Managementletter

Gemeente Oss
Boekjaar 2025

Aanbiedingsbrief

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

Onderwerp: Managementletter 2025
Kenmerk: definitief d.d. 9 oktober 2025

Geacht college,

Als onderdeel van de jaarrekeningcontrole van boekjaar 2025 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

Management Samenvatting

Algemene conclusie over interne beheersing

We hebben geen significante tekortkomingen in uw AO/IC geconstateerd. Onze aanbevelingen in deze managementletter zijn met name gericht op het verder optimaliseren van de (IT)-processen en bevatten de belangrijkste aandachtspunten richting jaarrekeningcontrole.

Kernpunten

Gezien de wijzigingen in de wetgeving met betrekking tot de materialiteitsbepalingen zullen we meer aandacht besteden aan de mogelijke onzekerheden met betrekking tot de prestatieleveringen binnen het sociaal domein. We hebben de organisatie gevraagd hieromtrent ook zelf een risicoanalyse op te stellen en de prestatieleveringen met meer diepgang dan voorgaande jaren aan te tonen.

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.

Rechtmatigheidsverantwoording

De wet- en regelgeving aangaande de rechtmatigheidsverantwoording is in april 2025 definitief geworden. Belangrijk is dat de goedkeuringstolerantie (materialiteit) voor zowel de controle van de accountant als de rechtmatigheidsverantwoording wijzigt. De goedkeuringstolerantie voor totaal van fouten en onzekerheden bedraagt nu 2% van de totale lasten exclusief dotaties aan de reserves. Het is van belang dat de gemeente Oss haar financiële verordening en haar controleverordening hierop tijdig aanpast.

Aandachtspunten jaarrekeningcontrole

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 grondexploitaties, de toereikende aanlevering van het dossier aangaande de SiSa-verantwoording, de afgrenzing van de kosten en de controle op de toereikendheid van uw (onderhouds)voorzieningen.

Actuele ontwikkelingen

Vanuit het oogpunt van onze natuurlijke adviesfunctie in deze managementletter hebben we een bijlage opgenomen met actuele ontwikkelingen. Wij vragen u hiervan kennis te nemen en hier indien noodzakelijk rekening mee te houden bij het opstellen van de jaarrekening 2025.

Gemeente Oss

bakertilly

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). 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.
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 focussen zich op die jaarrekeningposten, schattingen, processen of transacties waarvan wij van mening zijn dat het grootste risico bestaat op een afwijking van materieel belang in de financiële overzichten, hetzij als gevolg van fouten hetzij als gevolg van 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 zullen tijdens onze controle voortdurend aandacht houden 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 uw gemeente onderkende risico's / kernpunten in de controle zijn: • 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; • Waardering van uw grondexploitatie (inclusief waardering complex Heesch-West); • Het op marktconforme wijze tot stand komen van significante grondaankopen (dit gezien de hoge mate van subjectiviteit bij het aangaan van dit soort overeenkomsten); • Onterechte betalingen waardoor de lasten ten onrechte zijn verantwoord; • Getrouwheid rechtmatigheidsverantwoording; • Prestatielevering sociaal domein. 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 we dat de interne beheersing inclusief de IT in grote mate op orde is. We constateren dat de organisatie continu doende is om processen verder te verbeteren. We zien dit bijvoorbeeld op het vlak van bijvoorbeeld het inkoopproces. Hier wordt continu gezocht om de beheersing van het belangrijkste proces binnen de gemeente, het inkoopproces, verder te optimaliseren. Daarmee verbeteren de vastleggingen ten aanzien van enerzijds de rechtmatige totstandkoming van de inkoop en anderzijds de vastlegging van de prestatielevering. We merken daarbij wel op dat we begrijpen dat dossiervorming, zowel ten aanzien van het inkoopkeuzeproces als de prestatieverklaring nog verder verbeterd kan worden. In het kader van de jaarrekeningcontrole is onze verwachting, conform voorgaande jaren, dat de tekortkomingen in de dossiervorming door werkzaamheden vanuit de verbijzonderde interne controle worden opgelost. Ook ten aanzien van de IT beheersing constateren we dat ten opzichte van voorgaand jaar dat stappen zijn gezet om naar een meer beheerste omgeving te komen. We zien dat beheersing van procedures rondom toegang tot systemen en wijzigingen aan systemen (software-updates) is geïntensiveerd en geformaliseerd. 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 ontwikkelingen

Onderwerp	Omschrijving
Oss ontwikkelt door	Uw gemeente is onderweg de integrale digitale agenda verdere vorm en invulling te geven. Daarbij is ook oog voor ontwikkelingen in de wereld om ons heen, in de vorm van inzet van kunstmatige intelligentie (AI) en robotisering in processen (RPA). Ook op het gebied van informatiebeveiliging zijn verschillende stappen ondernomen of voortgezet. Denk daarbij aan periodieke scans en tests op kwetsbaarheden in de infrastructuur, verschillende bewustwordingsactiviteiten en de inzet van het Security Operations Center (SOC).
Cloud en leveranciers	Bij het vervangen of upgraden van applicaties wordt in de basis gekozen voor een cloud-strategie. Dit levert nieuwe uitdagingen op op het gebied van beveiliging en ook in de beheersing van risico's die zijn ondergebracht bij leveranciers. Wij benadrukken dat uitbestede risico's altijd van monitoring voorzien moeten zijn om zeker te zijn dat leveranciers adequaat invulling geven aan de (contractueel) gemaakte afspraken. We hebben begrepen dat u hier ook aandacht voor heeft.
Overgang salarisapplicatie	De keuze voor een nieuwe salarisapplicatie is inmiddels gemaakt, daarmee gaat u wisselen van leverancier en zullen (stam)gegevens uit de bestaande applicatie MotionPro overgaan naar AFAS. Dit levert specifieke risico's op als het gaat om de betrouwbare overdracht van gegevens van het bronsysteem naar het doelsysteem, voorgaand jaar rapporteerden wij reeds over onderwerpen die wij verwachten dat inzichtelijk zijn na de overgang.
NOREA reporting Initiative en opvolging multi-compiance	Voorgaand jaar rapporteerden wij over de suggestie om te zoeken naar een raamwerk waarmee multi-compliance aan alle verschillende rapportage- en auditverplichtingen. U heeft afgelopen periode deelgenomen aan een pilot van de beroepsorganisatie voor IT auditors in samenwerking met het Rijk voor het zogenaamde NOREA Reporting Initiative (NRI), waarbij een uniform framework leidt tot een IT-statement en auditverklaring. De pilot bevindt zich in de afrondende fase.

2. Kwaliteit interne beheersing

2.4 IT General controls - Detailbevindingen

Applicatie	Toegangsbeveiliging		Wijzigingsbeheer	Continuïteit	Belangrijkste bevindingen en gevolgen voor de controle
	Authenticatie	Autorisatie			
Netwerk	O	O	N.v.t.	O	Gevolgen voor de controle zijn beperkt, enkele aanbevelingen blijven relevant.
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
Motion Pro / BCS	O	A	A	O	Pakket wordt vervangen, toegangsprocedures beperkt gestructureerd

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

2.5 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 2025 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 2025 geactualiseerd en sluit aan bij relevante wet- en regelgeving
T	3. Het normenkader is uitgewerkt in een concreet werkprogramma met toetsingscriteria en controlewerkzaamheden
T	4. De VIC-werkzaamheden zijn tijdig en volgens planning uitgevoerd
G	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

2.4 Kwaliteit van Verbijzonderde interne controle

We merken op dat de 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 verbeteren. Belangrijkste aandachtspunt op dit moment is de capaciteit, als gevolg van personele wijzigingen en onderbezetting loopt de uitvoering beperkt achter op planning. Dit knelpunt is recent opgelost. We verwachten dat dit voor de jaarrekeningcontrole niet direct problemen op zal leveren, ook gelet op de ervaring van voorgaande jaren.

Gezien de wetswijzigingen in het Besluit Accountantscontrole Decentrale Overheden (BADO) is het nog noodzakelijk om de financiële en de controleverordening aan te passen en vast te stellen door de gemeenteraad. Deze documenten zijn op dit moment ook ter besluitvorming aangeboden. De belangrijkste wijziging is dat de verantwoordingsgrens van 1% naar 2% wordt verhoogd. Hiermee wordt aangesloten op de ook voor de accountant gewijzigde goedkeuringstolerantie. Wij onderschrijven het standpunt om de interne verantwoordingsgrens en de goedkeuringstolerantie van de accountant op gelijke hoogte vast te stellen.

De werkzaamheden van de VIC worden op dit moment uitgevoerd op basis van de oude goedkeuringstolerantie (1%). Gezien het feit dat de verantwoordingsgrens nog niet is vastgesteld, is dit een logische keuze. De gemeente kan ervoor kiezen om de goedkeuringstolerantie te verhogen naar 2%, om de tijd die daarmee wordt gewonnen te steken in doorontwikkeling van de VIC-functie. De gemeente kan er echter ook voor kiezen om 1% te blijven hanteren om strakker op de inrichting van de processen te sturen. Wij adviseren u om aan te sluiten op dezelfde goedkeuringstolerantie als waar wij als accountant mee controleren (2%). Daarnaast kan ons inziens de VIC-functie nog breder ingezet worden door enerzijds de interne controle op de IT-beheersing op te pakken en anderzijds door focus te leggen op andere (niet) materiële, maar wellicht wel foutgevoelige focusgebieden.

Het aangepaste normenkader wordt zoals te doen gebruikelijk binnen de gemeente Oss aan het begin van het nieuwe jaar ter vaststelling aan de gemeenteraad aangeboden , zodat geborgd is dat alle relevante van toepassing zijnde wet- en regelgeving is opgenomen in het normenkader.

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 2025 delen wij onze observaties en aanbevelingen aan de hand van 6 punten.

T	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 Voor verbetering vatbaar T Toereikend G Good practice

Wij constateren dat de gemeente een interne frauderisicoanalyse heeft opgesteld en signaleren hierbij de volgende aandachtspunten:

- In 2025 is de frauderisicoanalyse niet geactualiseerd. Wij adviseren u de actualiteit van de frauderisicoanalyse ieder jaar te bezien en te bepalen of dit mogelijk impact heeft op de uit te voeren VIC-werkzaamheden.

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 verassingen te voorkomen willen wij de volgende werkafspraken met u maken.

3. Voorbereiding jaarrekeningcontrole

3.1 Voorbereiding jaarrekeningcontrole

Wij starten met de jaarrekeningcontrole op 2 maart 2026. In het najaar van 2025 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 2025 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 2025 hebben wij gezamenlijk de jaarrekeningcontrole 2024 geëvalueerd. Behoudens enkele aandachtspunten voor beide partijen hebben wij geconcludeerd dat de controle over het boekjaar 2024 soepel en plezierig is verlopen. De gemaakte afspraken zien toe op een verdere ontwikkeling in de samenwerking.	n.v.t.
Opvolging van bevindingen VIC/accountant	Vanuit ons accountantsverslag hebben we de volgende adviezen opgenomen: - Krijg tijdiger grip op begrotingsafwijkingen, anders dan overschrijdingen van lasten. - Zorg voor juiste afgrenzing van kosten. - Neem een aparte paragraaf Openbaarheid in de jaarstukken op.	We verwachten van de gemeente dat zichtbaar opvolging gegeven is aan deze adviezen.
Ontwikkelingen bij klant	De gemeente Oss is voornemens nieuwe beheerplannen vast te stellen. Daarnaast vragen we aandacht met betrekking tot de kosteninschattingen op grondexploitaties en de wijzigingen in wet- en regelgeving.	We verwijzen naar de volgende pagina.
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.	Aanleggen van consistente balansdossiers met betrekking tot de SiSa oplevering.

3. Voorbereiding jaarrekeningcontrole

Grondexploitaties

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 we dat de totstandkoming van de rapportages verbeteren. Wel blijven we aandacht vragen voor de optimistische inschattingen qua timing ten aanzien van de kosten. Als we de inschatting van de verwachte bestedingen 2025 bij de jaarrekening 2024 vergelijken met de werkelijke bestedingen dan constateren dat de verwachte uitgaven vertragen in tijd. We vragen u bij de actualisering van de grondexploitaties bij de jaarrekening 2025 voor dit aspect extra aandacht te hebben.

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.

Onderhoudsvoorzieningen

Wij hebben begrepen dat de beheerplannen die ten grondslag aan de onderhoudsegalisatievoorzieningen liggen geactualiseerd zijn. De financiële consequenties hiervan worden meegenomen in de tweede bestuursrapportage. Gezien de complexe wet- en regelgeving rondom de onderhoudsegalisatievoorzieningen worden wij graag in een vroeg stadium betrokken aangaande de boekhoudkundige verwerking van de consequenties van de herziene beheerplannen.

3. Voorbereiding jaarrekeningcontrole

Aanpassing BADO en BBV leidt tot wijziging in o.a. financiële verordening

In de aanpassing van BADO op 16 april jl. is een belangrijke wijziging opgenomen: de maximale goedkeuringstolerantie van 1% voor fouten en 3% voor onzekerheden (dus samen 4%) wijzigt met ingang van dit boekjaar 2025 in een maximale goedkeuringstolerantie van 2% voor afwijkingen. Met afwijkingen worden zowel fouten als onzekerheden bedoeld. Daarnaast wijzigt ook de grondslag voor de goedkeuringstolerantie van lasten inclusief toevoegingen aan de reserves naar lasten exclusief toevoegingen aan de reserves.
Voor de rechtmatigheidsverantwoording geldt dat deze met ingang van 2025 maximaal 2% van de lasten exclusief toevoegingen aan de reserves mag bedragen (in 2023 en 2024 nog maximaal 3% van de lasten inclusief toevoegingen aan de reserves).

Om deze wijzigingen goed in de organisatie in te bedden adviseren wij u om tijdig deze aanpassingen in de financiële verordening, de controleverordening, het controleprotocol en het interne controleplan te verwerken. Gemeente Oss heeft deze aanpassingen grotendeels onderhanden en de aangepaste beleidsdocumenten worden voor 1 januari 2026 vastgesteld.

Gevolgen onzekerheden sociaal domein

De hiervoor genoemde aanscherping van de tolerantiegrens naar 2% voor afwijkingen heeft mogelijk gevolgen voor gemeenten. Omdat eerst onzekerheden apart tegen de 3% norm geëvalueerd mochten worden, moet nu diepgaander het risico beoordeeld worden ten aanzien van onzekerheden met betrekking tot de prestatielevering in het sociaal domein. Onder de nieuwe normering kunnen deze onzekerheden tezamen met de fouten sneller leiden tot een overschrijding van controletoleranties (en daarmee de aard van verklaring raken).

We hebben de gemeente gevraagd een diepgaande analyse van de stromen binnen het sociaal domein op te stellen en te onderbouwen per stroom hoe de gemeente afdoende zekerheid verkrijgt ten aanzien van de prestatielevering die aan de inwoners van de gemeente wordt geleverd. We verwachten dat deze analyse en ook de gegevensgerichte werkzaamheden hierop voor de start van de controle zijn afgerond.

3. Voorbereiding jaarrekeningcontrole

Controleverklaring in aparte paragraaf ‘Overige gegevens’

Met ingang van het boekjaar 2025 is het Besluit Begroting en Verantwoording (BBV) aangepast, waarbij de controleverklaring van de accountant voortaan wordt opgenomen onder het onderdeel ‘Overige gegevens’ van de jaarrekening. Deze paragraaf Overige gegevens moet in de jaarstukken worden opgenomen ná de jaarrekening en dus niet als onderdeel van de jaarrekening. Voor het proces van opstellen, goedkeuren en publiceren van de jaarstukken betekent dit dat de Raad een versie van de jaarstukken goedkeurt waarin de definitieve controleverklaring van de accountant is opgenomen. De publicatie van de jaarstukken op de website omvat voortaan de opgestelde versie inclusief de paragraaf Overige gegevens, met daarin de controleverklaring van de accountant. De gemeente Oss hanteerde al deze werkwijze, derhalve heeft deze wijziging beperkte impact op het proces van de jaarrekeningcontrole 2025 en verder.

Notitie grondbeleid (en rente) in jaarstukken

De wijzigingen hebben met name invloed op de verslaggevingsregels:

1. Voor het faciliterend grondbeleid zijn de verhaalsmogelijkheden van kosten uitgebreid. Tevens is de kostensoortenlijst uitgebreid, waardoor ook meer kosten verhaald kunnen worden.
2. De voorwaarden voor warme gronden zijn gewijzigd. Deze voorwaarden gelden met ingang van de nieuwe notitie ook voor bedrijventerreinen.
3. Gemaakte voorbereidingskosten mogen na 5 jaar ook worden voorzien in plaats van te worden afgeboekt. Hierdoor wordt het mogelijk gemaakt om in een later stadium alsnog deze kosten op te voeren.
4. In een gemengde grondexploitatie mag het resultaat gesaldeerd worden indien de deelgebieden in ontwikkeling onlosmakelijk met elkaar verbonden zijn.
5. Winstneming door middel van POC methode, kan alleen plaatsvinden als de looptijd van een grondexploitatie 10 jaar of korter is.
6. Belangrijkste wijziging is dat toerekening rente aan grondexploitaties ook conform de gemeentelijke omslagrente zal plaatsvinden.

Voor de gemeente Oss zijn met name punt 1, 4 en 6 relevant.

Actualiteiten

Afgelopen jaar heeft het Rijk enkele wijzigingen op het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) en het Besluit Accountantscontrole Decentrale Overheden (Bado) voorgesteld voor toekomstige jaren. Samenvattend zijn in dit hoofdstuk de belangrijkste voorgestelde wijzigingen opgenomen.

4. Actualiteiten

Wethouderspensioen

De nieuwe pensioenwet geldt vanaf 1 juli 2023, maar niet voor politieke ambtsdragers zoals wethouders. Zij vallen onder de aparte Appa-regeling, die zoveel mogelijk aansluit bij de ABP-regeling voor overheidswerknemers. Sinds juli 2022 zijn de verschillen tussen Appa en ABP grotendeels gelijkgetrokken. Gemeenten betalen nu nog pensioenen rechtstreeks, maar het is de bedoeling dat deze pensioenen via een collectieve waardeoverdracht worden ondergebracht bij het ABP. Hierdoor vervalt ook de pensioenvoorziening voor wethouders op de gemeentelijke balans.

We adviseren de gemeente Oss om bij het opstellen van de jaarrekening 2025 indien mogelijk reeds rekening te houden met de overdracht naar het ABP.

Notitie structurele en incidentele baten en lasten

De Commissie BBV heeft eind 2024 een vernieuwde notitie gepubliceerd over hoe gemeenten moeten omgaan met structurele en incidentele baten en lasten. Deze notitie geeft extra uitleg en nieuwe afspraken, vooral over het gebruik van geld uit de algemene reserve.

Belangrijkste wijziging: inzet van de algemene reserve

Vanaf begrotingsjaar 2025 is het toegestaan voor gemeenten om maximaal 10% van het overschot (surplus) van de algemene reserve gebruiken om structurele uitgaven te betalen. Dit mag alleen als:

- De solvabiliteit (de verhouding tussen eigen vermogen en totaal vermogen) minimaal 20% is en blijft.
- Er een goede risico-inventarisatie is gemaakt.
- Het weerstandsvermogen voldoende is om de risico's op te vangen.

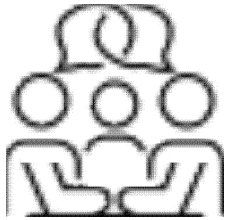
Wat moeten gemeenten doen?

- Zorg voor een duidelijke begroting. *Laat in de begroting en jaarrekening zien of er sprake is van een structureel evenwicht. Gebruik hiervoor het voorbeeld uit de notitie.*
- Maak onderscheid tussen incidenteel en structureel. *Neem in de financiële verordening een grensbedrag op: vanaf welk bedrag moeten incidentele lasten en baten apart worden toegelicht? Ligt deze incidentele baten en lasten toe in de jaarrekening.*
- *Dit zorgt voor duidelijkheid en consistentie.*
- Controleer het weerstandsvermogen. *Zorg dat het weerstandsvermogen groot genoeg is om de geïnventariseerde risico's te kunnen opvangen.*

4. Actualiteiten

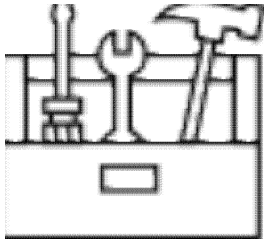
Notitie verbonden partijen

Op 24 juni jl. heeft commissie BBV de aangepaste Notitie Verbonden partijen gepubliceerd. Wijzigingen volgen met name uit de per 1 juli 2022 aangepaste Wet gemeenschappelijke regelingen (Wgr). De belangrijkste wijzigingen die in de notitie verder worden uitgewerkt zijn:



Versterking van de positie van gemeenteraden

- **Zienswijze indienen**: Gemeenteraden krijgen meer invloed én verantwoordelijkheid doordat ze zienswijzen mogen indienen bij belangrijke besluiten zoals de begroting, jaarrekening en beleidsnota's.
- **Adviescommissie**: De mogelijkheid om een gemeenschappelijke adviescommissie in te stellen, die gemeenteraden ondersteunt in hun taak, is geïntroduceerd.
- **Informatieplicht**: Colleges van burgemeester en wethouders moeten proactief de gemeenteraden op de hoogte houden van relevante ontwikkelingen binnen de GR's.



Introductie van aanvullende controle-Instrumenten raad

- **Recht van enquête**: Recht om onderzoek te doen naar mogelijke misstanden binnen een GR. Dit omvat het recht van enquête.
- **Onderzoek door rekenkamers**: Rekenkamers kunnen o.a. onderzoek doen naar het gevoerde bestuur van een GR. Omdat meerdere gemeenten en rekenkamers betrokken zijn bij GR's, worden audits waarschijnlijk vaker en grondiger uitgevoerd.
- **Evaluatie van de regeling**: Gemeenteraden kunnen nu afspraken maken over de frequentie en focus van evaluaties van de GR.

Verbetering van governance-structuren

- **Uittreding uit een regeling**: Het maken van duidelijke afspraken over de gevolgen voor het vermogen van de rechtspersoon bij uittreding uit een GR. Dit omvat zaken als personeel, contracten, huisvesting en investeringen.
- **Begrotingscyclus**: De termijnen voor de indiening van de kadernota, de ontwerpbegroting en de begroting zijn aangepast om een betere afstemming op de besluitvorming van de gemeenteraad te waarborgen.

De nieuwe verplichtingen en controle-instrumenten kunnen leiden tot een hogere ambtelijke en bestuurlijke capaciteitsdruk. Wij adviseren u uw interne processen te evalueren en waar nodig aan te passen. Daarnaast is het van belang om vast te stellen of de capaciteit binnen de gemeente voldoende is om te kunnen voldoen aan de mogelijk aanvullende belasting.

4. Actualiteiten

NIS2 / Cyberbeveiligingswet

De Cyberbeveiligingswet (Cbw), die de Europese NIS2-richtlijn implementeert, is op 17 juni 2025 ingediend bij de Tweede Kamer. De beoogde inwerkingtreding is het tweede kwartaal van 2026. De wet heeft als doel de digitale weerbaarheid van vitale en essentiële organisaties te versterken, waaronder gemeenten. Gemeenten gaan rechtstreeks onder de Cbw vallen omdat ze worden aangemerkt als essentiële overheidsentiteiten.

Hoewel de wet nog niet van kracht is, hebben sommige bepalingen uit de NIS2-richtlijn al directe werking. Gemeenten kunnen zich nu al vrijwillig registreren bij het Nationaal Cyber Security Centrum (NCSC) en gebruik maken van dienstverlening van dit centrum. De informatiebeveiligingsdienst heeft ook al diverse kennisproducten en hulpmiddelen voor gemeenten uitgewerkt.

Wij adviseren de gemeente om vooruitlopend op de inwerkingtreding al te starten met de implementatie van de cyberbeveiligingswet, gemeente Oss geeft daar al invulling in door extra capaciteit in te zetten voor de implementatie. U heeft ons geïnformeerd een programma te hebben gestart waarbij programmamanager is aangesteld, waarin al verschillende activiteiten zijn ondernomen om te voldoen aan onderstaande verplichtingen. Er wordt nog gezocht naar een Business Continuity Manager. Ook Baker Tilly kan u ondersteunen bij de voorbereiding op NIS2.

Aandachtspunten cyberbeveiligingswet

De wet introduceert de volgende verplichtingen voor gemeenten:

1. **Zorgplicht:** gemeenten moeten passende technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. De BIO2 normering biedt hiervoor de beoogde uitwerking.
2. **Meldplicht:** Ernstige cyberincidenten moeten worden gemeld aan de Rijksinspectie Digitale Infrastructuur (RDI), het CSIRT en de Informatiebeveiligingsdienst (IBD).
3. **Bestuurlijke verantwoordelijkheid:** Burgemeesters en wethouders zijn persoonlijk verantwoordelijk voor naleving. Zij moeten een verplichte training informatiebeveiliging volgen. Bij nalatigheid kunnen boetes oplopen tot € 10 miljoen voor de organisatie en € 25.000 voor individuele bestuurders.

Baker Tilly kan de gemeente helpen bij de volgende stappen die nu al (kunnen) worden gezet:

- Voer een NIS2 GAP-analyse uit om inzicht te krijgen in de huidige volwassenheid van de informatiebeveiliging.
- Werk daarbij volgens de Baseline Informatiebeveiliging Overheid (BIO 2.0), die als normenkader voor de Cbw zal dienen.
- Implementeer een Information Security Management System (ISMS) om structureel risico's te beheersen en compliance te borgen.
- Start met bewustwording en training van bestuurders, zodat zij hun rol in risicomanagement en besluitvorming effectief kunnen invullen.
- Leg verantwoording en toezicht vast in de gemeentelijke governance, inclusief betrokkenheid van de gemeenteraad.

4. Actualiteiten

Spendanalyse automatiseren

Gemeenten hebben de verantwoordelijkheid om publieke middelen doelmatig, transparant én rechtmatig in te zetten. Goed zicht op het inkoopproces en de uitgaven is daarbij essentieel. Een spendanalyse kan helpen om inzicht te krijgen in waar geld naartoe gaat, welke trends zich aftekenen en waar mogelijke besparingen of verbeteringen liggen.

Gemeenten maken meer en meer gebruik van innovatieve ontwikkelingen en data-analyse. Zeker waar (nog) onvoldoende kan worden gesteund op de beheersingsmaatregelen kan data-analyse waardevol zijn. De uitkomsten kunnen leiden tot betere managementinformatie met nieuwe, heldere en vooral ook concrete inzichten, gericht op nog betere (bij)sturing.

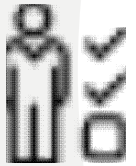
Door het inkoopproces systematisch te analyseren, ontstaat overzicht in onder andere aanbestedingen, contractbeheer en leverancierssprestaties. Dit draagt niet alleen bij aan doelmatiger inzet van middelen, maar ook aan het rechtmatig uitvoeren van aanbestedingen en het naleven van wet- en regelgeving.

Baker Tilly Advisory heeft een tool ontwikkeld die dit proces ondersteunt. Deze tool helpt gemeenten om spendanalyses sneller en efficiënter uit te voeren – op totaalniveau, per crediteur of per opdracht. Het is een middel dat gebruikt kan worden om op basis van data het gesprek te voeren over inkoop, kwaliteit en doelmatigheid.
De regie ligt bij de gemeente zelf. Wij denken mee over hoe deze inzichten op een toegankelijke manier kunnen worden ingezet om onderbouwd te sturen op beleid, uitvoering en rechtmatigheid.

Stap 1
Uploaden dump

Stap 2
Analyse op crediteurenniveau

Stap 3
Analyse op opdrachtniveau



Stap 4
Checklist

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 175 actieve accounts geen verlopend wachtwoord hebben, dat zijn er 10 meer dan vorig jaar. Het betreft met name service-accounts, mailboxen en tv schermen. Twee-factor authenticatie wordt afgedwongen voor benaderen van het netwerk vanuit externe locaties.	Er is geen functie-autorisatiematrix opgesteld waarmee gebruikers en rechten periodiek worden beoordeeld. We hebben vernomen dat er in toegangsbeheer tot applicaties stappen zijn gezet met de inrichting van een automatiseringsoplossing voor toegang tot applicaties. 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.
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	Wachtwoordinstellingen op het netwerk zijn in lijn zijn met de beleidsvoering van de organisatie.	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 Key2Financiën

	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.	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. Toegang tot Key2Financiën is via gescheiden aanvraag-procedures van overige applicaties ingericht. Wij zijn geïnformeerd dat Gemeente Oss een grootschalig project heeft opgestart om beheersing van toegang tot de systemen naar een hoger niveau te brengen. Wij onderschrijven het belang van dit project.
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 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. Ten aanzien van wijzigingsbeheer zien wij geen impact op de jaarrekeningcontrole.	

5. Bijlagen

Detailbevindingen interne beheersing – Wijzigingsbeheer Key2Financiën

	Wijzigingsbeheer
Constatering	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. Er zijn systeemaccounts actief in de applicatie waarvan het wachtwoord op netwerk-niveau niet verloopt. Deze systeemaccounts beschikken in de applicatie over hoge rechten.	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. Wij hebben vernomen dat incidenteel de gebruikers doorgelopen worden. Hierbij wordt geen functie-autorisatiematrix gebruikt. Toegang tot de applicatie is geïntegreerd in de organisatie brede procedure voor instroom, doorstroom, en uitstroom. Wij zijn geïnformeerd dat Gemeente Oss een grootschalig project heeft opgestart om beheersing van toegang tot de systemen naar een hoger niveau te brengen. Wij onderschrijven het belang van dit project.
Risico	Accounts waarvan wachtwoorden niet verlopen zijn kwetsbaarder als het gaat om authenticiteit van gebruikers. Omdat het gaat om een niet-persoonsgebonden account, is het risico hiervan beperkt aangezien de gebruikers dit jaar (nog) niet hebben ingelogd.	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. Ten aanzien van authenticatie zien wij geen impact op de jaarrekeningcontrole.	

5. Bijlagen

Detailbevindingen interne beheersing – Wijzigingsbeheer Suites voor het Sociaal Domein

	Wijzigingsbeheer
Constatering	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 Motion Pro

	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.	We hebben vernomen dat uw organisatie aanpassingen heeft doorgevoerd in de hoge rechten in de applicatie. We hebben vernomen dat alleen de functioneel beheerder nog rechten heeft om gebruikers aan te maken en rechten toe te kennen. Wij hebben vernomen dat incidenteel de gebruikers doorgelopen worden. Hierbij wordt geen functie-autorisatiematrix gebruikt. Toegang tot de applicatie is geïntegreerd in de organisatie brede procedure voor instroom, doorstroom, en uitstroom.
Risico	Geen risico geïdentificeerd.	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	Niet van toepassing.	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 Motion Pro

	Wijzigingsbeheer
Constatering	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. Aan de applicatie is niet ontwikkeld in 2025. U gaat overstappen naar AFAS voor de salarisverwerking.
Risico	De overgang naar een nieuwe applicatie introduceert verschillende risico's. Hierover informeren wij u in deze rapportage. Zie hoofdstuk 2.3 van deze managementletter, "Overgang salarisapplicatie".
Aanbeveling	Wij raden aan om in de toekomst de relevante stappen binnen het wijzigingsproces te blijven uitvoeren, ook in de nieuwe applicatie AFAS.
Gevolgen voor de jaarrekening-controle	Bij de controle van het nieuwe boekjaar zullen wij vragen naar de projectdocumentatie, het conversieverloop en -akkoord en de documentatie van de uitgevoerde testen.

5. Bijlagen

Detailbevindingen interne beheersing – Continuïteitsmaatregelen en beveiliging

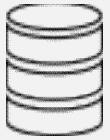
Onderwerp	Bevinding
Back-up	U heeft aangegeven dat back-ups periodiek en incrementeel worden gemaakt en extern worden opgeslagen. Er wordt minimaal een dagelijkse back-up gemaakt, waardoor het dataverlies beperkt wordt.
Recovery	Er wordt periodiek een recoverytest uitgevoerd. Wij hebben vernomen dat dit jaarlijks tijdens de uitwijktest wordt uitgevoerd. De recoverytest is in november 2024 succesvol uitgevoerd.
Uitwijk	Een uitwijklocatie is ingericht en deze wordt periodiek getest. Daarnaast heeft u met een externe IT partner afspraken gemaakt over (werkplek-) capaciteit indien de primaire hosting op locatie wegvalt.
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.
Remote acces	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.

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
+31 6 15 59 17 58

Kantoorgegevens:
Baker Tilly (Netherlands) B.V.
Kerkenbos 10-27
6546 BB Nijmegen
Postbus 10525
6500 MB Nijmegen