengsten kunnen genereren en in de toekomst mogelijk kunnen worden verkocht. Hierbij kan worden gedacht aan parkeergarages, parkeerhubs of vastgoed dat in het kader van een gebiedsontwikkeling wordt aangekocht en een zelfstandige economische waarde behoudt.

De Commissie BBV benadrukt dat gemeenten voor deze investeringen verschillende verwerkingsmogelijkheden hebben. Enerzijds kunnen deze investeringen worden opgenomen binnen de grondexploitatie (grex). Anderzijds kunnen zij worden geactiveerd als materiële vaste activa en vervolgens via afschrijvingen en rentelasten gedurende de gebruiksperiode ten laste van de exploitatie worden gebracht. De commissie spreekt daarbij een voorkeur uit voor volledige activering, omdat dit leidt tot stabielere en beter voorspelbare lasten in begroting en jaarrekening.

Daarnaast heeft de Commissie BBV verduidelijkt dat opbrengstgenererende vastgoedinvesteringen slechts beperkt binnen een grondexploitatie mogen worden opgenomen.

Indien opname van deze investeringen zou leiden tot een verliesgevende grondexploitatie, mag uitsluitend dat deel van de investering in de grondexploitatie worden verwerkt dat past binnen het positieve resultaat van de grex. Het resterende deel dient als materieel vast actief te worden geactiveerd. Ook dient deze afweging jaarlijks opnieuw te worden gemaakt bij actualisatie van de grondexploitatie, totdat de betreffende investering in gebruik is genomen.

Deze verduidelijking kan met name relevant zijn voor gemeenten die binnen gebiedsontwikkelingen investeren in voorzieningen met een zelfstandig opbrengstpotentieel, zoals parkeervoorzieningen of ander vastgoed dat later kan worden geëxploiteerd of verkocht. De nieuwe richtlijn kan gevolgen hebben voor de wijze waarop dergelijke investeringen worden verwerkt en voor de presentatie van resultaten binnen grondexploitaties.

Wij adviseren de gemeente om na te gaan of binnen lopende en toekomstige grondexploitaties sprake is van dergelijke opbrengstgenererende vastgoedinvesteringen en te beoordelen of de huidige verwerking en het gemeentelijk beleid aansluiten bij de per begrotingsjaar 2027 in werking tredende aanbeveling en stellige uitspraak van de Commissie BBV. Hiermee wordt het risico beperkt dat de verwerking van deze investeringen niet volledig in overeenstemming is met de actuele BBV-richtlijnen.

4. Actualiteiten

Zoals reeds tijdens onze interim-controle en door de gemeente zelf is gesignaleerd, is bij het recent in exploitatie genomen project Raadhuislaan-Zuid een vastgoedinvestering in de vorm van een parkeergarage toegerekend aan een verlieslatende grondexploitatie. Naar aanleiding van de in mei 2026 door de Commissie BBV gepubliceerde nadere toelichting op opbrengstgenererende vastgoedinvesteringen en de daaropvolgende verduidelijking van door de gemeente gestelde vragen, is gebleken dat deze verwerkingswijze onder de actuele BBV-richtlijnen niet langer mogelijk is. Indien sprake is van een opbrengstgenererende vastgoedinvestering die een zelfstandige waarde vertegenwoordigt, dient het deel dat niet binnen een ten minste kostendekkende grondexploitatie kan worden verwerkt als materieel vast actief te worden geactiveerd.

Het college heeft in het Najaarsbericht Grondbedrijf reeds aangegeven dat de financiële gevolgen van deze gewijzigde duiding zullen worden betrokken bij de actualisatie van de grondexploitaties ten behoeve van de jaarrekening 2026. Wij begrijpen dat bij de behandeling van de begroting de financiële dekking wordt herijkt en de dat de administratieve verwerking bij de jaarrekening mee wordt genomen.

4. Actualiteiten

Cyberbeveiligingswet (CBW)

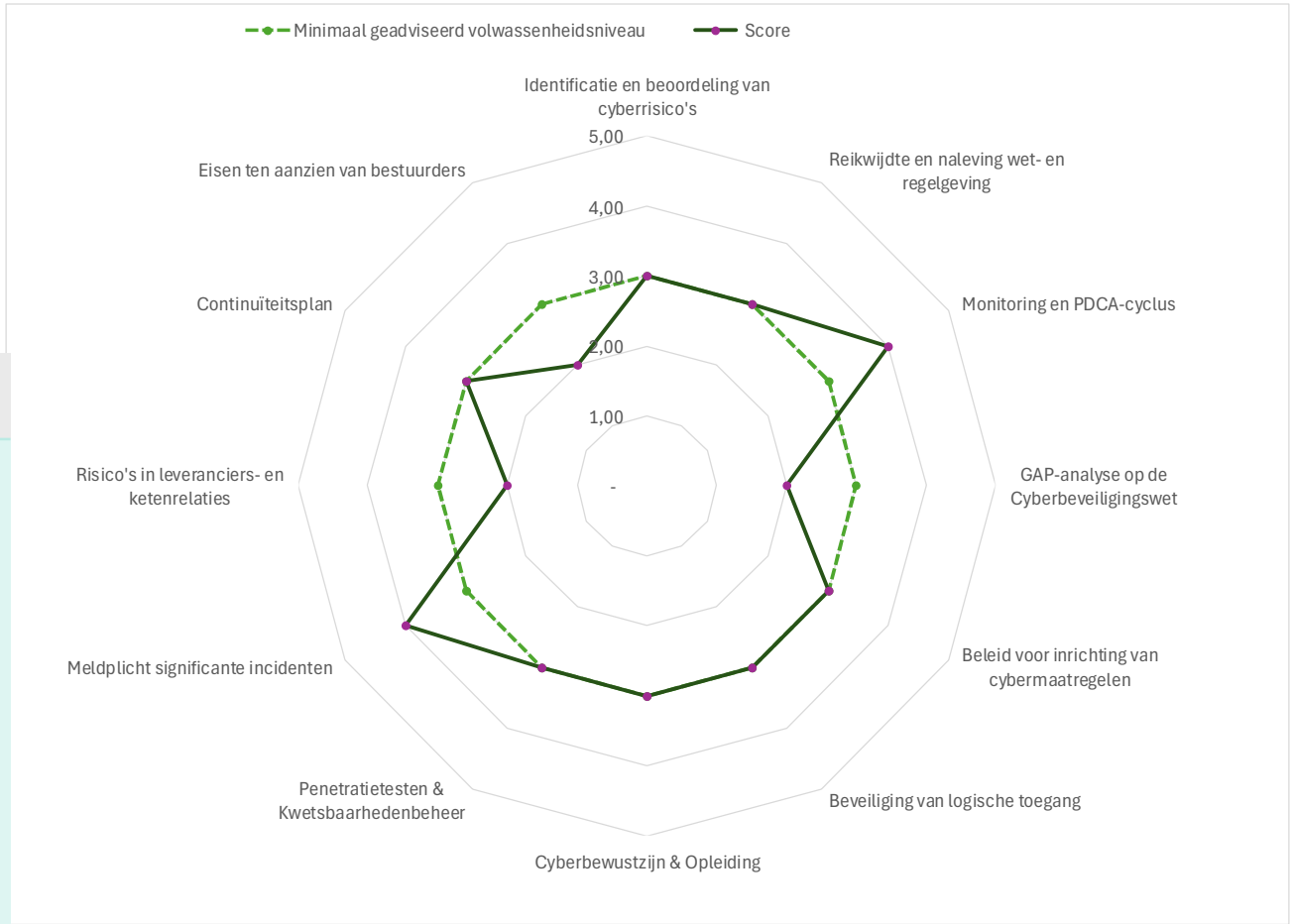
In het kader van onze jaarlijkse IT-audit hebben wij een oriënterende quick scan uitgevoerd op de mate waarin uw organisatie is voorbereid op de verplichtingen van de Cyberbeveiligingswet (Cbw), de Nederlandse implementatie van de Europese NIS2-richtlijn.

Wij hebben twaalf kernthema's geïdentificeerd. Op basis van een vragenlijst en verkregen inlichtingen hebben wij de antwoorden ingeschaald op een volwassenheidsniveau van 1 (initieel) tot 5 (geoptimaliseerd). De resultaten bieden een eerste inzicht in uw huidige positie ten opzichte van het minimaal geadviseerde volwassenheidsniveau van 3.

Belangrijkste observaties: Uw organisatie scoort op het gewenste volwassenheidsniveau

- ✓ Gemeente Oss heeft in vergelijking met vergelijkbare organisaties een relatief goed basisniveau als het gaat om informatiebeveiliging. Ten opzichte van de Cyberbeveiligingswet zijn er nog wel stappen te zetten.
- ✓ De basis voor informatiebeveiliging en risicobeheersing is aanwezig, met vastgesteld strategisch beleid, tactische beleidsstukken en periodieke monitoring via ENSIA.
- ✓ De gemeente is zich bewust van de verplichtingen vanuit de CBW en werkt actief aan de verdere invulling hiervan; een formele GAP-analyse moet echter nog worden uitgevoerd.
- ✓ Verdere aandacht is met name nodig voor leveranciers- en ketenrisico's, cyberbewustzijn, de structurele planning van penetratietesten en kwetsbaarheidsscans en de verdere uitwerking van continuïteitsplannen.
- ✓ In november staat een training gepland om bestuurders en management van verdere informatie over de wetgeving en Cyber Security te voorzien.

Volwassenheidsoverzicht: Cbw-scan Gemeente Oss



Management Samenvatting
Kwaliteit interne Beheersing & IT
Voorbereiding Jaarrekeningcontrole
Actualiteiten
Bijlagen

Bijlagen

5. Bijlagen

Detailbevindingen interne beheersing – Toegangsbeveiliging netwerk

	Authenticatie	Autorisatie
Constatering	De wachtwoordinstellingen zijn van voldoende niveau om op de authenticatie van de gebruikers te kunnen steunen. We hebben geconstateerd dat 138 actieve accounts geen verlopend wachtwoord hebben, dat zijn er 37 minder dan voorgaand jaar. Het betreft met name service-accounts, mailboxen en tv schermen. Eén gebruikersaccount van een IT medewerker heeft een niet verlopend wachtwoord, maar heeft dit wachtwoord wél gewijzigd gedurende 2026 en vormt daarmee geen aanvullend risico. Twee-factor authenticatie wordt afgedwongen.	Er is geen functie-autorisatiematrix opgesteld waarmee gebruikers en rechten periodiek worden beoordeeld, wel is in software ingericht welke applicaties toegekend worden per rol. We hebben vernomen dat automatisch toegangsbeheer tot applicaties voor financiële applicaties (nog) niet in gebruik is. De hoge rechten in de Active Directory zijn beperkt tot onafhankelijke functionarissen in het kader van de jaarrekeningcontrole. Er wordt gebruik gemaakt van een gestructureerde procedure van het instroom, doorstroom en uitstroom proces, ondersteund door grote mate van automatisering.
Risico	Gezien de aard van deze accounts (service-accounts, mailboxen, tv-schermen), achten wij het risico daarvan laag.	Door het ontbreken van een functie-autorisatiematrix en een periodieke controle op de inrichting van rollen en rechten, is er verminderde zekerheid dat gebruikers alleen toegang hebben tot rollen en rechten die behoren tot de functiegroep.
Aanbeveling	Wij zien dat u generieke gebruikersnamen verder beperkt heeft en adviseren periodiek te overwegen niet herleidbare netwerkgebruikers verder te beperken.	Wij moedigen de ontwikkeling van een technische en functionele oplossing van beheer tot toegang tot de applicaties aan.
Gevolgen voor de jaarrekening-controle	De accounts met niet-verlopende wachtwoorden hebben nagenoeg geen impact op de relevante applicaties voor de jaarrekeningcontrole. Wij steunen in de controle niet op beheersmaatregelen die leunen op de ingerichte autorisaties op netwerkniveau.	

5. Bijlagen

Detailbevindingen interne beheersing – Toegangsbeveiliging Centric Financiën

	Authenticatie	Autorisatie
Constatering	Er is geconstateerd dat wordt ingelogd middels Single Sign-On (SSO). Hierbij gelden de wachtwoordinstellingen van het netwerk. Deze zijn van voldoende niveau. Er zijn serviceaccounts actief in de applicatie waarvan het wachtwoord op netwerk-niveau niet verloopt. Deze serviceaccounts beschikken in de applicatie niet over rechten. Eén gebruikersaccount van een IT medewerker heeft een niet verlopend wachtwoord, maar heeft dit wachtwoord wél gewijzigd gedurende 2026 en vormt daarmee geen aanvullend risico.	Binnen de applicatie hebben wij 2 gebruikers met hoge rechten geïdentificeerd. Dit zijn onafhankelijke functionarissen in het kader van de jaarrekeningcontrole. Er wordt een periodieke controle uitgevoerd op gebruikers en rechten. Hierbij wordt geen functie-autorisatiematrix gebruikt, er wordt op basis van professional judgement een beoordeling gemaakt op de rechten. Toegang tot Centric Financiën is via gescheiden aanvraagprocedures van overige applicaties ingericht.
Risico	Accounts waarvan wachtwoorden niet verlopen zijn kwetsbaarder als het gaat om authenticiteit van gebruikers. Omdat het gaat om niet-persoonsgebonden accounts, is het risico hiervan beperkt.	Door het ontbreken van een functie-autorisatiematrix is het voor ons in de controle niet toetsbaar welke norm gehanteerd is.
Aanbeveling	Wij bevelen aan om te onderzoeken of het uitzonderen van de serviceaccounts en het medewerkersaccount noodzakelijk is.	Wij bevelen aan om een functie-autorisatiematrix op te stellen waarin staat vastgelegd welke rechten bij welke rollen horen. En welke functies welke rollen hebben. Met behulp van deze matrix kunnen de gebruikers en rechten periodiek getoetst worden.
Gevolgen voor de jaarrekening-controle	Ten aanzien van autorisatie steunen wij op dit moment nog niet optimaal op een inrichting van autorisaties die gedurende het jaar beheerst is/wordt.	

5. Bijlagen

Detailbevindingen interne beheersing – Wijzigingsbeheer Centric Financiën

	Wijzigingsbeheer
Constatering	Het proces voor softwarewijzigingen is conform onze verwachting ingericht. Softwarewijzigingen worden getest alvorens deze worden doorgevoerd in een gescheiden productieomgeving. De testwerkzaamheden zijn vastgelegd en geaccordeerd.
Risico	-
Aanbeveling	-
Gevolgen voor de jaarrekening-controle	Ten aanzien van wijzigingsbeheer zien wij geen impact op de jaarrekeningcontrole.

5. Bijlagen

Detailbevindingen interne beheersing – Toegangsbeveiliging Suites voor het Sociaal Domein

	Authenticatie	Autorisatie
Constatering	Gebruikers in Suites kunnen inloggen met een Microsoft account middels Single Sign-On (SSO). Hierbij gelden de wachtwoordinstellingen van het netwerk. Deze zijn van voldoende niveau. Enkele actieve gebruikers hebben geruime tijd niet ingelogd.	Binnen de applicatie hebben wij 11 gebruikers met hoge rechten geïdentificeerd. Deze gebruikers zijn niet direct betrokken bij het primaire proces van de applicatie. Daarom concluderen wij dat hoge rechten bij onafhankelijke functionarissen belegd. Een formele periodieke controle op gebruikers en rechten aan de hand van een functie-autorisatiematrix ontbreekt. Toegang tot de applicatie is geïntegreerd in de organisatie brede procedure voor instroom, doorstroom, en uitstroom.
Risico	-	Het niet uitvoeren van een gestructureerde periodieke controle op rollen en rechten met behulp van een functie-autorisatiematrix verhoogt het risico op doorbreking van functiescheiding.
Aanbeveling	Voor de jaarrekening zijn de risico's beperkt. We raden aan om de gebruikerslijst te controleren op welke gebruikers geen toegang meer hoeven te hebben.	We bevelen aan om een functie-autorisatie matrix op te stellen waarin staat vastgelegd welke gebruikers welke rechten mogen hebben. Hiermee dient periodiek een controle uitgevoerd te worden op rollen en rechten. Een functie-autorisatiematrix kan op basis van functiegroepen ingedeeld worden. Het overzicht dient daarbij ook formeel geaccordeerd te worden.
Gevolgen voor de jaarrekening-controle	Ten aanzien van autorisatie steunen wij op dit moment nog niet optimaal op een inrichting van autorisaties die gedurende het jaar beheerst is/wordt.	

5. Bijlagen

Detailbevindingen interne beheersing – Wijzigingsbeheer Suites voor het Sociaal Domein

	Wijzigingsbeheer
Constatering	Het proces voor softwarewijzigingen is conform onze verwachting ingericht. Uw organisatie werkt aan het ondervangen van de risico's in het softwarewijzigingen-proces. Softwarewijzigingen worden getest alvorens deze worden doorgevoerd in een gescheiden productieomgeving. De testwerkzaamheden zijn vastgelegd.
Risico	-
Aanbeveling	-
Gevolgen voor de jaarrekening-controle	Ten aanzien van wijzigingsbeheer zien wij geen impact op de jaarrekeningcontrole.

5. Bijlagen

Detailbevindingen interne beheersing – Toegangsbeveiliging AFAS

	Authenticatie	Autorisatie
Constatering	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.	Er zijn 10 actieve gebruikers in de applicatie met admin-rechten. Het betreft accounts van functioneel beheer, AFAS, leverancier Covio en één salarisadministrateur. Deze laatste gebruiker is direct betrokken bij het primaire proces van de applicatie. Daarom concluderen wij dat hoge rechten niet bij onafhankelijke functionarissen belegd. Een formele periodieke controle op gebruikers en rechten aan de hand van een functie-autorisatiematrix ontbreekt. Toegang tot de applicatie is geïntegreerd in (en het startpunt van) de organisatie brede procedure voor instroom, doorstroom, en uitstroom.
Risico	-	Het niet uitvoeren van een gestructureerde periodieke controle op rollen en rechten met behulp van een functie-autorisatiematrix verhoogt het risico op doorbreking van functiescheiding.
Aanbeveling	-	We bevelen aan om een functie-autorisatie matrix op te stellen waarin staat vastgelegd welke gebruikers welke rechten mogen hebben. Hiermee dient periodiek een controle uitgevoerd te worden op rollen en rechten. Een functie-autorisatiematrix kan op basis van functiegroepen ingedeeld worden. Het overzicht dient daarbij ook formeel geaccordeerd te worden.
Gevolgen voor de jaarrekening-controle	Ten aanzien van authenticatie zien wij geen impact op de jaarrekeningcontrole. Ten aanzien van autorisatie steunen wij op dit moment niet op een inrichting van autorisaties die gedurende het jaar beheerst is/wordt.	

5. Bijlagen

Detailbevindingen interne beheersing – Wijzigingsbeheer AFAS

	Wijzigingsbeheer
Constatering	Voor applicatie AFAS is wijzigingsbeheer grotendeels uitbesteed aan de leverancier van het pakket. Hierover wordt verantwoording afgelegd in een Assurance-verklaring. Hiermee krijgt u inzicht in de getroffen beheersmaatregelen van deze partijen. Daarnaast zijn er beheersmaatregelen waarvoor de Gemeente Oss zelf verantwoordelijk is om deze in te richten, de User Entity Controls. De beschikbare rapportages worden niet (zichtbaar) beoordeeld door de gemeente Oss.
Risico	Wanneer de leverancier verantwoordelijkheden bij gemeente Oss legt, die niet worden uitgevoerd, ontstaat een leemte in de beheersing.
Aanbeveling	Wij raden aan om in de toekomst de assurance-verklaring te beoordelen en eventueel aanvullende maatregelen te treffen wanneer nodig.
Gevolgen voor de jaarrekening-controle	Wij hebben de User Entity Controls voor de assurance verklaring van 2025 beoordeeld en toegepast op gemeente Oss. Daarbij hebben we geen significante leemten geïdentificeerd.

5. Bijlagen

Detailbevindingen interne beheersing – Continuïteitsmaatregelen en beveiliging

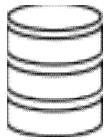
Onderwerp	Bevinding
Back-up	U heeft aangegeven dat back-ups periodiek en incrementeel worden gemaakt en extern worden opgeslagen. Er wordt minimaal een dagelijkse back-up gemaakt, voor verschillende scopes vaker, waardoor het dataverlies beperkt wordt.
Recovery	Er wordt periodiek een recoverytest uitgevoerd. Wij hebben vernomen dat dit jaarlijks tijdens de uitwijktest wordt uitgevoerd. De recoverytest is in november 2025 succesvol uitgevoerd.
Uitwijk	Een uitwijklocatie is ingericht en deze wordt periodiek getest. In November 2025 is een disaster recovery test en uitwijktest uitgevoerd.
Fysieke beveiliging	De servers zijn ondergebracht in een aparte ruimte. De serverruimtes worden niet gebruikt voor andere doeleinden. Naast toegang zijn er maatregelen getroffen omtrent klimaatbeheersing en branddetectie.

5. Bijlagen

Logische toegangsbeveiliging

Wij onderscheiden vijf bouwstenen ten aanzien van toegangsbeveiliging. De bouwstenen leveren gestapeld, naast een sterke IT-beheersing, ook de meeste controlezekerheid op. Beperkingen in de onderliggende steen zorgen voor een verzwakking van de bovenliggende stenen. Onderstaand zijn de bouwstenen schematisch weergegeven.

Authenticatie

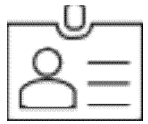


Database
Basis voor toegangsbeveiliging van een applicatie is dat de applicatie de enige toegangspoort is en dat niet rechtstreeks op de database gemuteerd kan worden.



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.

5. Bijlagen

Wijzigingsbeheer

Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat wijzigingen een proces doorlopen, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden. Onderstaand hebben wij per fase onze verwachting aangegeven. Onder wijzigingen verstaan wij niet alleen nieuwe versie updates, maar ook aanpassingen in (kritieke) systeemconfiguraties.

Proces	Verwachting
Risico-inschatting	Voor iedere softwarewijziging is het relevant om te beoordelen wat de risico's zijn die de wijziging met zich meebrengt voor de hoofdprocessen. Daarnaast moet beoordeeld worden welke geïdentificeerde technische en organisatorische wijzigingsrisico's er spelen bij het uitvoeren van de change, in het bijzonder wanneer er sprake is van maatwerk. Hiermee beoordeelt u per wijziging welke nieuwe of gewijzigde functionaliteit een risico vormt voor een goede werking van uw bedrijfsvoering.
Opstellen testplan en aanpak	Vanuit de geïdentificeerde risico's kan een testplan worden gemaakt, waarin de te testen elementen van de software benoemd zijn evenals de inhoudelijk uit te voeren testwerkzaamheden op deze elementen. Belangrijke elementen hierin zijn go/no-go momenten, het maken van een back-up voor implementatie, een fall-back scenario in het geval een implementatie mislukt en het definiëren van de impact op de organisatie (denk bijvoorbeeld aan het opleiden van medewerkers).
Testen en documenteren	Softwarewijzigingen kunnen gestructureerd worden getest na het correct uitvoeren van de voorgaande twee stappen. Het maken van een gedegen vastlegging van testwerkzaamheden is van belang voor de aantoonbaarheid en controleerbaarheid van de uitgevoerde stappen. Daarnaast kan de vastlegging van testwerkzaamheden een belangrijke bron van informatie zijn als er onverhoopt na het doorvoeren van de wijziging toch verstoringen van uw bedrijfsvoering optreden.
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.

Contact

drs. B. (Barry) Smeenk RA
Director Audit
b.smeenk@bakertilly.nl

M.J.H.G. (Mick) Broenland MSc RA
Manager Audit
m.broenland@bakertilly.nl

Kantoorgegevens:
Baker Tilly (Netherlands) B.V.
Kerkenbos 10-207
6546 BB Nijmegen
Postbus 10525
6500 MB Nijmegen



Now, for tomorrow