

MANAGEMENTLETTER 2024

# Gemeenschappelijke Regeling Werkvoorzieningschap Regio Eindhoven (Ergon)

Aan:

Ergon  
t.a.v. Ingrid Hems  
Rooijakkersstraat 3  
5652 BA Eindhoven

Eindhoven, 13 februari 2025

Kenmerk:  
1070002/RdLvW/SP/250042

**Geachte directie,**

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2024 van Gemeenschappelijke Regeling Werkvoorzieningschap Regio Eindhoven (hierna: Ergon) brengen wij met deze managementletter verslag uit over onze bevindingen naar aanleiding van onze interim-controle. Voor een nadere omschrijving van onze opdracht, de reikwijdte en aanpak van onze controle en overige afspraken verwijzen wij naar de opdrachtbevestiging 2024.

Deze managementletter bevat onze belangrijkste bevindingen ten aanzien van de processen binnen Ergon en de daarin opgenomen beheersingssystemen. In deze rapportage richten wij ons met name op mogelijke verbeterpunten in de bedrijfsvoering en de processen die wij hebben onderzocht in het kader van de controle van de jaarrekening en onze nulmeting. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelf controlerend vermogen van uw organisatie.

Tijdens onze bezoeken aan Ergon komen wij ook in aanraking met andere ontwikkelingen van uw organisatie en bedrijfsvoering. We bespreken graag een aantal van die andere ontwikkelingen met u. In deze managementletter besteden we daarom ook aandacht aan ontwikkelingen op andere gebieden dan de processen.

Op basis van Nederlands recht en overige beroepsregels, zoals de ‘Verordening inzake de onafhankelijkheid van accountants bij assuranceopdrachten’ (ViO), is vereist dat wij onafhankelijk zijn ten opzichte van onze controle-cliënten. Wij zijn van mening dat door ons is voldaan aan deze eisen. Wij verrichten op dit moment geen overige dienstverlening naast de controle van de jaarrekening.

Wij hopen u met dit verslag van dienst te zijn. Vanzelfsprekend zijn wij graag bereid om een nadere toelichting op de inhoud te geven.

*Met vriendelijke groet,*

BDO Audit & Assurance B.V.  
namens deze,

**drs. D.O. Meeuwissen RA**  
Partner en extern accountant Gemeenschappelijke Regeling Ergon



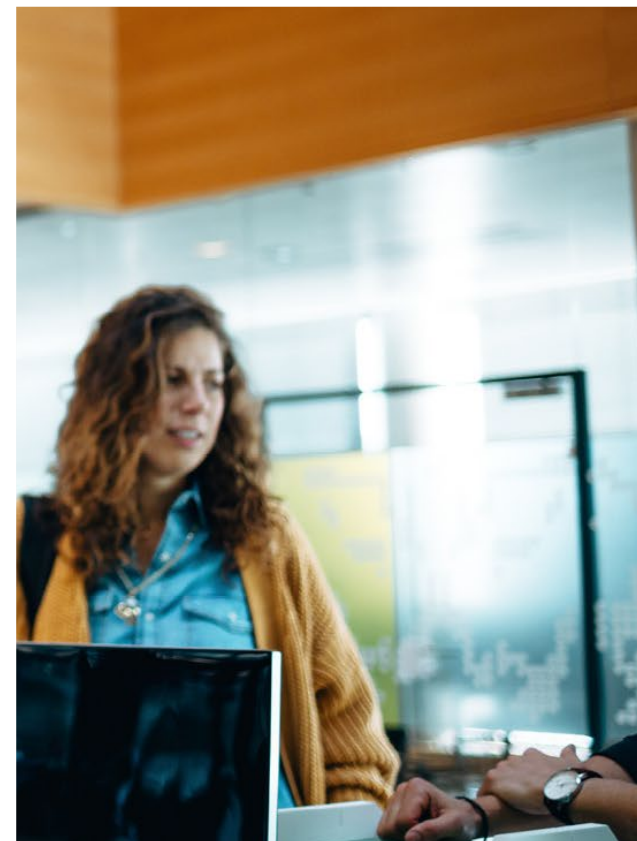
01

Dashboard  
interim-controle



02

Ontwikkelingen &  
aandachtspunten



03

Bevindingen  
interim-controle

# 1. Dashboard interim-controle

---

## 1.1 Dashboard interim-controle

---

5

---

---

---

---

---

---

---



UW INTERNE BEHEERSING

- ▶ Op basis van onze observaties tijdens de interim-controle concluderen wij dat de interne beheersing en controleomgeving voor zover relevant voor onze jaarrekeningcontrole van voldoende niveau is.
- ▶ Wij kunnen nog niet altijd steunen op de interne beheersing in de processen; de VIC en onze controle is daarmee hoofdzakelijk gegevensgericht en achteraf. U heeft overigens uit efficiency overwegingen bewust gekozen voor de huidige inrichting.
- ▶ Interne controles gedurende 2024 hebben diverse aanbestedingsonrechtmatigheden aan het licht gebracht. Op basis van een eerste analyse schat u in dat de geconstateerde onrechtmatigheden de verantwoordingsgrens zullen overschrijden. Opvolging hiervan is onder uw aandacht.
- ▶ Voor het toegroeien naar een systeemgerichte controle is het volgende van belang:
  - Jaarlijks actualiseren en bestuurlijk agenderen van de (fraude)risicoanalyse.
  - Jaarlijks bestuurlijk agenderen van uitkomsten van de verbijzonderde interne controles.
  - Identificeren van de kwaliteit van systeemgerichte interne beheersingsmaatregelen en beschikbaarheid data-exports.
- ▶ Tijdens de interim-controle zijn de IT-beheersmaatregelen (AFAS) in kaart gebracht. Op basis van onze observaties zien wij ruimte tot verbetering met betrekking tot:
  - Procedure autorisatiebeheer, specifiek bij indienst en uitdiensttredingen.
  - Periodieke controle op toegang en juistheid ingerichte autorisaties.Als gevolg van bovenstaande observaties zijn aanvullende gegevensgerichte werkzaamheden gepland in het kader van de jaarrekeningcontrole.

STATUS PROCESSEN

|                         | Opzet/<br>bestaan<br>2024 | Opzet/<br>bestaan<br>2023 | VIC    |
|-------------------------|---------------------------|---------------------------|--------|
| Memoriaalboekingen      | ☹                         | ☹                         | —      |
| WNT                     | 😊                         | 😊                         | n.v.t. |
| Ontvangst Rijksmiddelen | 😊                         | 😊                         | n.v.t. |
| Baten groenvoorziening  | NEW                       | 😊                         | 😊      |
| Baten detacheringen     | 😊                         | 😊                         | 😊      |
| Inkopen & betalingen    | 😊                         | ☹                         | 😊      |
| Personeelsproces        | ☹                         | ☹                         | ☹      |
| LKS                     | ☹                         | ☹                         | 😊      |

ONTWIKKELINGEN & AANDACHTSPUNTEN

VIC en rechtmatigheidsverantwoording

- ▶ Verbijzonderde interne controle:
  - Verdiepingsslag in bevindingen en rapportering door het toetsen op de werking van systemen zoveel als mogelijk bij de teams zelf (eerste lijn) of in de tweede lijn te beleggen. De VIC kan dan meer acteren als derde lijn waarbij het hun taak is om de betrouwbaarheid van informatievoorziening van de eerste en tweede lijn te beoordelen.
  - Verbreding werkzaamheden naar processen als memoriaalboekingen, salarismutaties en loonkostensubsidie (LKS).
  - Verbeterslag in VIC-rapportages door aandacht te schenken aan monitoring van bevindingen.
- ▶ U heeft in 2024 een M&O beleid vastgesteld.
- ▶ Aanpassing van de financiële verordening in verband met de definitie van tijdigheid van melden begrotingsafwijkingen is gerealiseerd.

Network and Information Security 2 (NIS2)

Ergon is aangemerkt als een essentiële entiteit en valt daardoor direct onder de Cyberbeveiligingswet. Om te voldoen aan BIO versie 2 en NIS2 dienen nog enkele stappen genomen te worden. U heeft aangegeven de analyse die hiervoor de basis vormt, uit te zullen voeren wanneer de wetgeving definitief is. Volledigheidshalve melden we op dat bovenstaande geen gevolgen heeft voor de jaarrekeningcontrole 2024.

BEVINDINGEN SIGNIFICANTE PROCESSEN

Belangrijkste bevindingen

- ▶ Wij hebben uit mediaberichten begrepen dat er een onderzoek naar de cultuur binnen Ergon heeft plaatsgevonden. Wij hebben kennisgenomen van uw visie op de uitkomsten en opvolging van dit onderzoek en onderkennen met u het belang van een goede verankering van de verbeteracties in de organisatie.
- ▶ Memoriaal: een controle op memoriaalboekingen wordt niet zichtbaar vastgelegd.
- ▶ Groenvoorziening: onvoldoende controle-technische functiescheiding rondom de registratie van projecten (incl. aanneemsom). Het risico op niet factureerbare projecten of onjuiste aanneemsommen is hiermee aanwezig, wat in het kader van projectbeheersing het risico op onvolledigheid van baten omvat. We adviseren een invoercontrole in Groenvision.
- ▶ Inkoop- en betalingsorganisatie: gebruik van de inkoopmodule in het kader van de registratie van verplichtingen wordt (nog) niet afgedwongen. Het risico op een niet volledig beeld van de verplichtingen is hierdoor aanwezig.
- ▶ Personeel: een zichtbare controle op loonmutaties, declaraties en verlofregistratie ontbreekt.

## 2. Ontwikkelingen & Aandachtspunten

|     |                                               |    |
|-----|-----------------------------------------------|----|
| 2.1 | <u>Rechtmatigheidsverantwoording</u>          | 7  |
| 2.2 | <u>Informatiebeveiliging en cybersecurity</u> | 9  |
| 2.3 | <u>Wet DBA</u>                                | 10 |
| 2.4 | <u>Aandachtspunten WNT</u>                    | 12 |
| 2.5 | <u>Relevante wijzigingen in het BBV</u>       | 13 |
| 2.6 | <u>Duurzaamheidsverantwoording</u>            | 14 |

## 2.1 Rechtmatigheidsverantwoording (1/2)

### Rechtmatigheidsverantwoording

Het dagelijks bestuur heeft voorgaand jaar voor het eerst expliciet verantwoording afgelegd over de financiële rechtmatigheid. De totstandkoming van de rechtmatigheidsverantwoording is een proces met interactie tussen verschillende gremia dat start bij het bepalen van de verantwoordingsgrens door het algemeen bestuur. Deze verantwoordingsgrens heeft Ergon vastgesteld op 1% van de lasten inclusief dotaties reserves. Dit is gelijk aan de wettelijke materialiteit die in het kader van de jaarrekeningcontrole over 2024 door ons wordt gehanteerd. De tolerantie voor rapportage van afwijkingen in de paragraaf bedrijfsvoering is door Ergon vastgesteld op € 100.000.

In de jaarrekening 2023 heeft u gerapporteerd over het ontbreken van een M&O beleid. U heeft hier adequate opvolging aan gegeven door in 2024 een M&O beleid vast te stellen. Daarnaast hebben we met u besproken over aanpassing van de financiële verordening in het kader van de definitie van tijdigheid van melden begrotingsafwijkingen. Dit is inmiddels opgevolgd.

### Wijziging wet - en regelgeving

Het wetgevingstraject rondom de rechtmatigheidsverantwoording is nog niet afgerond. Bij het schrijven van deze managementletter zijn de wijzigingen in het BBV en BADO in verband met de invoering van de rechtmatigheidsverantwoording voor advisering voorgelegd aan de Raad van State. Wijzigingen met betrekking tot de wettelijke materialiteit in het kader van de jaarrekeningcontrole en de bandbreedte voor de verantwoordingsgrens zijn niet te verwachten.

Wij houden u uiteraard op de hoogte omtrent de ontwikkelingen op dit vlak en de mogelijke impact hiervan op uw organisatie en de jaarrekeningcontrole.

Op 22 oktober 2024 is de aangepaste Kadernota Rechtmatigheid 2024 gepubliceerd. Na het jaar van invoering heeft de Commissie BBV vragen, ervaringen, aanbevelingen en adviezen ontvangen. Deze hebben geleid tot aanpassingen in de Kadernota Rechtmatigheid 2024. Hierin heeft de Commissie ook de Q&A rechtmatigheidsverantwoording, die in november 2023 is gepubliceerd, verwerkt. De belangrijkste wijzigingen in de Kadernota Rechtmatigheid 2024 zijn:

- ▶ Tekstuele aanpassing in de modelverantwoording ten aanzien van de geconstateerde bevindingen, specifiek in relatie tot de omvang van niet rechtmatig tot stand gekomen verantwoorde baten, lasten en balansmutaties en welk deel acceptabel is op basis van de vastgestelde afspraken;
- ▶ Een aangepast hoofdstuk 2 om het bestuurlijk belang van rechtmatigheid voor raadsleden te verduidelijken;
- ▶ Er is een overzicht opgesteld dat als voorbeeld kan dienen op welke wijze de (begrotings)onrechtmatigheden inzichtelijk kunnen worden gemaakt en in de rechtmatigheidsverantwoording kan worden opgenomen met daarbij de vermelding van fouten en/of onduidelijkheden (tabel uit de Q&A van november 2023);
- ▶ Verduidelijking wanneer overschrijdingen ten aanzien van wel of niet tijdig melden als onrechtmatig worden beschouwd. Daarnaast verduidelijking van wanneer welke begrotingsonrechtmatigheden als gevolg van overschrijding van lasten en/of investeringen als acceptabel (passend in het beleid) worden beschouwd (dus wel onrechtmatig, maar acceptabel);
- ▶ Het niet meer in de rechtmatigheidsverantwoording opnemen van geconstateerd misbruik waarbij het M&O beleid is toegepast en heeft geleid tot bijvoorbeeld terugvorderingen en het opleggen van sancties. De jaarrekening is in deze situatie immers getrouw en de financiële effecten van het misbruik zijn teniet gedaan. Wel dient via de paragraaf bedrijfsvoering inzicht te worden gegeven in de aard en (financiële) impact van het bij de gemeenschappelijke regeling geconstateerde misbruik.

## 2.1 Rechtmatigheidsverantwoording (2/2)

### Mogelijke doorontwikkeling VIC

Voor de VIC is ten aanzien van de rechtmatigheidsverantwoording een belangrijke coördinerende rol weggelegd. U heeft de processen zo ingericht dat met name de VIC-werkzaamheden, vastleggingen en uitkomsten de basis vormen voor de rechtmatigheidsverantwoording. De verantwoordelijkheden voor de rechtmatigheidsverantwoording liggen veel breder, alle organisatieonderdelen en het dagelijks bestuur zijn hiervoor verantwoordelijk. Het toetsen op de werking van systemen of het eventueel aanvullen met gegevensgerichte werkzaamheden kan ook bij de teams zelf (eerste lijn) of in de tweede lijn worden belegd. De VIC kan dan meer acteren als derde lijn waarbij het hun taak is om de betrouwbaarheid van informatievoorziening van de eerste en tweede lijn te beoordelen. Er vindt dan een verschuiving plaats van 'de VIC als onderbouwing van de rechtmatigheidsverantwoording' naar 'de VIC als bevestiging van de getrouwheid van de rechtmatigheidsverantwoording van de verschillende teams'.

Bij Ergon worden de controles uitgevoerd door de interne controlefunctie en dit zijn veelal gegevensgerichte werkzaamheden met als doel de rechtmatigheidsverantwoording te onderbouwen. De werkzaamheden richten zich momenteel in hoofdzaak op de processen rondom inkopen, verkopen en personeelsmutaties. Wij adviseren u de werkzaamheden te verbreden naar de processen rondom memoriaalboekingen, salarismutaties en loonkostensubsidie (LKS). Om daarnaast eigenaarschap te vergroten in de eerste en tweede lijn, verdient het aanbeveling om de interne beheersingsmaatregelen zoveel als mogelijk daar te laten plaatsvinden. Dit is een ontwikkeling die u nog kunt maken en die u helpt meer in control te zijn in de lijn, fouten te voorkomen en het lerend vermogen in de organisatie te vergroten.

### Samenwerking VIC

Wij maken zoveel als mogelijk gebruik van de door u uitgevoerde (verbijzonderde) interne controlewerkzaamheden.

Vooraf heeft hierover per kwartaal afstemming plaatsgevonden met de VIC, zodat de juiste werkzaamheden door u worden gedaan wat een korte doorlooptijd van de controle bevordert. De tijdigheid en kwaliteit van de werkzaamheden van VIC is van belang. Ten tijde van de interim-controle zijn de werkzaamheden door de interne controle zoals beschreven in het interne controleplan over het eerste half jaar uitgevoerd. In de VIC-rapportage wordt momenteel geen expliciete aandacht geschonken aan opvolging van vorige aanbevelingen en of (geactualiseerde) processen worden nageleefd. In het kader van lerend vermogen van de organisatie en continue verbetering vragen wij u aandacht hiervoor.

De VIC-rapportages worden opgesteld door de VIC-medewerker in samenspraak met de manager planning en control. Afstemming met de verantwoordelijke proceseigenaar is hier onderdeel van. Wat nog ontbreekt is een reactie van de proceseigenaar alvorens deze definitief wordt gemaakt. De belangrijkste bevindingen uit de VIC-rapportages worden aan het directieteam gerapporteerd. Wij bevelen u aan om minimaal eens per jaar ook het (dagelijks)bestuur te informeren over de belangrijkste bevindingen, opvolging en vervolgacties.

### Bevindingen rechtmatigheidscontroles 2024

Ten tijde van de interim-controle heeft u een aantal aanbestedingsonregelmatigheden geconstateerd. Op basis van een eerste analyse heeft u de verwachting dat de onrechtmatigheden over boekjaar 2024 de verantwoordingsgrens zullen overschrijden. Wij adviseren u om het bestuur tussentijds te informeren over deze dossiers en een afwijkbesluit te laten vaststellen voor deze aanbestedingen. Wij zullen een gedetailleerde controle uitvoeren op de rechtmatigheidsverantwoording en onregelmatigheden bij de eindejaarscontrole.



## 2.2 Informatiebeveiliging en cybersecurity

### NIS2 - digitale weerbaarheid verankerd in wet- en regelgeving vanuit de EU

Om de digitale weerbaarheid van organisaties te verhogen is de NIS2 (Network and Information Security 2) richtlijn vanuit de EU vastgesteld. De NIS2 richtlijn is een update van de in 2016 ingevoerde NIS-richtlijn. In Nederland ook wel bekend als NIB2 (Netwerk- en informatiebeveiligingsrichtlijn) en/of de Wbni (Wet Beveiliging Netwerk- en Informatiesystemen). Lokale overheden zijn door de NIS2 aangewezen als organisaties die van vitaal belang zijn voor de samenleving waardoor ook uw organisatie verplicht is om de NIS2-maatregelen te implementeren. In Q4 2024 wordt NIS2 naar Nederlandse wetgeving vertaald onder de noemer 'Cyberbeveiligingswet' en deze wordt medio 2025 van kracht. Organisaties vallen direct onder de Cyberbeveiligingswet, als zij actief zijn in aangewezen sectoren en gekenmerkt worden als 'essentiële' of 'belangrijke' entiteit. Direct wil zeggen dat bovengenoemde verplichtingen voor deze organisaties direct gaan gelden zodra de wet in werking treedt

Belangrijk is dat NIS2 aanvullende eisen stelt, die niet volledig door de huidige Baseline Informatiebeveiliging Overheid (BIO) worden afgedekt, wat betekent dat in de komende periode additionele maatregelen moeten worden getroffen ten einde aan NIS2 te voldoen. De volgende verplichtingen vallen onder NIS2:

- ▶ **Zorgplicht:** organisaties dienen een risicobeoordeling uit te voeren en op basis daarvan passende maatregelen te nemen om hun diensten te beveiligen.
- ▶ **Opleidingsplicht:** bestuursorganen dienen opgeleid te zijn, en optioneel ook werknemers, om cyberrisico's te identificeren, impact te bepalen en beveiligingsmaatregelen te selecteren.
- ▶ **Meldplicht:** cyberincidenten dienen binnen 24 uur bij de toezichthouder te worden gemeld. Tevens dient een cyberincident ook bij een sectorspecifiek Computer Security Incident Response Team (CSIRT) te worden gemeld, wat eventueel hulp en bijstand kan verlenen.
- ▶ **Toezicht:** een onafhankelijk toezichthouder zal naleving van de verplichtingen uit de richtlijn borgen.

Het is van belang dat Ergon proactief onderzoekt of de NIS2-verplichtingen op de organisatie van toepassing zijn. De Rijksinspectie Digitale Infrastructuur (RDI) heeft hiertoe een self-assessment tool ontwikkeld, waarmee organisaties zelf kunnen evalueren of ze onder de NIS2-richtlijn vallen en of ze gekenmerkt worden als essentieel of belangrijk.

In de audit is het onderwerp Cyber Security en de komst van NIS2 besproken. Ergon zal dit jaar nog een ISMS (Information Security Management System) implementeren. Het ISMS ondersteunt om aanvullende maatregelen op een juiste manier te implementeren die voortkomen uit de BIO versie 2 en de NIS2. Ergon zal een analyse maken tussen de huidige situatie en de gewenste situatie om zo te bepalen welke acties nog ondernomen moeten worden om te voldoen aan BIO versie 2 en NIS2. Hiervoor wacht Ergon wel tot beide zaken definitief zijn. Daarnaast zijn er door Ergon diverse technische maatregelen genomen om de Cyber weerbaarheid te verhogen. Zo heeft Ergon onder andere Nordwave SIEM SOC en Microsoft Defender voor netwerk monitoring geïmplementeerd.

## 2.3 Wet DBA

### Kwalificatie van arbeidsrelaties

Het aantal zelfstandigen zonder personeel (zzp) is de afgelopen jaren flink gestegen. Een deel van deze groep kwalificeert als schijnzelfstandige. Dit betekent dat op basis van wet- en regelgeving eigenlijk sprake is van een arbeidsovereenkomst. Het kabinet vindt deze situatie onwenselijk, omdat de beschermende werking van het arbeidsrecht wordt ontlopen en het sociale stelsel onder druk komt te staan. Daarom zet het kabinet de komende jaren in op het aanscherpen van regels en handhaving.

Sinds de introductie van de Wet DBA in 2016 is sprake van een handhavingsmoratorium. Dit betekent dat de Belastingdienst niet controleert en handhaaft op het bestaan van een dienstbetrekking, tenzij sprake is van kwaadwillendheid. Vanaf 1 januari 2025 komt het handhavingsmoratorium naar verwachting te vervallen en gaat de Belastingdienst weer volledig handhaven. Hierdoor kunnen naheffingsrisico's ontstaan.

Daarnaast werkt het kabinet aan nieuwe wetgeving voor de beoordeling van arbeidsrelaties. In het Hoofdlijnenakkoord is te lezen dat de behandeling van deze wetgeving door het nieuwe kabinet zal worden voortgezet. Kort gezegd zal de nieuwe wetgeving meer nadruk leggen op de vraag of het werk en de werkende organisatorisch zijn ingebed in de organisatie van de werkverschaffer. Daarmee wordt bedoeld of het werk een kernactiviteit van de organisatie vormt en zij aan zij met werknemers wordt verricht. In dat geval zal eerder sprake zijn van een arbeidsovereenkomst. De nieuwe wetgeving zal naar verwachting niet eerder ingaan dan 1 januari 2026.

Organisaties die werken met zelfstandigen die eigenlijk werknemer zijn lopen financiële risico's. Zo is er vanaf 1 januari 2025 sprake van een naheffingsrisico vanuit de Belastingdienst. Ook kunnen zelfstandigen die eigenlijk werknemer zijn vorderingen instellen op grond van arbeidsrechtelijke verplichtingen en kunnen verplichte pensioenregelingen leiden tot pensioenvorderingen. Om dergelijke risico's te voorkomen is het voor organisaties die zelfstandigen inhuren van belang om de huidige inhuur van zelfstandigen en het inhuurproces onder de loep te nemen.

Volledigheidshalve melden we dat dit actuele onderwerp op de agenda staat bij de directeur HR en uit inlichtingen blijkt dat diverse acties in gang zijn gezet. Wij zullen met ingang van boekjaar 2025 verder aandacht geven aan dit onderwerp en de impact hiervan bepalen op onze controle.

## 2.4 Aandachtspunten Wet Normering Topinkomens (WNT)

### Bestuurderswissel en interim-bestuurder 2025

Per 1 januari 2025 is Ingrid Hems aangesteld als interim-bestuurder. Mevrouw Hems wordt daarmee gedurende de periode van haar aanstelling als topfunctionaris voor de WNT gekwalificeerd. Wij hebben begrepen dat u voornemens bent om de functie van directeur-bestuurder in 2025 te vervullen met een vaste aanstelling van een nieuwe directeur-bestuurder.

Bij de wisseling van een WNT-topfunctionaris is het belangrijk om goed te kijken naar de toepassing van de WNT. De WNT kent complexe regels voor de beloning van topfunctionarissen, welke bij indienst- en uitdiensttreding van een functionaris soms een ongewenste uitwerking hebben, bijvoorbeeld door een periode van non-activiteit of de financiële afwikkeling van verlofrechten waarmee WNT-drempelbedragen kunnen worden overschreden. Daarnaast is het belangrijk om te kijken naar de beloning van de interim-bestuurder. Deze beloning moet ook voldoen aan de regels van de WNT.

Ergon kent een extra complexiteit doordat medewerkers indienst kunnen zijn bij verschillende entiteiten (Stichting BWSW, Stichting WGA, en de GRWRE). De keuze bij welke entiteit de topfunctionaris in dienst is kan gevolgen hebben voor de WNT-verantwoording van alle entiteiten.

In dit kader adviseren wij u om tijdig advies in te winnen bij een specialist op het gebied van de WNT, om herstelacties in een later stadium te voorkomen.

## 2.5 Relevante wijzigingen in het BBV

### Notitie Overhead

De commissie BBV heeft in de notitie Overhead 2023 de regelgeving met betrekking tot de toerekening van Overhead geactualiseerd, verduidelijkt en samengevoegd in één notitie. De notitie is van toepassing vanaf begroting 2026 (eventueel 2025). De belangrijkste uitspraken en aanbevelingen, voor zover voor Ergon relevant, zijn als volgt:

- ▶ **Stellige uitspraak:** De definitie van overhead is aangescherpt waardoor alle functies die onderdeel uitmaken van een specifieke taak geen onderdeel zijn van de overhead.
- ▶ **Aanbevelingen:** De commissie adviseert om overhead niet bij de begroting vorm te geven maar door middel van de financiële verordening of door een notitie overhead aan het algemeen bestuur voor te leggen en deze periodiek te herzien. In deze nota neemt de gemeenschappelijke regeling keuzes op ten aanzien van: kaderstelling, methodiek en onderscheiding primaire processen en overhead.

Wij adviseren u om de notitie overhead uiterlijk in het voorjaar van 2025 te actualiseren.

## 2.6 Duurzaamheidsverantwoording (1 / 2)

1/2

### Context & ontwikkelingen

Voor grote, niet-beursgenoteerde ondernemingen is het vanaf 2025 verplicht te rapporteren over de impact van hun activiteiten op duurzaamheid (de CSRD). In deze regels is vastgelegd waarover verantwoording moet worden afgelegd, waarbij een actieve dialoog met de belangrijkste belanghebbenden een wezenlijk onderdeel vormt. Deze standaarden verdelen duurzaamheid in drie onderdelen: ESG (environment, social, governance).

Voor gemeenschappelijke regelingen geldt deze verplichting nog niet. Breder in overheidsland vervullen de gemeenten echter wel een belangrijke rol bij het realiseren van verduurzaming in de samenleving vanuit hun maatschappelijke en regisserende rol. Denk aan de regionale energiestrategie (RES), het toezicht op energie labels van kantoorgebouwen in de gemeente en de aandacht voor meer circulariteit in de bouwopgaven. Tal van decentrale overheden maken inmiddels afspraken en sluiten zich aan bij initiatieven over het rapporteren over duurzaamheid. Een goed voorbeeld hiervan is het SDG-initiatief van de VNG (<https://www.sdgnederland.nl/>) waar circa 140 gemeenten bij zijn aangesloten. Een bredere en diepere uitwerking van duurzaamheid wordt gevonden in het gedachtegoed van 'brede welvaart', een begrip dat meer gangbaar is binnen overheden en bijvoorbeeld ook door CBS wordt gemonitord.

Al de activiteiten die overheden bedenken en uitvoeren komen nog maar beperkt concreet en meetbaar terug in beleid en verantwoording. Dit blijkt ook uit onderzoek dat de Rijksuniversiteit Groningen voor BDO heeft uitgevoerd in 2023 en waarvan begin 2025 een actualisatie wordt gepubliceerd. Deze observaties en de CSRD die voor het bedrijfsleven gaat gelden, hebben geleid tot de oprichting van "the coalition of the willing", een samenwerking van o.a. gemeenten, banken, BDO en het CBS. Door deze groep is een concept handreiking opgesteld om decentrale overheden te ondersteunen bij het selecteren, structureren en inzicht bieden in de voor hen meest relevante duurzaamheidsthema's. Deze handreiking gaat ook in op de wijze waarop u als gemeenschappelijke regeling deze informatie in uw begroting en jaarstukken kan opnemen, zodat hierin ook de gewenste transparantie ontstaat voor uw belanghebbenden.

Alhoewel geen wettelijke plicht bestaat voor decentrale overheden hierover te rapporteren, krijgen overheden wel steeds meer te maken met dit thema vanuit de waardeketen van bedrijven en banken waartoe decentrale overheden ook behoren. Het is niet ondenkbaar dat op termijn ook voor decentrale overheden een rapportageverplichting over de belangrijkste duurzaamheidsindicatoren volgt. Hierover is geen verdere informatie bekend, anders dan dat het Ministerie van Binnenlandse Zaken zich hier over buigt en al dan niet via de Commissie BBV een nadere duiding aan geeft.



## 2.6 Duurzaamheidsverantwoording (2/2)

2/2

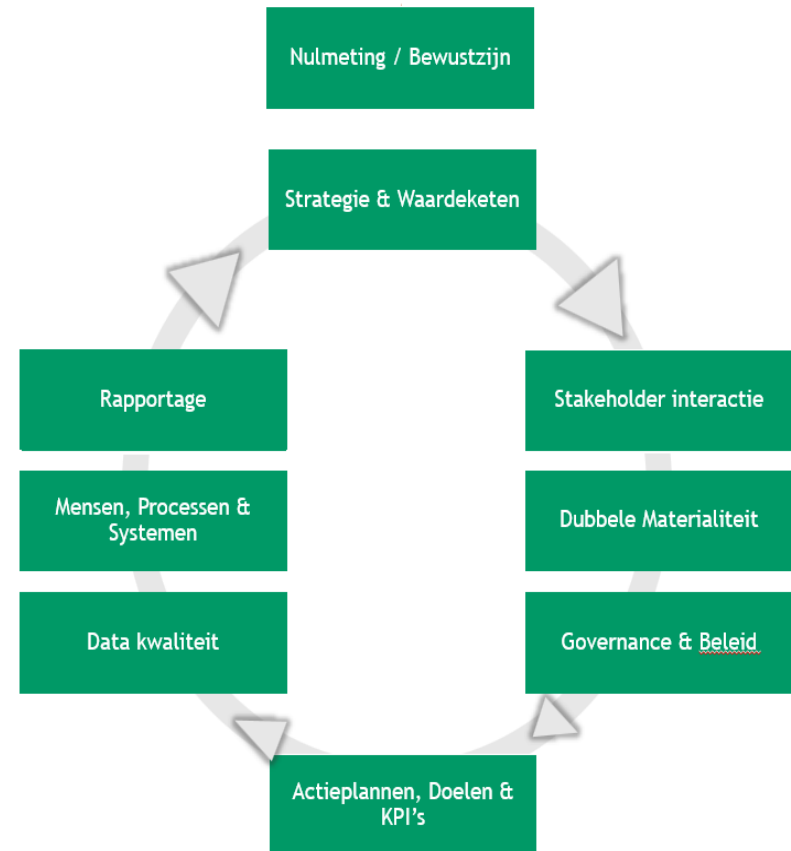
### Duurzaamheidsindicatoren

Met de betrokkenheid van het CBS bij de totstandkoming van de concept handreiking is gerealiseerd dat een set aan relevante indicatoren is opgesteld. Het CBS heeft van veel van deze indicatoren data beschikbaar, dan wel werkt aan de ontsluiting en monitoring hiervan. Het voordeel hiervan is dat voor gemeenten de externe data zodoende eenvoudig beschikbaar is, naast de eigen data.

### Pak de handschoen op

Wij adviseren u kennis te nemen van de handreiking zodra deze beschikbaar komt en een dialoog aan te gaan tussen dagelijks bestuur en algemeen bestuur over de route om tot meetbaar en transparant beleid hierop te komen. Zolang nog geen sprake is van verplichte toepassing is er alle ruimte om keuzes in de indicatoren of duurzaamheidsthema's te maken, bijvoorbeeld door te starten met de meest belangrijke qua impact. Deze ervaring kunt u inzetten om het inzicht en de verantwoordings stap voor stap te verrijken. Tegelijkertijd verwachten wij de komende periode nog meer informatie en praktische handvatten en zal op termijn ook vanuit het Ministerie van Binnenlandse Zaken, dan wel vanuit de commissie BBV een reactie volgen.

Ergon heeft in haar begroting, jaarstukken en op haar website nog geen passages opgenomen over duurzaamheidsverslaggeving. vier van de vijf deelnemende gemeenten in Ergon zijn Global Goals gemeenten en zetten zich in voor de doelen in de wereldwijde duurzaamheidsagenda 2030. Dit betreffen de gemeenten Eindhoven, Heeze-Leende, Valkenswaard en Veldhoven. Naast het maatschappelijk belang van Ergon, kan Ergon voor deze deelnemende gemeenten ook toegevoegde waarde leveren op het gebied van duurzaamheid door meer aandacht aan duurzaamheidsverslaggeving te schenken.



## 3. Bevindingen interim-controle

|     |                                                                     |    |
|-----|---------------------------------------------------------------------|----|
| 3.1 | <u>Onze werkzaamheden</u>                                           | 15 |
| 3.2 | <u>Onze werkzaamheden bij de processen</u>                          | 17 |
| 3.3 | <u>Overzicht van onze bevindingen bij de processen</u>              | 18 |
| 3.4 | <u>Overzicht van onze bevindingen t.a.v. de IT General Controls</u> | 22 |

## 3.1 Onze werkzaamheden (1/2)

### 1/2 Aandacht voor fraude

#### Controleaanpak en doel van de interim-controle

Het doel van de jaarrekeningcontrole is een oordeel tot uitdrukking brengen over de getrouwheid van de jaarrekening van Ergon. De controle heeft onder meer betrekking op het overwegen van de interne beheersing die voor het opstellen van de jaarrekening relevant is, teneinde controlewerkzaamheden op te zetten die in de gegeven omstandigheden passend zijn, maar niet met het doel een oordeel over de effectiviteit van de interne beheersing tot uitdrukking te brengen. Het gaat hierbij niet alleen over de kwaliteit van de accountantscontrole, maar ook over de wijze waarop Ergon haar interne processen beter kan inrichten.

Op basis van onze bevindingen bij deze werkzaamheden, geven wij, in het kader van onze natuurlijke adviesfunctie, in deze managementletter aanbevelingen over de opzet van de administratieve organisatie en berichten wij u over vastgestelde tekortkomingen in de uitvoering daarvan en in hoeverre corrigerende maatregelen door management zijn genomen.

De aangelegenheden waarover wij rapporteren betreffen die tekortkomingen die tijdens de controle zijn geïdentificeerd en waarbij wij van mening zijn dat deze voldoende belangrijk zijn om verslag van te doen.

#### Onze inschatting van de aandachtspunten

In het kader van de controle van de jaarrekening 2024 en onze aanpak hebben wij een zogenaamde initiële risico-inschatting gemaakt. Wij zien de volgende aandachtspunten bij de controle van de jaarrekening van Ergon:

- ▶ In onze controlestandaarden (NV COS) wordt expliciet het risico van management override (bewuste beïnvloeding door bestuur of management van de jaarcijfers) als belangrijk te onderkennen theoretisch risico benoemd. Als accountant moeten wij in onze werkzaamheden hier specifiek aandacht aan besteden. Om het resterende risico te beperken beoordelen wij schattingsprocessen en bijzondere journaalposten in detail.
- ▶ Ongeautoriseerde handelingen in Afas als gevolg van mogelijk te ruim ingerichte autorisaties en bevoegdheden.
- ▶ Volledigheid van de opbrengstverantwoording op de opbrengsten groenvoorziening, groepsdetachering en individuele detachering.
- ▶ Volledigheid van de gerapporteerde bevindingen in de rechtmatigheidsverantwoording.

# 3.1 Onze werkzaamheden (2/2)

## 2/2 - Aandacht voor fraude

### Onze bevindingen

Bij de planning voor de jaarrekeningcontrole houden wij rekening met het risico dat de jaarrekening als gevolg van fraude en onregelmatigheden onjuistheden van materieel belang zou kunnen bevatten. Daarnaast hebben wij beoordeeld in hoeverre sprake kan zijn van een risico omtrent corruptie of een risico omtrent het niet-naleven van wet- en regelgeving.

Eén van de door ons uitgevoerde maatregelen is het bespreken van de mogelijke frauderisico's en mogelijke fraudesituaties met uw concerncontroller en fiscaal en financieel adviseur. Hiertoe hebben wij de mogelijke frauderisico's en -situaties, mede aan de hand van de door u opgestelde frauderisicoanalyse en de compliancevragenlijst, besproken. Deze besprekingen en onze controlewerkzaamheden hebben geen indicaties voor materiële fraude opgeleverd.

| ONZE BEVINDINGEN                                              |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fraude                                                        | 2024 | Evaluatie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Frauderisicoanalyse uitgevoerd                                | ☹️   | In 2024 heeft u een fraudeprotocol opgesteld en vastgesteld. In dit protocol zijn onder meer de fraudedriehoek en een frauderesponsplan opgenomen. Een verdere verbetering is mogelijk door ook de interne en externe kaders op te nemen, alsmede de risicobereidheid van de organisatie. Tevens zijn enkele jaren geleden frauderisico's naar voren gekomen uit een extern onderzoek (Coppens). Deze frauderisico's zien voornamelijk op fraude als gevolg van onvoldoende functiescheiding en ontvreemding van middelen, en zijn toe aan een actualisering, verbreding en koppeling aan uw administratie processen. Hierbij kunt u denken aan het potentiële frauderisico management override. Wij adviseren u het risico 'dat de reguliere procesgang opzij wordt gezet' concreet te maken, onder andere door aan te geven op welk(e) proces(sen) dit risico betrekking heeft en op welke wijze. Tevens missen wij nog het risico en daaraan gerelateerde beheersmaatregelen ten aanzien van onjuiste verslaggeving. Daarnaast adviseren we u de frauderisico analyse jaarlijks bestuurlijk te agenderen. |
| Gedragscodes, klokkenluidersregeling en incidentenregistratie | 😊    | U beschikt over diverse interne kaders. Een overzicht van de interne kaders is opgenomen in paragraaf 2 van de notitie frauderisicobeheersing. De interne kaders dateren uit 2024 of later en zijn daarmee ook recent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Frauderesponsplan                                             | 😊    | In 2024 heeft u een frauderesponsplan opgesteld, waarin staat opgenomen hoe moet worden gehandeld wanneer een incident zich voordoet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Incidenten                                                    | 😊    | Ergon beschikt onder andere over een informatiebeveiligingsbeleid 2024, een procedure melding datalekken en voor andersoortige incidenten gelden algemene protocollen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Corruptie                                                     | 😊    | Ergon beschikt over een actueel M&O beleid dat in 2024 door het dagelijks bestuur is vastgesteld.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## 3.2 Onze werkzaamheden bij de processen

### Belangrijkste processen

Aan de navolgende processen hebben wij specifiek aandacht geschonken tijdens onze interim-controle:

- ▶ Het planning & controlproces;
- ▶ Het proces omtrent de opbrengsten uit ontvangen bijdragen, bestaande uit de gemeentelijke bijdragen en de Rijksbijdragen;
- ▶ De processen omtrent opbrengsten, bestaande uit groenvoorziening, groepsdetachering, individuele detachering;
- ▶ Het proces omtrent inkopen & betalingsorganisatie;
- ▶ Het personeelsproces;
- ▶ Het proces omtrent loonkostensubsidie (LKS);
- ▶ Verbijzonderde Interne controle (rechtmatigheidsverantwoording).

Natuurlijk zijn er meerdere processen te onderkennen met financiële gevolgen, maar deze processen zien wij als de belangrijkste processen.

Voor elk proces beoordelen wij de volgende onderdelen:

- ▶ **Controle technische functiescheiding (CTFS):** Is binnen de belangrijkste processen sprake van voldoende functiescheiding?
- ▶ **AO/IB:** Is sprake van een actuele en toereikende procesbeschrijving met voldoende beheersmaatregelen?
- ▶ **IT-maatregelen:** Zijn in en rondom het systeem voldoende waarborgen getroffen ten aanzien van de betrouwbaarheid van de gegevensverwerking?
- ▶ **VIC:** Heeft de VIC de interne beheersmaatregelen getoetst en kunnen wij daar gebruik van maken?

Indien al deze vragen positief kunnen worden beantwoord, is de organisatie optimaal in control en kunnen ook wij gebruik maken van uw eigen interne beheersing. De vaak tijdrovende en gedetailleerde gegevensgerichte werkzaamheden (die ook nog eens achteraf plaatsvinden), kunnen dan beperkt blijven tot een minimum.

Een totaaloverzicht van de effectiviteit van de processen is opgenomen in paragraaf 3.3. Voor het proces rondom de verbijzonderde interne controle verwijzen we naar paragraaf 2.1.

### Data-analyse

Registratie van financiële data alsmede de interne beheersingsmaatregelen daarop vinden digitaal plaats. Indien er sprake is van een toereikende kwaliteit van de interne beheersingsmaatregelen, kan hiervan gebruik gemaakt worden voor zover relevant voor de jaarrekeningcontrole. Door gebruik te maken van beschikbare digitale informatie, kan er inzicht in de beheersing van de organisatie verkregen worden. Daarnaast kan hierdoor ingespeeld worden op risico's en uitzonderingen, wat bijdraagt aan de kwaliteit van de organisatie.

Voor de periode van 1 januari tot en met 30 september 2024 is een export van de digitale inkoopflow uit Afas gedraaid. De digitale inkoopflow geeft informatie over de controle en autorisatie van inkoopfacturen, die hebben geleid tot het boeken van kosten alsmede het uitvoeren van betalingen. Deze informatie kan efficiënt en effectief gebruikt worden om de interne beheersing rondom de controle en autorisatie van kosten in kaart te brengen en te toetsen door de VIC.

In samenspraak met de VIC vindt momenteel een nadere analyse plaats van de export van de digitale inkoopflow. Hierbij wordt de kwaliteit van de data-exports, inrichting van de autorisaties in Afas en de doorlopen autorisatieflow nadere geanalyseerd. Mogelijke uitkomsten rapporteren we in ons accountantsverslag.

# 3.3 Overzicht van onze bevindingen t.a.v. de processen (1/2)

## 1/2 - Totaaloverzicht processen

In het volgende overzicht geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook paragraaf 3.4 t.a.v. ICT).

| PROCESSEN               |                      |                      |        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|----------------------|----------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | Opzet / bestaan 2024 | Opzet / bestaan 2023 | VIC*   | Toelichting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Memoriaalboekingen      | ☹️                   | ☹️                   | —      | <p>Ten aanzien van het maken van memoriaalboekingen stellen wij vast dat een verbetering is aangebracht in 2024 door het implementeren van een maandelijkse beoordeling op geregistreerde memoriaalboekingen door de financiële afdeling. De beoordeling is risico gericht en heeft als doel onjuiste memoriaalboekingen achteraf te detecteren en indien nodig te corrigeren.</p> <p>Een verdere verbetering is mogelijk door het implementeren van een preventieve maatregel door een goedkeuring op memoriaalboekingen voorafgaand de verwerking, of het creëren van functiescheiding tussen het voorstellen en inboeken van memoriaalboekingen. Het versterken van de beoordeling door de financiële afdeling kan plaatsvinden door deze zichtbaar te maken en gericht te laten zijn op alle memoriaalboekingen.</p> <p>De VIC heeft geen werkzaamheden gepland op memoriaalboekingen. Wij adviseren dit onderwerp toe te voegen aan uw interne controleplan.</p> |
| Ontvangst Rijksmiddelen | 😊                    | 😊                    | n.v.t. | Geen wijzigingen ten opzichte van voorgaand jaar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Baten groenvoorziening  | NEW                  | 😊                    | 😊      | <p>Het pakket GroenVision is in 2024 geïmplementeerd als projectadministratie en factureringssyteem in het kader van de werkzaamheden groenvoorziening. Rondom het proces van registratie van (nieuwe) projecten is geen sprake van controle technische functiescheiding. Hierdoor is er geen sprake van controle en autorisatie bij het aanmaken van nieuwe projecten in GroenVision. Hierdoor bestaat het risico dat niet factureerbare projecten of projecten met een onjuiste aanneemsom in GroenVision geregistreerd worden, wat in het kader van projectbeheersing het risico op onvolledige baten omvat.</p> <p>Wij adviseren een invoercontrole te implementeren, waarbij een autorisatie plaatsvindt voordat een nieuw project aangemaakt kan worden in GroenVision. Eenzelfde controle en autorisatie zou ook van toepassing dienen te zijn bij mutaties van een aanneemsom.</p>                                                                            |
| Baten detacheringen     | 😊                    | 😊                    | 😊      | Geen wijzigingen ten opzichte van voorgaand jaar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

*\*) De verbijzonderde interne controles voor het eerste half jaar zijn uitgevoerd volgens de planning en werkwijze die u de afgelopen jaren heeft gehanteerd. De werkzaamheden over het tweede halfjaar 2024 zijn nog niet uitgevoerd ten tijde van de interim-controle en worden door ons bij de eindejaarscontrole 2024 gecontroleerd.*



## 3.3 Overzicht van onze bevindingen t.a.v. de processen (2/2)

### 2/2 - Totaaloverzicht processen

| PROCESSEN            |                            |                            |        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|----------------------------|----------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Opzet /<br>bestaan<br>2024 | Opzet /<br>bestaan<br>2023 | VIC*   | Toelichting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Inkopen & betalingen | 😊                          | 😐                          | 😊      | In het inkoop- en betalingsproces is een verbetering zichtbaar doordat steeds meer gebruik wordt gemaakt van de inkoopmodule in AFAS. Het gebruik is evenwel nog niet structureel. Hierdoor blijft een risico op een onvolledig beeld van aangegane verplichtingen en prijsafspraken bestaan. Hierbij bestaat het risico dat het vereiste inzicht bij budgethouders onvoldoende is, wat kan leiden tot budgetoverschrijdingen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Personeelsproces     | 😐                          | 😐                          | 😐      | <p>Het personeelsproces is in opzet toereikend. Er is sprake van functiescheiding in de primaire registratie en controle van salarisgegevens. Tevens constateren we dat er adequate functiescheiding bestaat tussen werkzaamheden die door de medewerker salarisadministratie wordt uitgevoerd, waaronder het aanvullen van ontbrekende gegevens en het opstellen van de maandelijkse loonrun/proefverloning, en de controle door de medewerker planning &amp; control op het standenregister en het aanmaken van de bankopdracht. Een zichtbare controle op loonmutaties, declaraties en verlofregistratie ontbreekt.</p> <p>De VIC verricht een interne controle op in- en uitdiensttreding. Daarmee zijn nog niet alle onderdelen van het personeelsproces onderworpen aan interne controle. De volgende stap in de interne controle kan worden genomen door ook de loonmutaties, declaraties en verlofregistratie toe te voegen aan de controlewerkzaamheden.</p> |
| LKS                  | 😐                          | 😐                          | 😊      | <p>Het LKS-proces is in opzet toereikend. In het team dat belast is met de uitvoering van het LKS proces hebben in 2024 maar beperkt personele wijzigingen plaatsgevonden, in tegenstelling tot eerdere jaren. Hierdoor is de kwaliteit van de uitvoering van dit proces gedurende het jaar consistent geweest.</p> <p>Ten aanzien van de VIC merken wij op dat u de interne controles heeft verstevigd door meer waarnemingen uit te voeren ten opzichte van voorgaand jaar.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| WNT                  | 😊                          | 😊                          | n.v.t. | Geen wijzigingen ten opzichte van voorgaand jaar.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## 3.4 Overzicht van onze bevindingen t.a.v. de IT General Controls (1/4)

### Bevindingen IT General Controls

Hierna zijn de bevindingen opgenomen met betrekking tot de opzet en het bestaan van de door ons in het kader van de jaarrekeningcontrole onderzochte IT General Controls. Per bevinding is de status in het huidige jaar en in het voorgaande jaar aangegeven met betrekking tot de onderzochte IT-applicatie, zijnde Afas, en de hieraan gerelateerde IT-infrastructuur voor zover relevant voor de jaarrekeningcontrole. Onze relevante bevindingen en overige IT-gerelateerde bevindingen treft u op de volgende pagina's aan.

De scope van relevante IT General Controls wordt jaarlijks beoordeeld en kan hierdoor afwijken van de scope van voorgaande jaren.

### Geautomatiseerde gegevensverwerking

De accountant dient op basis van artikel 2:393, lid 4 BW aandacht te besteden aan de bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Wij hebben de automatiseringsorganisatie uitsluitend in het kader van de jaarrekeningcontrole beoordeeld. De interim-controle heeft hierbij geen tekortkomingen in de continuïteit en betrouwbaarheid van de geautomatiseerde gegevensverwerking aan het licht gebracht. Continuïteit is belegd bij de leverancier Afas, welke beschikt over een ISAE3402 verklaring. Hierin zijn geen uitzonderingen geconstateerd door de serviceauditor op het gebied van continuïteit.

## 3.4 Overzicht van onze bevindingen t.a.v. de IT General Controls (2/4)

### 1/2 - Afas

| OVERZICHT EN EVALUATIE VAN ITCG - PER APPLICATIE                           | AFAS                                                                                |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Logische toegangsbeveiliging                                               | 2024                                                                                |
| LT.1 - Procedure autorisatiebeheer                                         |  |
| LT.2 - Periodieke controle op toegang en juistheid ingerichte autorisaties |  |
| LT.3 - Identificatie van gebruikers voor toegang tot applicaties           |  |
| LT.4 - Authenticatie                                                       |  |
| LT.5 - Administrator- en superuser-accounts                                |  |
| Change management                                                          |                                                                                     |
| CM.1 - Wijzigingsbeheer applicaties                                        |  |
| CM.2 - Gescheiden IT-omgevingen                                            |  |

Als gevolg van bovenstaande observaties zijn aanvullende gegevensgerichte werkzaamheden gepland in het kader van de jaarrekeningcontrole.

## 3.4 Overzicht van onze bevindingen t.a.v. de IT General Controls (3/4)

### 2/2 - Afas

| BEVINDINGEN                                                             |                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prioriteit                                                              | Bevinding - incl. risico                                                                                                                                                                                                                             | Aanbeveling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Reactie management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LT.1 - Middel                                                           |                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Procedure autorisatiebeheer                                             | Wij hebben vastgesteld dat er in de aanvragen van gebruikers gebruik wordt gemaakt van een voorbeeldgebruiker of een voorganger van de nieuwe gebruiker om de autorisaties aan te vragen. Er wordt geen gebruik gemaakt van een formele normpositie. | Door het ontbreken van adequate naleving van gebruikersbeheerprocedures bestaat het risico dat personen over te veel of onjuiste autorisaties beschikken. Hierdoor bestaat de mogelijkheid dat de beoogde functiescheiding doorbroken kan worden met het risico op ongeautoriseerde handelingen in Afas. Tevens bestaat het risico dat een medewerker na uitdiensttreding toegang behoudt tot de betreffende applicaties en hierin transacties kan uitvoeren.                                    | Bij de procedure autorisatiebeheer is tijdens de controle vastgesteld dat er nog gebruik gemaakt wordt van kopie van medewerkersprofielen. Dit is nu niet meer toegestaan en wordt er bij een nieuwe functie of gewijzigde functie gekeken naar gewenste autorisatie en gecontroleerd door 4 ogen principe. Het is correct dat wij nog niet voor alle functies beschreven profielen hebben voor autorisatie. Hiervoor is het project autorisatie gestart waarbij we terug gaan naar de standaard normprofielen van AFAS. Dit wordt op dit moment december 2024 getest in een testomgeving. Dit dient 1e kwartaal 2025 te zijn geïmplementeerd in de productieomgeving. |
| LT.2 - Laag                                                             |                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Periodieke controle op toegang en juistheid van toegekende autorisaties | Voor Afas is geen zichtbare controle uitgevoerd op de actualiteit van gebruikers en juistheid van de toegewezen autorisaties.                                                                                                                        | Doordat gedurende het boekjaar geen review is uitgevoerd op de ingerichte autorisaties, loopt Ergon het risico dat medewerkers over ruimere autorisaties dan noodzakelijk voor uitoefening van hun functie kunnen beschikken, dan wel de beoogde functiescheiding kunnen doorbreken. Tevens kan met de huidige werkwijze van controleren een fout in de autorisatietoekenning te laat of niet worden opgemerkt met mogelijke doorbreking van functiescheiding en ongewenste mutaties tot gevolg. | Dit is mogelijk met de autorisatie tool online van AFAS. Hierbij zijn inderdaad geen lijsten van vastgelegd dat deze online controle heeft plaatsgevonden. Ook dit is onderdeel van het autorisatieproject met realisatie 1e kwartaal 2025.                                                                                                                                                                                                                                                                                                                                                                                                                            |

# 3.4 Overzicht van onze bevindingen t.a.v. de IT General Controls (4/4)

## Continuïteit

| OVERZICHT EN EVALUATIE VAN ITGC  |      |
|----------------------------------|------|
| Beheersmaatregelen in het proces | 2024 |
| CON.1 - Back-up maatregelen      | 😊    |
| CON.2 - Restoretests             | 😊    |

