Eshuis

MANAGEMENTLETTER 2025

Veiligheidsregio Utrecht

24 FEBRUARI 2026

Per saldo persoonlijker

Vertrouwelijk
Aan het dagelijks bestuur van de gemeenschappelijke regeling Veiligheidsregio Utrecht
T.a.v. de heer J. Donker
Postbus 3154
3502 GD UTRECHT

Datum
24 februari 2026

Ons kenmerk
1019048-2025-ML

Behandeld door
G.C. Helminck RA MSc EMA

Amersfoort, 24 februari 2026

Geacht bestuur, geachte directie,

Het algemeen bestuur heeft Eshuis Registeraccountants opdracht gegeven om de jaarrekening 2025 van gemeenschappelijke regeling Veiligheidsregio Utrecht (hierna: VRU) te controleren. Voor een nadere omschrijving van onze opdracht verwijzen wij u naar onze opdrachtbevestiging.

Als onderdeel van onze controle onderzoeken wij onder andere de administratieve organisatie en de interne beheersing bij uw gemeenschappelijke regeling. Naar aanleiding daarvan brengen wij deze managementletter uit. Hierin richten wij ons met name op mogelijke verbeterpunten in de processen die wij hebben onderzocht om een bijdrage te leveren aan de interne beheersing en het zelf controlerend vermogen.

Wij beginnen deze managementletter met een samenvatting van onze belangrijkste boodschappen voor u en de belangrijkste risico's die wij bij de controle van de VRU onderkennen. Daarna geven wij een oordeel op hoe de relevante processen zijn opgezet en adviseren wij u over verbetermogelijkheden. Voor zover er naar aanleiding van onze bevindingen door u nog aanvullende werkzaamheden zijn vereist worden deze met u gedeeld in de eerstvolgende paragraaf. De laatste paragraaf benutten wij voor een aantal relevante actualiteiten die wij graag met u delen.

Wij danken uw organisatie voor de samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken

Met vriendelijke groet,

Eshuis Registeraccountants B.V.

Antine van de Groep

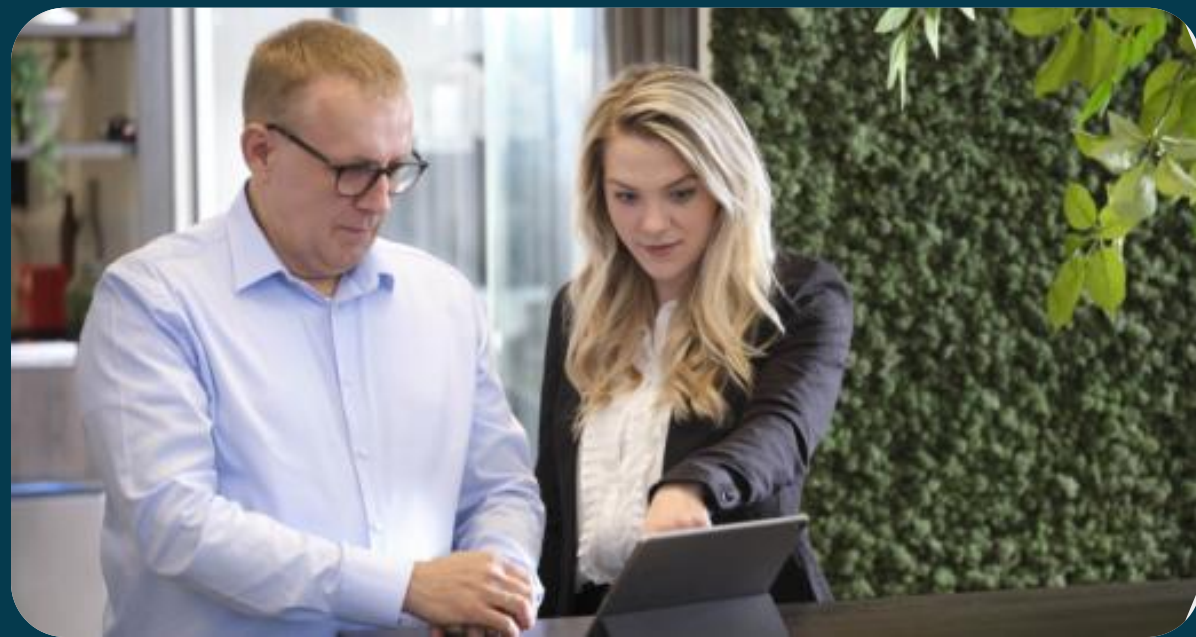
Digitaal ondertekend door Antine van de Groep
DN: cn=Antine van de Groep, c=NL, o=Antine van de Groep
Datum: 2026.02.24 10:18:14 +01'00'

A. (Antine) van de Groep MSc RA

Inhoudsopgave

Eshuis

Management samenvatting



Per saldo persoonlijker

Managementsamenvatting

Onderwerp	Boodschap
Interim controle	Voor u ligt de managementletter 2025, waarin wij verslag uit brengen over de interim-controle die in het laatste kwartaal van 2025 en januari 2026 is uitgevoerd. Wij kijken terug op een fijne samenwerking met de ambtelijke organisatie. De interim-controle is primair gericht op het beoordelen van de interne beheersmaatregelen (key controls) in de voor de jaarrekening relevante bedrijfsprocessen. Dit zijn die processen binnen uw organisatie die een koppeling hebben met materiële posten in de jaarrekening en ook processen waarin wij verhoogde (fraude)risico's onderkennen. We hebben daarbij oog voor onderwerpen die naar onze mening van belang zijn voor uw bedrijfsvoering of die richting kunnen geven aan het verder verbeteren van de procesbeheersing.
Belangrijkste bevindingen	Afgelopen jaren heeft de VRU uitdagingen gehad als gevolg van capaciteitsproblemen door onder andere ziekteverzuim en wisselingen van het personeelsbestand op de afdeling financiën & control. Wegens deze uitdagingen zijn onder meer op een aantal gerapporteerde bevindingen uit de eerdere managementletters strategische keuzes gemaakt en/of bepaalde risico's geaccepteerd. Daarmee zijn echter de risico's niet weg en hebben wij de bevindingen vanuit onze zorg- en informatieplicht alsnog opgenomen. Wij onderkennen dat de VRU de wil en ambitie heeft om de kwaliteit van de AO/IB te optimaliseren, maar daarbij ook de nuchtere afdronk maakt dat het wel binnen de capaciteitsuitdagingen moet passen. Voor boekjaar 2025 zien wij de belangrijkste uitdaging op het realiseren van de werkzaamheden vanuit het VIC-controleplan op de rechtmatigheidsverantwoording. Tot slot zijn uit de IT-audit bevindingen gebleken.
IT-systemen	Goed functionerende geautomatiseerde systemen kunnen bijdragen aan de doorontwikkeling van processen zodat de VRU toekomstbestendig kan blijven opereren en risico's effectief en efficiënt kan mitigeren. Informatievoorziening is een belangrijk aandachtspunt, en wij merken op dat de gemeenschappelijke regeling hierin nog enkele stappen dient te zetten. Het verkrijgen van zekerheid over de interne beheersing van IT-processen die de organisatiedoelstellingen van de VRU ondersteunen, wordt steeds belangrijker. Als gevolg hiervan is IT een belangrijk onderwerp voor zowel de jaarrekening- als rechtmatigheidscontrole. Hoewel u als veiligheidsdienst niet onder NIS2 valt, is dit wel een richtlijn die voor u handreikingen biedt in het beheersen van (cyber)risico's. Dat veiligheidsdiensten niet onder NIS2 vallen heeft immers niets te maken met het (vermeende) niveau van het cybersecuritymanagement bij veiligheidsdiensten, maar eerder met hun rol in het veiligheidsstelsel. In het kader van de jaarrekeningcontrole hebben wij een IT-audit uitgevoerd bij de VRU. Uit deze audit blijkt dat er op meerdere gebieden nog verbeteringen nodig zijn. In 2025 is sprake van een gelijk gebleven IT-beheersing. Wij vragen wederom uw aandacht voor onze bevindingen en bevelen aan om hier actief mee bezig te gaan.
Rechtmatigheids-verantwoording	De aanscherping van de controlegrenzen zoals die met ingang van 2025 is ingevoerd door een wijziging in het besluit accountantscontrole decentrale overheden (BADO) vraagt om een herziening van verordeningen en auditplannen. Voor wat betreft de verordening heeft de VRU reeds in voorgaande jaren gekozen om aan te sluiten bij het wettelijke maximum. U kiest ervoor dat u in 2026 het auditplan herziet. Deze keuze kan wel tot gevolg hebben dat onrechtmatigheden in niet materiële financiële stromen in uw foutenevaluatie bij de rechtmatigheidsverantwoording dienen te worden betrokken. Inmiddels is de nieuwe kadernota rechtmatigheid 2025 gepubliceerd. De wijzigingen in het BADO zijn in deze versie opgenomen. Op het moment van schrijven is de praktijkhandreiking voor accountants bij de rechtmatigheidsverantwoording geconsulteerd. Deze consultatie kan leiden tot bijstellingen en wijzigingen in onze controleaanpak. Wij zullen deze tijdig met de organisatie bespreken.

Managementsamenvatting

Onderwerp	Boodschap
Verbijzonderde interne controle (VIC)	Ten aanzien van de VIC merken wij op dat de organisatie voor het derde jaar de volledige verantwoordelijkheid draagt voor het uitvoeren van de financiële rechtmatigheidscontroles. Op basis van de gesprekken die wij hebben gevoerd tijdens de interim-controle constateren wij dat de VIC in 2025 achterliep ten opzichte van de planning. Dit is het gevolg van medewerkers die de organisatie hebben verlaten. De formatie is voor de afwikkeling van de interne controles over 2025 in het voorjaar van 2026 ingevuld door zowel vaste medewerkers als tijdelijke inhuur. Hiermee heeft de VRU invulling gegeven aan het langdurig binden van medewerkers aan de organisatie. Voor wat betreft formaliteiten merken wij op dat als gevolg van de wijziging in het BADO formele stukken zoals de financiële verordening, controleverordening en het controleplan herzien dienen te worden. Voor wat betreft dat laatste is er in uw geval sprake van een verlichting, omdat de verantwoordingsgrens in uw geval ten opzichte van eerdere jaren omhoog gaat. Dit is ook het moment om te kijken welke transactiestromen en rechtmatigheidsvereisten uit uw normenkader niet langer getoetst zouden moeten worden. Deze ontwikkeling en de tijdelijke inhuur op met name de controle op de Europese aanbestedingen kunnen bijdragen aan het tijdig en goed afronden van de interne controle over 2025. Ondanks de achterlopende controle op de Europese aanbestedingen heeft 2025 in het teken gestaan van het voltooien van een aantal Europese aanbestedingen voor crisisnoodcontracten. Hier tegenover staat dat een aantal crisisnoodcontracten (nog) niet aanbesteed zijn. Hierdoor ontstaat een spagaat omdat bepaalde contracten bewust (nog) niet aanbesteed zijn. Het dagelijks bestuur zal met onafhankelijke ondersteuning vanuit de VIC dienen te oordelen of deze contracten (on)rechtmatig zijn en deze conclusie juist verwoorden in de rechtmatigheidsverantwoording. Voorgaande vraagt meer commitment vanuit het dagelijks bestuur naar uw VIC als het gaat om het goed kunnen uitvoeren van de controlewerkzaamheden en vrijelijk kunnen oordelen en rapporteren.
Fraude, misbruik & oneigenlijk gebruik	Jaarlijks herziet de VRU haar interne frauderisicoanalyse. Wij hebben in voorgaand jaar aandacht gevraagd voor de doorontwikkeling van de frauderisicoanalyse naar een fraudebeheersplan inclusief een fraude-escalatieladder. Hierbij dient de organisatie op basis van "plan, do, check, act" aan te tonen dat zij de geïdentificeerde frauderisico(factoren) van adequate en tijdige beheersingsmaatregelen heeft voorzien. Daarnaast dienen binnen de organisatie de nodige afspraken gemaakt te worden over de wijze waarop omgegaan moet worden met fraude(signalen). Deze doorontwikkeling inclusief de toetsing op frauderisico(factoren) heeft in 2025 nog niet plaatsgevonden.
Anticorruptie-programma	Afgelopen twee jaar hebben wij als onderdeel van het anticorruptieprogramma uw aandacht gevraagd voor het verbeteren van de registratie en afscherming van (integriteits)meldingen alsmede nevenfuncties. De VRU heeft het implementeren en verbeteren van de registratie en afscherming van integriteitsmeldingen nog onderhanden. Als het gaat om de beleidsmatige stukken zoals het integriteitsbeleid, de klachtenregeling, de klokkenluidersregeling en de gedragscode merken wij op dat de VRU in 2025 stappen heeft gezet om deze te actualiseren dan wel op te stellen. Voor wat betreft het managen van integriteitsrisico's merken wij op dat het integriteitsbeleid wel spreekt over deze (en andere risico's) maar dat deze niet concreet zijn vastgelegd en voorzien van beheersingsmaatregelen. Op dit concrete onderdeel kan de VRU nog stappen zetten. De stukken zijn opgesteld en onderdeel van de dagelijkse gang van zaken binnen de organisatie alsmede periodieke overleggen op managementniveau. Medewerkers met nevenfuncties lopen in theorie corruptierisico's. Het beoordelen van nevenfuncties is voor verbetering vatbaar, voornamelijk als het gaat om het zichtbaar controleren van de opgegeven nevenfuncties.

Managementsamenvatting

Onderwerp	Boodschap
Actualiteiten	Wij hebben in hoofdstuk Actualiteiten een aantal actualiteiten opgenomen waar wij aandacht voor vragen.
Vooruitblik richting Jaarrekening-controle 2025	We hebben met uw organisatie afspraken over de jaarrekeningcontrole 2025 gemaakt. Op voorhand identificeren we een aantal aandachtsgebieden met verhoogde aandacht in onze controle. Dit betreffen met name de controle op de betaalomgeving, de controle op de getrouwheid van de rechtmatigheidsverantwoording, de WNT en de getrouwe en rechtmatige totstandkoming van de SiSa bijlage alsmede de verrekening van de activiteiten rondom de crisisnoodopvang. Wij constateren dat in dat laatste geval sprake is van voorfinanciering door de VRU waardoor ultimo boekjaar sprake is van een omvangrijke posities nog te facturen en te ontvangen. Dit kan gaan om circa € 12 miljoen. Wij vragen uw aandacht voor het tussentijds factureren van deze posities en waar mogelijk tussentijds afstemmen van de projectvoortgang met de financier. Begin juni 2025 is de Meldkamer Midden-Nederland geactiveerd. Medewerkers van de VRU voeren ten behoeve van de samenwerkende organisaties specifieke taken en werkzaamheden uit. Over de dekking en doorbelasting van de kosten van deze medewerkers alsmede eventuele overheadkosten zijn afspraken gemaakt in een aparte dienstverleningsovereenkomst. Wij hebben voorgaande besproken met uw medewerkers en de accountant van één van de samenwerkende organisaties. Verantwoording afleggen hoort nu eenmaal bij uitbesteding en zowel de VRU als Eshuis streven een praktische invulling na. De VRU heeft dit verantwoordingsproces onderdeel gemaakt van de jaarrekeningcontrole en neemt in de bijlagen van de jaarrekening 2025 de benodigde informatie op waarmee de samenwerkende organisaties zekerheid kunnen verkrijgen over de doorbelaste kosten. In het verlengde van voorgaande hebben wij tussentijds kennisgenomen van de diverse verlofstanden binnen uw organisatie, waaronder het spaarverlof, gekocht verlof en het (boven)wettelijk verlof. Arbeidsgerelateerde verplichtingen van jaarlijks gelijkblijvend volume (zowel in uren als in euro's) worden enkel buiten de balans opgenomen, en niet onder de passiva. Uit onze beoordeling blijkt een omvangrijke, maar geen materiële stijging van het spaarverlof. Dit wordt veroorzaakt doordat de medewerkers van de Meldkamer Midden-Nederland in 2025 in dienst zijn getreden bij de VRU. Daarbij zijn de verlofrechten van de voorgaande organisaties overgenomen. Voor wat betreft de financiële afwikkeling zal de VRU de samenwerkende organisaties om een bijdrage vragen. De VRU onderzoekt nog of de overname van deze rechten gefactureerd dient te worden inclusief of exclusief BTW. De VRU gaat een onderzoek uitvoeren op welke wijze deze rechten opgenomen kunnen gaan worden door medewerkers zodat de omvang in de komende tijd afneemt en (misschien nog wel belangrijker) medewerkers verlof opnemen. Wij plaatsen daarbij wel de kanttekening dat zodra grote groepen medewerkers ineens verlof opnemen er binnen de flexibele schil vervanging gevonden moet worden.

Eshuis

De belangrijke risico's

De belangrijkste risico's

Wij vinden het van belang dat u weet waar wij bij uw organisatie de belangrijkste risico's zien die tot mogelijke afwijkingen dan wel onzekerheden in de jaarrekening van uw organisatie kunnen leiden. Bij onze inschatting van de risico's laten wij ons leiden door bijv.de bevindingen van de VIC, belangrijke gebeurtenissen en voorschriften van onze beroepsorganisatie. De belangrijkste risico's zijn dus niet dingen die zeker fout gaan, maar de risico's waar zich fouten kunnen voordoen die van invloed kunnen zijn op onze verklaring. U kunt dit zien als de lijst met onderwerpen waar de accountant in ieder geval op gaat letten. Voor het jaar 2025 onderkennen wij de volgende belangrijkste risico's:

Risico	Motivatie	Normaal risico	Significant risico	Fraude-risico	Plan steunen op AO/IB
Doorbreken interne beheersing door het management risico is niet direct gerelateerd aan onze eigen observaties en bevindingen binnen de gemeenschappelijke regeling. Dit risico kan zich echter wel voordoen bij met name memoriaalboekingen, boekingen buiten de reguliere bedrijfsvoering om en transacties met verbonden partijen.	Het hiernaast genoemde risico ziet niet toe op een specifieke post, maar is op basis van onze controlestandaarden voorgeschreven bij iedere controle. De daaraan gekoppelde standaard-werkzaamheden dienen door ons uitgevoerd te worden. Hiernaast dienen wij aanvullende werkzaamheden op te zetten en uit te voeren op (onderdelen van) de verantwoording, in casu de jaarrekening van de gemeenschappelijke regeling.	☐	☑	☑	☐
Ongeautoriseerde betalingen als gevolg van leemtes in de bankapplicatie en het proces van inlezen van de betaallijst	Als gevolg van leemtes in de AO/IB met betrekking tot het proces van inlezen en controleren van de betaallijst onderkennen wij dit significante risico. Gelden kunnen onttrokken worden uit de organisatie, en dat betreft een frauderisico.	☐	☑	☑	☐
Het risico is onder andere gericht op het voldoen aan de WNT van de volgende onderwerpen: • overeenkomsten met topfunctionarissen • gemaakte afspraken / regelingen • bezoldiging / ontslaguitkering • of materiele bedragen de WNT toetsing niet ontlopen	Wij onderkennen een significant risico bij de WNT-verantwoording vanwege de zeer lage materialiteit, complexe regelgeving en de vele uitzonderings-bepalingen. De WNT bevat strikte normen, maar ook diverse interpretaties en overgangsregelingen die de juiste toepassing bemoeilijken. Onjuiste verantwoording kan leiden tot boetes, terugvorderingen en reputatieschade. Daarom achten wij extra aandacht noodzakelijk voor de naleving van de WNT in de jaarrekening, om het risico op materiële fouten te beperken.	☐	☑	☐	☐

De belangrijkste risico's

Risico	Motivatie	Normaal risico	Significant risico	Fraude-risico	Plan steunen op AO/IB
De rechtmatigheidsverantwoording geeft geen getrouw beeld.	Voor de controle verwachten wij verdere verduidelijking via aanvullende handleidingen van of de commissie BBV en/of de NBA. De controle blijft desalniettemin relatief nieuw en complex. Ondanks deze factoren hebben wij vastgesteld dat de organisatie in staat is om zowel methodologisch als controletechnisch controle-werkzaamheden uit te voeren en op de juiste wijze de verantwoording in te vullen. Wij onderkennen derhalve een normaal risico bij de rechtmatigheids-verantwoording.	☑	☐	☐	☑

De aard van deze risico's brengt met zich mee dat wij met name bij de controle van de jaarrekening hier aandacht aan besteden. In ons accountantsverslag dat wij naar aanleiding van de controle van de jaarrekening uitbrengen zullen wij rapporteren hoe deze risico's naar een acceptabel niveau zijn verlaagd.

Eshuis

Totaaloverzicht procesbeheersing

Totaaloverzicht procesbeheersing

Tijdens deze interim-controle richten wij ons vooral op de opzet en bestaan van de administratieve organisatie. Wij verrichten werkzaamheden ten aanzien van de procedures binnen de organisatie voor zover deze van belang zijn om een oordeel te vormen over de getrouwheid van de jaarrekening van de VRU. Wij hebben hieronder een samenvatting opgenomen van de getoetste processen. Voor onderliggende details en bevindingen verwijzen wij naar het hoofdstuk detailbevindingen.

Onze algemene indruk van de gehele administratieve organisatie en interne beheersing binnen VRU is ongewijzigd ten opzichte van eerdere jaren. Dit houdt met name verband met de bevindingen uit eerdere jaren die nog niet opgelost zijn en het feit dat wij geen nieuwe bevindingen hebben geconstateerd. Wij constateren wel dat het beleid en het opnemen van prestatielevering bij inkoopfacturen voor verbetering vatbaar zijn ondanks dat acties ingezet zijn. De gewenste resultaten zijn helaas nog niet zichtbaar voor ons en wij vragen wederom uw aandacht voor dit onderwerp.

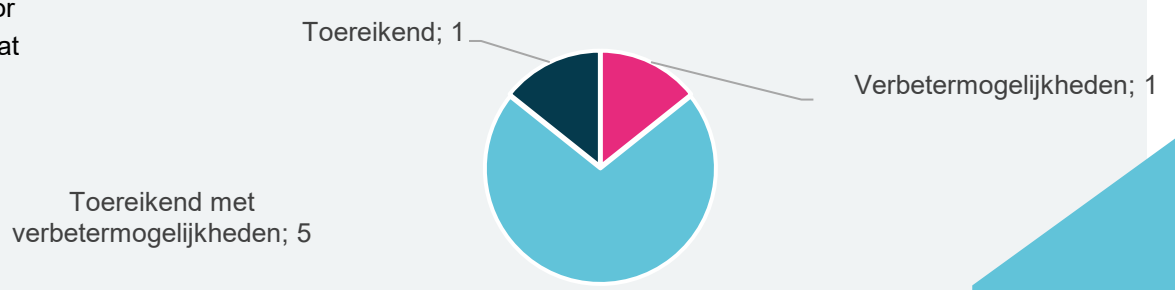
Ten aanzien van de verbijzonderde interne controle merken wij op dat de organisatie voor het derde jaar de volledige verantwoordelijkheid draagt voor het uitvoeren van de financiële rechtmatigheidscontroles. Wij constateren dat de VRU op dit onderdeel achterloopt en vragen u om prioriteit te geven aan het inhalen van deze achterstand. Tevens vragen wij u om tijdig met ons te schakelen indien blijkt dat het inhalen van deze achterstand een te grote uitdaging is. Hiermee zorgen we er samen voor dat capaciteit- en procestempo niet te koste gaan van kwaliteit.

Voor wat betreft het herzien van het auditplan is er in uw geval sprake van een verlichting, omdat de verantwoordingsgrens omhoog gaat. Dit is ook het moment om te kijken welke transactiestromen en rechtmatigheidsvereisten uit uw normenkader niet langer getoetst zouden moeten worden.

Wij adviseren u om deze herijkingsexercitie in samenhang te lezen met onze evaluatie van de IT-omgeving in hoofdstuk IT-audit. Ook bij VRU is het mogelijk om zekerheid te verkrijgen uit de 1e lijn i.c.m. IT systemen en daarmee de bedrijfsvoering te ondersteunen. Die optimalisatieslag geldt ook de controle van de VIC-functie voor de rechtmatigheidsverantwoording en daarmee ook voor de accountantscontrole. Daarmee kan de capaciteit die u tot uw beschikking heeft, worden ingezet op die aandachtsgebieden die menselijke oordeelsvorming vragen.

Het proces met verbetermogelijkheden betreft het gebruik van de bankapplicatie inclusief betaallijsten. Deze constatering houdt verband met de geconstateerde tekortkomingen zoals benoemd op de volgende pagina's. Hierin zien wij nog belangrijke aandachtspunten. Overigens merken wij op dat deze leemte veroorzaakt wordt door de leverancier van het financieel pakket. De verwachting is dat in het voorjaar van 2026 een werkende koppeling beschikbaar is. De overige processen voldoen aan de daaraan vanuit de accountantscontrole te stellen eisen.

Conclusies per getoetst proces



Totaaloverzicht procesbeheersing

Onderstaand vatten wij ons oordeel over de opzet en het bestaan per proces samen. Ten aanzien van opzet en bestaan geven wij het proces een classificatie mee:

- **Verbetermogelijkheden**: Binnen het proces is sprake van significant risico en/of er is sprake van verschillende tekortkomingen/observaties binnen de AO/IB en vragen hier op korte termijn uw aandacht voor;
- **Toereikend met verbetermogelijkheden**: Binnen het proces is sprake van verhoogd risico en/of er is sprake van verschillende observaties binnen de AO/IB en vragen hier op middellange termijn uw aandacht voor;
- **Toereikend**: Binnen het proces is sprake van risico en er is geen sprake van observaties binnen de AO/IB. Hiermee concluderen wij dat dit proces in opzet en bestaan voldoende is om het proces van het opstellen van de jaarrekening te ondersteunen.

Proces	Conclusie opzet en bestaan 2025	Conclusie opzet en bestaan 2024
Administratie & verslaglegging	Toereikend met verbetermogelijkheden	Toereikend met verbetermogelijkheden
Inkopen & aanbesteden	Toereikend met verbetermogelijkheden	Toereikend met verbetermogelijkheden
Factuurverwerking en betalingen	Toereikend met verbetermogelijkheden	Toereikend met verbetermogelijkheden
Opbrengstenstromen	Toereikend met verbetermogelijkheden	Toereikend met verbetermogelijkheden
Personeel en salarisadministratie	Toereikend	Toereikend
Fraude- en anti-corruptiebeheersing	Verbetermogelijkheden	Verbetermogelijkheden
Geautomatiseerde omgeving	Toereikend met verbetermogelijkheden	Toereikend met verbetermogelijkheden

Totaaloverzicht procesbeheersing

Bijgaande legenda is ten behoeve van de bevindingen op de volgende pagina's:

	Nieuwe bevinding
	Eerder gerapporteerde bevinding, niet opgelost
	De bevinding uit eerdere jaren ziet toe op een laag risico. Derhalve heeft de organisatie ervoor gekozen om de beheersing op dit proces op een ander moment in de controlecyclus alsmede elders in de organisatie onder te brengen. Wij onderschrijven deze keuze van de organisatie.
	Bevinding opgelost / beheersing voldoende

	Significante bevinding met een **hoog risico** en potentieel een grote impact op de jaarrekening, compliance en/of operationele prestaties. Een bevinding waar het management direct actie op moet ondernemen.
	Bevinding met een **gemiddeld risico** en potentieel een gemiddelde impact op de jaarrekening, compliance en/of operationele prestaties. Een bevinding waarvoor stappen dienen te worden genomen door het management gebaseerd op een actieplan, inclusief einddata.
	Bevinding met een laag risico en potentieel een **lage impact** op de jaarrekening, compliance en/of operationele prestaties. Een bevinding waarvoor actie voor kan worden ondernomen door het management, maar waarvan het risico ook kan worden geaccepteerd.

Totaaloverzicht procesbeheersing

Hieronder vindt u een overzicht van de geconstateerde bevindingen. Voor details verwijzen wij naar hoofdstuk detailbevindingen financiële interim.

Nr.	Bevinding	Status 2025	Status 2024
1	**Personeel & salarisadministratie** – Handmatige verwerking presentie bij vrijwilligers	↻	↻
2	**Anti-corruptieprogramma** – Het anti-fraude en –corruptieprogramma en de omgang met integriteits-meldingen kan verder worden versterkt	↻	↻
3	**Inkopen en aanbestedingen** – Prestatielevering	↻	↻
4	**Factuurverwerking & betalingen** – Mogelijkheid tot omzeilen vierogenprincipe bij betalingen	↻	!
5	**Personeel & salarisadministratie** – Controle op declaraties	↻	!

De bevindingen gerelateerd aan de IT-audit zijn opgenomen in navolgend hoofdstuk. Wij merken op dat een aantal bevindingen nog onderhanden zijn. Daarom vinden wij het van belang om u te voorzien van een inhoudelijke updaten ten aanzien van deze punten. De bevindingen in het personeelsproces zien toe op een laag risico, en vragen de nodige procesmatige aanpassingen alsmede automatiseringsslag. De VRU heeft het implementeren en verbeteren van de registratie en afscherming van integriteitsmeldingen nog onderhanden. Het beoordelen en zichtbaar controleren van nevenfuncties zijn voor verbetering vatbaar. Ten aanzien van prestatielevering merken wij op dat het (tijdig) vastleggen van de prestatielevering in AFAS voor verbetering vatbaar is. Daarnaast kan het beleid rondom prestatielevering verder aangescherpt worden door op basis van een risicoanalyse vast te stellen op welke deelpopulaties sprake is van een verhoogd risico op het indien van onjuiste/onrechtmatige facturen. Hierbij valt bijvoorbeeld te denken aan de inhuur van derden. De VRU wil de nodige verandering op korte termijn realiseren door in AFAS te werken met een drempelbedrag. De VRU heeft met haar leverancier afspraken gemaakt om de beheersing van de betalingsomgeving in 2026 naar een hoger niveau te tillen.

Eshuis

IT-audit

Per saldo persoonlijker

IT-audit

In dit digitale tijdperk, waarbij organisaties geautomatiseerde informatietechnologie (IT)-systemen gebruiken om hun informatie te verwerken voor een betere ondersteuning van hun missies, spelen IT-risico's en controles een cruciale rol bij het beschermen van de informatiemiddelen van een organisatie en daarmee van haar missie. Het belangrijkste doel van een organisatie in het kader van (IT) risico's & controles, zou moeten zijn: het beschermen van de organisatie en haar vermogen om de geformuleerde missie uit te voeren, en niet enkel de IT-middelen. Wij zijn van mening dat een effectieve IT-risico- en beheeromgeving, een belangrijk onderdeel is van een succesvolle IT-strategie welke onderdeel uitmaakt van de bedrijfsstrategie.

Onze jaarrekeningcontrole is gericht op het geven van een oordeel over de jaarrekening zelf en is niet primair gericht op het doen van uitspraken over de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan. Onze bevindingen hebben betrekking op de onderdelen die wij onderzocht hebben in het kader van de jaarrekening, wat wil zeggen dat wij geen volledigheid pretenderen.

In het kader van de jaarrekeningcontrole over het boekjaar 2025 heeft Eshuis IT-audit werkzaamheden uitgevoerd met betrekking tot de opzet en het bestaan van de algemene ICT beheersmaatregelen binnen de automatiseringsomgeving van de VRU. Wij hebben daarbij uitsluitend die maatregelen getest die het meest relevant zijn in het kader van de jaarrekeningcontrole. Tijdens de werkzaamheden zijn de algemene IT beheersmaatregelen in opzet en bestaan beoordeeld van de meest kritische applicaties rond de salarisadministratie, de inkoopfactuurverwerking en het grootboek.

Wij hebben enkele bevindingen geconstateerd waar verbetering nodig is, zeker ook in relatie tot nieuwe regelgeving met betrekking tot de op 23 september 2025 vastgestelde BIO2. Cruciaal is het verder professionaliseren van de periodieke beoordelingen die ook vanuit de BIO2 worden verwacht op toegang, maar ook het in lijn brengen van het wachtwoordbeleid met de norm conform de BIO2.

IT-audit

Benadering en scope

Ten behoeve van de jaarrekeningcontrole hebben wij voor elk van deze bevindingen onze eigen classificatie bepaald op basis van prioriteit van opvolging, waarbij drie niveaus zijn onderscheiden: hoog, midden en laag. Het management blijft verantwoordelijk voor haar eigen oordeelsvorming over de inschatting van de risico's als gevolg van de geconstateerde bevindingen, de daarvan af te leiden prioriteitstelling en de opvolging van de aanbevelingen.

Tijdens de werkzaamheden voor de 2025 jaarrekeningcontrole zijn voor de VRU de algemene IT beheersmaatregelen in opzet en bestaan beoordeeld voor de volgende applicaties:

Betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking

Overeenkomstig artikel 2:393, lid 4 van het Burgerlijk Wetboek zijn wij verplicht om onze bevindingen te rapporteren met betrekking tot de betrouwbaarheid en continuïteit van uw geautomatiseerde gegevensverwerking. Onze controle heeft geen aangelegenheden geïdentificeerd die op dit gebied aan u gerapporteerd moeten worden, anders dan de waarnemingen zoals hiervoor besproken.

Applicatie	Besturingssysteem	Database	Datacenter locatie
AFAS Online	SAAS oplossing, derhalve onderdeel van ISAE 3402 type II.	SAAS oplossing, derhalve onderdeel van ISAE 3402 type II.	SAAS oplossing, derhalve onderdeel van ISAE 3402 type II.
Veiligheidspaspoort	SAAS oplossing, echter geen ISAE 3402 type II rapport beschikbaar.	SAAS oplossing, echter geen ISAE 3402 type II rapport beschikbaar.	SAAS oplossing, echter geen ISAE 3402 type II rapport beschikbaar.

IT-audit

Hieronder vindt u een overzicht van de geconstateerde bevindingen, inclusief de stand van zaken ten aanzien van in eerdere jaren geconstateerde bebindingen. Voor details verwijzen wij naar hoofdstuk detailbevindingen IT audit.

Nr.	Bevinding	Status 2025	Status 2024
1	**Wijzigingsbeheer -** Geïnstalleerde wijzigingen tot AFAS en VP worden niet eerst getest op basis van een zichtbaar vastgesteld testprotocol en akkoord bevonden in een acceptatieomgeving, in tegenstelling tot het gestelde beleid binnen de VRU.		
2	**Toegangsbeheer -** Hoge rechten te ruim uitgegeven aan personen vanuit de lijnorganisatie, die geen toegang zouden moeten hebben. Ook vastgesteld dat de VRU gebruik maakt van generieke accounts en testaccounts met hoge rechten accounts in VP en AFAS, wat niet wenselijk is. Tevens beschikken externe consultants over continue beheerderstoegang tot AFAS.		
3	**Toegangsbeheer** – Periodieke review op toegang tot AFAS en VP ontbreekt: A) Er is geen zichtbare periodieke review uitgevoerd door afdelingshoofden op de actieve gebruikers binnen AFAS en VP. B) Er ontbreekt een zichtbare periodieke review op de verschillende rechten en rollen van de actieve gebruikers. C) Tevens ontbreekt een onderliggende functiematrix waarmee functiescheiding tussen gebruikersrollen wordt aangetoond.		

IT-audit

Legenda:

●	Significante bevinding met een hoog risico en potentieel een grote impact op de jaarrekening, compliance en/of operationele prestaties. Een bevinding waar het management direct actie op moet ondernemen.
●	Bevinding met een gemiddeld risico en potentieel een gemiddelde impact op de jaarrekening, compliance en/of operationele prestaties. Een bevinding waarvoor stappen dienen te worden genomen door het management gebaseerd op een actieplan, inclusief einddata.
●	Bevinding met een laag risico en potentieel een lage impact op de jaarrekening, compliance en/of operationele prestaties. Een bevinding waarvoor actie voor kan worden ondernomen door het management, maar waarvan het risico ook kan worden geaccepteerd.

	Nieuwe bevinding
	Eerder gerapporteerde bevinding, niet opgelost
✓	Bevinding opgelost / beheersing voldoende
⊘	Niet getest

Eshuis

Detailbevindingen IT-audit

Per saldo persoonlijker

Bevindingen IT-audit

Nr. 1 - Wijzigingsbeheer	**Geïnstalleerde wijzigingen tot AFAS en VP worden niet eerst getest op basis van een zichtbaar vastgesteld testprotocol en akkoord bevonden in een acceptatieomgeving, in tegenstelling tot het gestelde beleid binnen de VRU. Daarnaast heeft de VRU de acceptatieomgeving van AFAS nog niet ingericht, waardoor er geen mogelijkheid bestaat om een adequaat wijzigingsbeheerproces te volgen.**
Beschrijving control	GITC-10: Applicatie wijzigingen zijn op gepaste wijze getest en goedgekeurd voordat ze doorgevoerd worden naar de productie omgeving
Observatie	Wij hebben het volgende geconstateerd: • Geïnstalleerde wijzigingen tot AFAS en VP worden niet eerst getest op basis van een vastgesteld testprotocol en akkoord bevonden in een acceptatieomgeving, dit in tegenstelling tot het gestelde beleid binnen de VRU. Daarnaast ontbreken testplannen hiervoor, met daarin aan de voorkant geïdentificeerde kritische functionaliteit van de VRU.
Impact	Het risico bestaat dat er ongeautoriseerde wijzigingen vanuit de ontwikkelfase in het systeem direct worden doorgevoerd. Hierdoor bestaat het risico dat er fouten worden geïnstalleerd op de productieomgeving, waardoor het zelfs mogelijk is dat het systeem niet meer bruikbaar is totdat herstel heeft plaatsgevonden.
Aanbeveling	Het verdient aanbeveling om zichtbare testwerkzaamheden uit te voeren voordat wijzigingen tot de productieomgeving worden geïnstalleerd. Deze werkzaamheden dienen te worden vastgelegd waarbij inzichtelijk wordt gemaakt dat er testen zijn uitgevoerd en dat goedkeuring is verleend door het management voor het doorvoeren van de wijziging tot de productie-omgeving. Verder benadrukken wij dat deze bevinding toe ziet op de volgende verplichte maatregelen vanuit de BIO2 die vanuit de NIS2 als zorgplicht gelden: • Beheersmaatregel 8.32 Wijzigingsbeheer: Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer. • Beheersmaatregel 8.32.01 In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: • het administreren van wijzigingen, hierin ook de resultaten van het testplan; • risicoafweging van mogelijke gevolgen van de wijzigingen hieronder ook een beschreven rollbackplan; • goedkeuringsprocedure voor wijzigingen. • Beheersmaatregel 8.32.02 Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.

Bevindingen IT-audit

Nr. 2 - Toegangsbeheer	**Hoge rechten te ruim uitgegeven aan personen vanuit de lijnorganisatie, die geen toegang zouden moeten hebben. Ook vastgesteld dat de VRU gebruik maakt van generieke accounts en testaccounts met hoge rechten accounts in VP en AFAS, wat niet wenselijk is. Tevens beschikken externe consultants over continue beheerderstoegang tot AFAS.**
Beschrijving control	GITC-06: Toegang op Privilegeniveau (bijv. configuratie, gegevens en veiligheidsbeheerders) is geautoriseerd en op gepaste wijze beperkt
Observatie	AFAS Online Wij hebben vastgesteld middels inlichtingen en inspectie van, vastgesteld dat er 12 accounts bestaan in AFAS met applicatiebeheer rechten (toegang tot de autorisatietool) waarvan: -2 accounts betrekking hebben op personen bij de softwareleverancier. Volgens werkafspraak hebben deze personen enkel op 'consultancydagen' toegang. Echter, in de praktijk blijkt dat betreffende accounts vaak niet worden geblokkeerd na afloop van 'consultancydagen'. VP Wij hebben vastgesteld middels inlichtingen en inspectie van systemen, dat er 4 accounts bestaan in VP omgeving met applicatiebeheer rechten, waarvan: - 2 accounts betrekking hebben op personen die formeel onderdeel zijn van de lijnorganisatie, wat niet wenselijk is.
Impact	Het risico bestaat dat als beheerrechten niet zijn beperkt tot gebruikers en accounts die rechten benodigd hebben voor het uitvoeren van hun functie dit kan leiden tot ongeautoriseerd toegang tot systemen, met daarbij het risico op onjuistheden en onvolledigheden in de data. Daarnaast doorbreken deze rechten alle functiescheiding die mogelijk is aangebracht binnen AFAS en VP, wat niet wenselijk is vanuit mogelijke cyber- en frauderisico's.
Aanbeveling	Het verdient aanbeveling om zorg te dragen dat beheerrechten in AFAS en VP beperkt worden uitgegeven en alleen worden uitgegeven aan individuele personen en accounts die dit benodigd hebben voor het uitvoeren van hun functie (lees IT verantwoordelijken). Daarnaast verdient het aanbeveling om dit periodiek te beoordelen op juistheid. Verder benadrukken dat deze bevinding toe ziet op de volgende verplichte maatregelen vanuit de BIO2 die vanuit de NIS2 als zorgplicht gelden: • Beheersmaatregel 5.03 Functiescheiding: Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden. • Beheersmaatregel 8.03.02 Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak. • Beheersmaatregel 8.02 Speciale toegangsrechten: Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd. • Beheersmaatregel 8.02.01 De uitgegeven of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld.

Bevindingen IT-audit

Nr. 3 - Toegangsbeheer	**A) Er is geen zichtbare periodieke review uitgevoerd door afdelingshoofden op de actieve gebruikers binnen AFAS/VP. B) Er ontbreekt een zichtbare periodieke review op de verschillende rechten en rollen van de actieve gebruikers. C) Tevens ontbreekt een onderliggende functiematrix waarmee functiescheiding tussen gebruikersrollen wordt aangetoond.**
Beschrijving control	GITC-03: Gebruikerstoegang wordt periodiek beoordeeld GITC-04: Functiescheiding wordt gemonitord en conflicterende toegang wordt verwijderd of toegewezen aan mitigerende interne beheersingsmaatregelen, die zijn gedocumenteerd en getoetst
Observatie	Tijdens onze controlewerkzaamheden hebben wij vastgesteld dat er is geen zichtbare periodieke review wordt uitgevoerd door afdelingshoofden op de actieve gebruikers binnen AFAS/VP. Hierdoor ontbreekt ook een zichtbare periodieke review op de verschillende rechten en rollen van de actieve gebruikers. Tevens ontbreekt een onderliggende functiescheidingsconflictenmatrix waarmee functiescheiding tussen gebruikersrollen wordt aangetoond. Met een dergelijke functiescheidingsconflictenmatrix wordt beoogd om schematisch aan te tonen dat op groepsrollen de nodige functiescheiding is gewaarborgd, waardoor leidinggevende een juiste afweging kunnen maken bij het aanvragen van rechten voor nieuwe gebruikers. Dit geldt tevens als controlemiddel in de periodieke review die minstens jaarlijks dient plaats te vinden.
Impact	Het risico bestaat dat als rechten niet juist zijn beperkt tot gebruikers en accounts die deze rechten benodigd hebben voor het uitvoeren van hun functie dit kan leiden tot ongeautoriseerde transacties.
Aanbeveling	Wij bevelen aan om de actieve gebruikers van AFAS Online en VP per kwartaal te onderwerpen aan een controle van de directe leidinggevende en aan de hand van gegevens in AFAS ter toetsing of deze account überhaupt toegang zouden moeten hebben tot het systeem. Wij bevelen daarnaast aan om middels een functiescheidingsconflictenmatrix op praktische wijze de functiescheiding inzichtelijk te maken in de huidige rollen binnen AFAS Online en VP. Deze matrix dient dan als norm dienen in de periodieke review, naast beschikbare autorisatiematrices (SOLL-matrix). Verder benadrukken wij dat deze bevinding toeziet op de volgende verplichte maatregelen vanuit de BIO2 die vanuit de NIS2 als zorgplicht gelden: • Beheersmaatregel 5.18.02 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. Een risicoafweging bepaalt of dit sneller moet. • Beheersmaatregel 8.02.01 De toegewezen of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld. • Beheersmaatregel 5.03 Functiescheiding: Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden

Eshuis

Actualiteiten & Vooruitblik

Per saldo persoonlijker

Actualiteiten & vooruitblik

Verslaggevingskader

In het BBV bevat ten opzichte van voorgaand jaar een aantal wijzigingen. Eén betreft de vereisten rondom verbonden partijen. De Wet gemeenschappelijke regelingen (Wgr) is per 1 juli 2022 gewijzigd. De voornaamste doelstelling van deze wet is om de positie van gemeenteraden binnen gemeenschappelijke regelingen te versterken. Het BBV heeft ten aanzien van verbonden partijen de volgende drie categorieën veranderingen voorgesteld:

• Versterking van de positie van gemeenteraden bij besluitvorming in gemeenschappelijke regelingen.

• Introductie van aanvullende controle-instrumenten voor gemeenteraden.

• Verbetering van de positie van gemeenteraden met betrekking tot het functioneren van de regeling.

Daarnaast is de notitie structurele en incidentele baten en lasten in 2025 herzien. Hierin staat het onderscheid tussen structureel en reëel evenwicht centraal. Voor het inzicht in de financiële positie op korte en langere termijn is het voor de raad van groot belang om een goed beeld te hebben van het structureel begrotingssaldo. Ook bij het nemen van besluiten met grotere financiële gevolgen is het van belang dat raadsleden kunnen zien wat de gevolgen daarvan zijn op langere termijn.

Daarnaast merken wij op dat de controleverklaring onderdeel moet zijn van de integrale jaarstukken. De indeling van de inhoudsopgave is anders doordat op het hoofdniveau de rechtmatigheidsverantwoording vermeld moet gaan worden.

Kadernota Rechtmatigheid 2025

De commissie BBV heeft in september 2025 de nieuwe Kadernota Rechtmatigheid 2025 uitgebracht. De belangrijkste wijzigingen zijn:

- De verantwoordingsgrens valt vanaf 2025 binnen de bandbreedte van 0% tot 2% van de totale lasten van de organisatie. Dit was tot en met 2024 binnen de bandbreedte van 0% tot 3%.
- Het percentage voor de verantwoordingsgrens geldt vanaf 2025 voor de rechtmatigheidsfouten en onduidelijkheden samen. Tot en met 2024 gold het percentage van de verantwoordingsgrens afzonderlijk voor rechtmatigheidsfouten en voor onduidelijkheden.
- Vanaf 2025 geldt dat de omvangbasis voor het percentage van de verantwoordingsgrens de lasten van de gemeenschappelijke regeling exclusief toevoegingen aan de reserves is. Tot en met 2024 was dit inclusief toevoegingen aan de reserves.

De aanscherping van de controlegrenzen zoals die met ingang van 2025 is ingevoerd door een wijziging in het besluit accountantscontrole decentrale overheden zorgt, zeker in combinatie met de kadernota rechtmatigheid 2025, voor een vernieuwde focus op de wijze waarop in de controle en in de rechtmatigheidsverantwoording omgegaan wordt en kan worden met het begrip 'onzekerheden' en 'onduidelijkheden'. We zien dat regelmatig het identificeren van een onzekerheid het eindpunt van de controle is geworden.

De aanscherping van het BADO zorgt ervoor dat de controlemarges smaller worden. Onzekerheden zullen daardoor in de praktijk sneller leiden tot een aangepast oordeel. Vanuit ons perspectief, zeker bij een aangepast oordeel, is het identificeren van een onzekerheid het startpunt van een vervolgproces. Niet zelden wordt het ontbreken van informatie meteen vertaald in een onzekerheid.

Actualiteiten & vooruitblik

In dergelijke situaties dient u echter aantoonbaar en tijdig inspanningen te verrichten om de informatie alsnog te verkrijgen. Dat kan door bijvoorbeeld zelfstandig (eigen) onderzoek te doen door aanvullende informatie uit te vragen bij verbonden partijen of leveranciers of door schattingen beter te onderbouwen. Daardoor kunnen onzekerheden worden verkleind of opgelost.

Indien organisaties dit eigen onderzoek niet doen of niet kunnen doen, zullen wij dit onderzoek zelfstandig alsnog moeten gaan verrichten. De aard van het onderzoek hangt af van de exacte situatie, onze risico-inschatting en de wel aanwezige informatie. Het is evident dat deze laatste optie niet onze voorkeur heeft maar ook onherroepelijk leidt tot druk op de bestuurlijke planning van de jaarrekening 2025. Tijdgebrek of bestuurlijke afspraken zijn immers geen vrijbrief om dit onderzoek niet uit te voeren. Om die reden adviseren wij u dan ook om na te gaan of de ervaringen uit het verleden aanleiding kunnen zijn om afspraken over de aanlevering van informatie te herzien of voorbereidingen te treffen om zelfstandig onderzoek uit te voeren.

Wij wijzen erop dat met name adequate onderbouwingen van schattingsposten en zichtbare toets op schattingen uit het verleden, voor verbetering vatbaar zijn.

Onder voorgenoemde schattingen valt bij uw organisatie te denken aan:

- Verplichtingen rondom vrijwilligersvergoedingen over 2025 die in 2026 worden uitbetaald;
- Bijstelling en onderbouwing van de voorziening RVU;
- Onderzoek en onderbouwing op de oplopende verlofsaldi inclusief het (eventueel) opnemen van een voorziening voor het niet jaarlijks gelijkblijvende deel;
- Onderzoek en onderbouwing van (eventuele) verplichtingen uit hoofde van overige personele verplichtingen, waaronder bijvoorbeeld de regeling PTSS;
- Onderzoek en onderbouwing van overige verplichtingen die ontstaan uit de activiteiten van de organisatie, bijvoorbeeld naar aanleiding van juridische procedures, rechtszaken en/of claims.

Voor de onduidelijkheden in de rechtmatigheidsverantwoording geldt dat met name in juridisch complexe situaties hier sprake van kan zijn. Dat betekent ook dat een dergelijke identificatie tevens een opdracht inhoudt voor de directie om deze onduidelijkheid op te lossen. Het is een hoge uitzondering dat deze situatie in continuïteit voortduurt. Dezelfde kwestie meer dan eens aanduiden als onduidelijk, kan erop wijzen dat onvoldoende inspanningen zijn verricht om de onduidelijkheid op te lossen. Ook het bijvoorbeeld uitfaseren in de tijd van de onduidelijkheid, wat in aanbestedingsvraagstukken kan voorkomen, is in beginsel niet mogelijk. Ook hiervoor geldt dat wij in voorkomende gevallen u zullen vragen de onduidelijkheid alsnog op te heffen.

WNT

De algemene bezoldiging voor een topfunctionaris mag voor 2026 niet meer bedragen dan € 262.000 per jaar. Daarnaast dienen instellingen de salarissen openbaar te maken van overige medewerkers (inclusief – wanneer aan bepaalde voorwaarden is voldaan – ingehuurd personeel) die een bezoldiging ontvangen boven deze norm. Ten slotte stelt de WNT een aantal overige eisen, zoals een maximale ontslagvergoeding voor topfunctionarissen van € 75.000.

Actualiteiten & vooruitblik

NIS2, Cyberbeveiligingswet, BIO2 en ENSIA IT audit

Met de recente ontwikkelingen op het gebied van informatiebeveiliging binnen de overheid informeren wij u over veranderingen die als gevolg van ketenaansprakelijkheid een impact zullen hebben op uw gemeenschappelijke regeling. Deze ontwikkelingen zijn relevant voor risicomanagement en de naleving van nieuwe wet en regelgeving op het gebied van informatiebeveiliging.

NIS2 – Europese richtlijn voor cyberweerbaarheid

De NIS2 is reeds sinds 16 januari 2023 in werking getreden en dient te worden omgezet in nationale wetgeving door de lidstaten van de Europese Unie. Deze NIS2 richtlijn verplicht onder andere overheidsorganisaties en vitale sectoren om hun cyberweerbaarheid versterkt in te richten en incidenten tijdig te melden. De BIO2 fungeert als normenkader waarmee gemeenten (waaronder ook gemeenschappelijke regelingen) en andere overheidslagen aan de NIS2 eisen kunnen voldoen, te weten de meest wezenlijke plicht namelijk de zorgplicht.

Voor uw organisatie betekent dit:

- het treffen van passende en evenredige technische, operationele en organisatorische maatregelen om de risico's te beheren en afgestemd op de voor de organisatie relevante risico's en deze beheersen;
- het goedkeuren van te nemen maatregelen voor het beheer van cyberbeveiligingsrisico's;
- het toezien op de kwaliteit van de uitvoering en het beheer van de maatregelen.

Cyberbeveiligingswet – verwachte implementatie

De Cyberbeveiligingswet is de omzetting in nationale wetgeving van de Europese NIS2-richtlijn. Deze richtlijn heeft als doel om de weerbaarheid van de lidstaten van de Europese Unie te versterken door ervoor te zorgen dat organisaties voldoende weerbaar zijn tegen allerlei dreigingen. De Rijksoverheid roept organisaties dan ook op om zich voor te bereiden op de komst van de wet en de onderliggende regelgeving.

In de week van 10 november 2025 zijn er diverse concept ministeriële regelingen onder de Cyberbeveiligingswet uitgebracht die uitvoering geven aan de Cbw en waarop tot en met 21 december 2025 kan worden gereageerd. De ministeriële regelingen vormen de nadere uitwerking van de Cyberbeveiligingswet, de Wet weerbaarheid kritieke entiteiten, het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten. De meeste departementen zullen een eigen ministeriële regeling opstellen voor de sectoren waarvoor zij verantwoordelijk zijn. Zo ook voor uw als decentrale overheid, waarbij Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zal komen met deze regeling. Meest wezenlijke hierin betreft de zorgplicht en de invulling hiervan door de vaststelling van de nieuwe BIO2 normen. De maatregelen die decentrale overheden vanuit de aankomende Cyberbeveiligingswet moeten nemen, kosten tijd en aandacht. Daarom adviseren wij u om niet af te wachten tot de inwerkingtreding, maar om alvast voorbereidingen te treffen.

BIO2 – Vernieuwd normenkader voor informatiebeveiliging (zorgplicht)

In augustus 2024 is de vernieuwde Baseline Informatiebeveiliging Overheid (BIO2) gelanceerd en formeel vastgesteld door het Overlegorgaan Baseline Informatiebeveiliging Overheid (OBDO) op 23 september 2025 en is te vinden op de website van de BIO-overheid.

Actualiteiten & vooruitblik

Daarmee is BIO2 het leidende normenkader geworden voor informatiebeveiliging binnen de gehele overheid. De nieuwe BIO2 zal uiteindelijk wettelijk verankerd zal worden in de Cbw. Decentrale overheden blijven tot de inwerkingtreding van de Cbw formeel de BIO 1.04 gebruiken, maar kunnen de BIO2 nu al toepassen als richtinggevend kader.

Belangrijke kenmerken van BIO2:

• De BIO2 is opgebouwd volgens de internationale normen NEN EN ISO/IEC 27001 en NEN EN ISO/IEC 27002.

• De BIO2 is in lijn gebracht met de NIS2 richtlijn en de Cyberbeveiligingswet (Cbw), als juridisch kader voor de sector Overheid.

• De BIO2 bevat overheidsmaatregelen zoals "basishygiëne", "ketenhygiëne" en "overheidsrisico's".

Een voorbeeld van een ingrijpende verandering door de komst van de BIO2 betreft de vereisten rondom assurancerapportages van uw leveranciers. De BIO2 introduceert in maatregel 5.20.03 een belangrijke verplichting voor ketenbeveiliging. Deze maatregel vereist dat alle softwareleveranciers die diensten of systemen leveren rondom kritische processen aan overheidsorganisaties beschikken over een onafhankelijke assurance-rapportage (zoals een ISAE- of SOC-verklaring).

Deze verplichting geldt niet alleen voor commerciële leveranciers, maar ook voor samenwerkende gemeenten, regionale ICT-samenwerkingen en gemeenschappelijke regelingen die software of digitale diensten ontwikkelen, beheren of hosten voor andere overheden. Hiermee waarborgt de BIO2 dat elke schakel in de keten aantoonbaar voldoet aan de beveiligingseisen en voorkomt dat onvoldoende beveiliging bij één partij risico's oplevert voor de gehele overheid.

Een andere belangrijke wijziging is de opname van beheersmaatregel 5.17.01 uit de BIO2 die duidelijke eisen stelt aan het gebruik van Single Sign-On (SSO) en Multi-Factor Authenticatie (MFA) binnen overheidsorganisaties. In de praktijk betekent dit dat veel organisaties hun huidige applicatielandschap moeten moderniseren.

Voor veel traditionele on-premise applicaties is namelijk geen veilige of volwaardige koppeling mogelijk met moderne identiteitsplatformen zoals Azure AD (Entra ID) of vergelijkbare identity providers. Daardoor kan MFA niet op het vereiste beveiligingsniveau worden toegepast. Als gevolg hiervan stappen steeds meer organisaties over naar SaaS-varianten van hun applicaties of moderniseren zij hun architectuur, zodat deze koppelbaar wordt met een centrale tenant in de "cloud". Hiermee wordt voldaan aan de strengere eisen voor sterke authenticatie, vermindert het risico op identiteitsmisbruik en wordt de beveiliging in lijn gebracht met de meest actuele normen binnen de BIO2 en NIS2-zorgplicht.

De twee beschreven aspecten — de verplichting tot assurancerapportages van softwareleveranciers (maatregel 5.20.03) en de strengere eisen voor SSO en MFA (maatregel 5.17.01) — zijn op zichzelf al zo ingrijpend dat zij voor iedere decentrale overheidsorganisatie strategische keuzes noodzakelijk maken. Deze veranderingen raken niet alleen de IT-afdeling, maar hebben brede impact op de hele organisatie. Ze vereisen investeringen in modernisering van applicatielandschappen, herziening van ketencontracten en governance, en aanpassing van operationele processen. Het succes van de implementatie hangt daarmee af van organisatiebreed commitment en samenwerking, waarbij bestuur of directie, beleid, beheer en uitvoerende afdelingen gezamenlijk verantwoordelijkheid moeten nemen om te voldoen aan de BIO2 en Cbw-zorgplicht.

Actualiteiten & vooruitblik

<u>RDI – Toezicht en handhaving</u>

De Rijksdienst voor Digitale Infrastructuur (RDI) fungeert als toezichthouder voor overheidsorganisaties — gemeenten, gemeenschappelijke regelingen, provincies en waterschappen. Zij bewaakt de naleving van de BIO2, de NIS2 richtlijn en de Cyberbeveiligingswet. Bij overtreding van de regelgeving kan de RDI boetes opleggen. Voor specifieke overtredingen is een boete van 2% van de jaaropbrengsten of omzet van de organisatie mogelijk.

Zodra de Cyberbeveiligingswet formeel door de Tweede en Eerste Kamer is aangenomen, zal de BIO2 dienen als het toetsingskader voor de zorgplicht onder de wet. Dit betekent dat het voldoen aan de BIO2 niet alleen normatief is, maar ook als juridisch referentiekader fungeert voor handhaving.

<u>Conclusie en advies</u>

De invoering van BIO2, de komst van de NIS2 richtlijn en de implementatie van de Cyberbeveiligingswet vraagt om een herziening van uw informatiebeveiligingsbeleid en auditprocessen. Wij adviseren om:

- Zo spoedig mogelijk te starten met de implementatie van de noodzakelijke maatregelen.
- De verantwoordelijkheden rond informatiebeveiliging opnieuw in te richten.

Door proactief aan de slag te gaan, zorgt uw organisatie ervoor dat zij tijdig voldoet aan de eisen van BIO2, NIS2 en de Cyberbeveiligingswet en voorkomt u mogelijke boetes tot 2 % van de jaaropbrengsten.

Eshuis

Bijlagen

Bijlage 1: Onafhankelijkheid

Wij zijn onafhankelijk van de VRU

De voorschriften in het kader van onafhankelijkheid zijn binnen de Koninklijke Nederlandse Beroepsorganisatie van Accountants (de NBA) opgenomen in de "Verordening inzake Onafhankelijkheid (ViO)" en vormen een belangrijk onderdeel van het 'normenkader' waaraan een accountant moet voldoen. De naleving van de ViO is binnen de organisatie van Eshuis ingebed.

Ons zijn geen relaties bekend tussen Eshuis Registeraccountants B.V. en haar zuster- en of dochterondernemingen en de gemeenschappelijke regeling, die naar ons professionele oordeel mogelijk van invloed kunnen zijn op onze onafhankelijkheid.

Stelsel van waarborgen om onze onafhankelijke positie te waarborgen

Eshuis beschikt over een stelsel van maatregelen om haar onafhankelijke positie bij controlecliënten te waarborgen. Dit stelsel van maatregelen is een integraal onderdeel van de bestuurlijke organisatie en van het voor de gehele organisatie van toepassing zijnde stelsel van kwaliteitsbeheersingsmaatregelen. Bijgaande niet-limitatieve opsomming geeft u een indruk van de maatregelen die bijdragen aan het waarborgen van onze onafhankelijke positie:

- Schriftelijke onafhankelijkheidsbepalingen waarin alle bestaande onafhankelijkheidsvereisten en de risico's ten aanzien van de bedreiging van de onafhankelijkheid en de daaraan gerelateerde waarborgen zijn verwerkt.
- Procedures voor tijdige bekendmaking van de voorschriften en de daarin aangebrachte wijzigingen aan alle partners en werknemers bij Eshuis.
- Procedures voor de organisatie van periodieke trainingen inzake de toepassing van de onafhankelijkheidsvoorschriften.
- Procedures die erop gericht zijn dat onze partners en werknemers in specifieke casussen en omstandigheden de onafhankelijkheidsvoorschriften naleven.
- Procedures voor het interne toezicht in relatie tot de toetsing en bewaking van de naleving van de onafhankelijkheidsvoorschriften.

Bijlage 2: Disclaimer en beperking in het gebruik

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

Hierdoor is onze analyse en evaluatie beperkter dan dat deze zou zijn geweest in het kader van een opdracht tot het geven van een oordeel omtrent de opzet, het bestaan, de effectiviteit en de efficiency van de interne beheersing als geheel en deze bestrijkt daarom niet noodzakelijkerwijze alle in de interne organisatie vervatte tekortkomingen. Wij attenderen u erop dat deze managementletter is opgesteld ten behoeve van het bestuur van de gemeenschappelijke regeling en daarom niet zonder onze toestemming aan derden mag worden verstrekt..