

6 januari 2024

MANAGEMENT LETTER 2023

# Gemeente Weert

**BDO**

# Aanbiedingsbrief

Aan:

Gemeente Weert  
t.a.v. het college van B&W  
Postbus 950  
6000 AZ WEERT

Eindhoven, 6 januari 2024

Kenmerk:

## Ter informatie

De digitale versie van dit document is vanaf de inhoudsopgave interactief. Aan de hand van de navigatiebalk onderaan de pagina en/of de menustructuur bovenaan de pagina kan door het document genavigeerd worden.



VORIGE PAGINA



VOLGENDE PAGINA



INHOUDSOPGAVE



SAMENVATTING

Geacht college,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2023 van de gemeente Weert brengen wij u met deze management letter 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 onze opdrachtbevestiging.

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.

Wij vertrouwen erop u met deze management letter naar aanleiding van onze interim-controle 2023 van dienst te zijn geweest. Wij willen de organisatie bedanken voor de prettige samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Met vriendelijke groet,

BDO Audit & Assurance B.V.  
namens deze,

Drs. D.O. Meeuwissen RA  
Partner en extern accountant gemeente Weert

# Inhoudsopgave



## 1. DASHBOARD INTERIM-CONTROLE



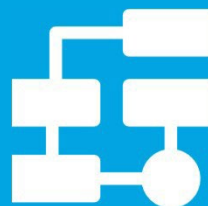
## 2. ONTWIKKELINGEN & AANDACHTSPUNTEN



## 3. ONS BEELD VAN DE INTERNE BEHEERSING



## 4. BEVINDINGEN IT-BEHEER



## 5. VOORUITBLIK JAARREKENING



## BIJLAGEN

# 1. Dashboard interim-controle

## 1.1 Dashboard interim-controle

# 1.1 Dashboard interim-controle

## ONS BEELD VAN DE INTERNE BEHEERSING

- ▶ Op basis van onze observaties hebben wij geconstateerd dat de interne beheersing en controleomgeving van voldoende niveau is om tot een betrouwbare jaarrekening te komen. Dit vormt een solide basis voor de accountantscontrole.
- ▶ Voor de insteek van de accountantscontrole kunnen wij niet volledig steunen op de processen, waardoor onze controleaanpak overwegend gegevensgericht is. Het is belangrijk om op te merken dat deze situatie ongewijzigd is en aansluit bij de bewuste werkwijze van uw organisatie, waarbij de Verbijzonderde Interne Controle (VIC) als achtervang wordt gebruikt.
- ▶ Uit de VIC over het eerste halfjaar 2023 komen geen bijzonderheden naar voren die in het kader van onze jaarrekeningcontrole van materieel belang zijn. Inmiddels treft de VIC voorbereidingen om de controle over het tweede halfjaar 2023 op te pakken.

## RECHTMATIGHEIDSVERANTWOORDING

- ▶ De rechtmatigheidsverantwoording is met ingang van boekjaar 2023 ingevoerd. De voorbereidende werkzaamheden voor de rechtmatigheidsverantwoording zijn onderhanden door de organisatie.
- ▶ De landelijke kaders zijn nog in ontwikkeling. Bij het schrijven van deze rapportage zijn diverse documenten gepubliceerd, ter consultatie aangeboden of onderhanden. Wij adviseren u deze ontwikkelingen nauw te volgen en hierop te anticiperen.

## ONTWIKKELINGEN EN AANDACHTSPUNTEN

- ▶ Over- en onderschrijdingen van baten of onderschrijdingen van lasten/investeringen betreffen op zichzelf geen begrotingsonrechtmatigheden maar het kan wel onrechtmatig zijn als deze afwijkingen niet tijdig in de (bijgestelde) begroting zijn verwerkt. Wat tijdig is, wordt bepaald door de interne afspraken tussen de gemeenteraad en het college van B&W over het rapporteren van afwijkingen en het aanpassen van de begroting.
- ▶ In het verlengde van het toenemende aantal specifieke uitkeringen heeft de gemeente medewerkers ingezet rondom de beheersing van specifieke uitkeringen waarmee verrassingen in de jaarafsluiting zoveel mogelijk worden voorkomen.

## IT-BEHEER

- ▶ Op basis van artikel 2:393, lid 4 BW dienen wij als accountant aandacht te besteden aan de bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.
- ▶ Beoordeelde systemen: Coda en Xworks.
- ▶ Onze bevindingen over de algemene IT-beheersmaatregelen uit voorgaande jaren blijven van kracht en zijn een bewuste keuze van de organisatie. Onze conclusie dat deze maatregelen overwegend ineffectief zijn blijft onveranderd derhalve zijn aanvullende (gegevensgerichte) werkzaamheden noodzakelijk om vast te stellen dat er zich geen materiële fouten en of risico's hebben kunnen voordoen tijdens de controle van de jaarrekening 2023.
- ▶ In hoofdstuk 4 is de vergelijking tussen 2022 en 2023 per onderdeel inzichtelijk gemaakt. De detailbevindingen zijn opgenomen in bijlage A.



## VOORUITBLIK JAARREKENING 2023

Naast de zichtbare follow-up van de bevindingen en aanbevelingen uit deze managementletter (hoofdstuk 2 tot en met hoofdstuk 4) vragen wij uw aandacht voor de volgende onderwerpen in de voorbereiding op het jaarrekeningtraject 2023.

- ▶ Het opstellen van een analyse van de begrotingsrechtmatigheid (zie nadere toelichting paragraaf 2.3);
- ▶ Actualisatie van de grondexploitatieopzetten per 31-12-2023 inclusief financiële doorrekeningen;
- ▶ Aanlevering van spendanalyse over gehele vierjaars- periode 2020-2023 met een interne toetsing op naleving van Europese aanbestedingsregels en bepaling omvang en aard geconstateerde rechtmatigheidsfout(en);
- ▶ Aanlevering van de WNT-verantwoording en onderliggende brondocumentatie;
- ▶ Tijdige beschikbaarheid verantwoordingsinformatie vanuit BsGW, centrumgemeente Roermond, CJG en zorgaanbieders.

## 2. Ontwikkelingen & Aandachtspunten

- 2.1 Rechtmatigheidsverantwoording
- 2.2 Rapporteren over fraude en continuïteit in de controleverklaring
- 2.3 Ontwikkelingen en aandachtspunten jaarrekening 2023

Geen apart oordeel rechtmatigheid in controleverklaring

### Invoering rechtmatigheidsverantwoording met ingang van 2023

Vanaf dit boekjaar geeft het college de rechtmatigheidsverantwoording voor wat betreft de financiële rechtmatigheid (het begrotingscriterium, voorwaardencriterium en misbruik en oneigenlijk gebruik) af. De rechtmatigheidsverantwoording maakt onderdeel uit van de jaarrekening. De accountant geeft een getrouwheidsoordeel af bij de jaarrekening en daarmee ook bij de rechtmatigheidsverantwoording. Dit betekent dat de accountant vanaf boekjaar 2023 in haar controleverklaring geen apart oordeel meer afgeeft over de rechtmatigheid. Ten aanzien van de SiSa-bijlage geeft de accountant nog wel een oordeel over de rechtmatigheid.

Bij het schrijven van deze managementletter zijn diverse documenten gepubliceerd, ter consultatie aangeboden of onderhanden:

- ▶ Het Besluit accountantscontrole decentrale overheden en de aanpassing van het BBV zijn ter consultatie gepubliceerd;
- ▶ De NBA-Handreiking 1152 rechtmatigheidstoelichting decentrale overheden is ter consultatie gepubliceerd;
- ▶ De kadernota rechtmatigheid van de commissie BBV is begin oktober 2023 openbaar gemaakt. De notitie van de commissie BADO wordt hierna geactualiseerd.

De SiSa-verantwoording wordt onderdeel van de rechtmatigheidsverantwoording in de jaarrekening, maar ook van de accountant zal worden verwacht dat deze ook rapporteert over de rechtmatigheid van de SiSa-verantwoording. Dat doen wij in het accountantsverslag maar mogelijk ook in de controleverklaring bij de jaarrekening als geheel.

De rechtmatigheidsverantwoording zorgt voor meer bewustwording bij de ambtelijke organisatie, het college en raad van haar verantwoordelijkheid voor een goed financieel beheer. De kaders en uitgangspunten voor de rechtmatigheidsverantwoording liggen enerzijds vast in wet- en regelgeving en worden anderzijds bepaald door de raad. Deze opzet stimuleert het dualisme waarin de raad een kaderstellende en controlerende rol inneemt.

De totstandkoming van de rechtmatigheidsverantwoording is een proces met interactie tussen verschillende gremia dat start bij het bepalen van de verantwoordingsgrens door de raad. Deze verantwoordingsgrens ligt tussen de 0% en 3% en de gemeente Weert heeft deze in een addendum op de financiële verordening 2021 (zoals voorgelegd in de raad d.d. 7 juni 2023) vastgesteld op 1% van de totale lasten van de gemeente inclusief de dotaties aan de reserves. De rapporteringsgrens is gelijk gesteld aan de verantwoordingsgrens.

Op de volgende pagina hebben wij een vereenvoudigde weergave van het proces van de totstandkoming van de rechtmatigheidsverantwoording in een afbeelding opgenomen.

Meer bewustwording verantwoordelijkheid

Verantwoordingsgrens vastgesteld op 1%

### Proces totstandkoming rechtmatigheidsverantwoording

#### Proces totstandkoming rechtmatigheidsverantwoording

- De organisatie voert de controles van het VIC-plan uit op basis van werklijsten en legt bevindingen vast in het VIC-verslag
- Het college stelt de rechtmatigheidsverantwoording op, waarin de bevindingen van het VIC-verslag zijn verwerkt en waarop toelichting plaatsvindt in de paragraaf bedrijfsvoering
- De accountant beoordeelt dat de rechtmatigheidsverantwoording getrouw is weergegeven in de jaarrekening



- De organisatie stelt op basis van het VIC-plan werklijsten op
- De organisatie stemt het VIC-plan én de werklijsten af met de accountant ter borging van de juistheid en volledigheid van uitgevoerde VIC-controles

- De raad bepaalt de verantwoordingsgrens en rapportagegrens
- De raad stelt het normenkader vast
- Grenzen en normenkader zijn opgenomen in het controleprotocol

- De organisatie operationaliseert het normenkader in een toetsingskader. *Aandachtspunt is dat alle toetspunten uit het kader zichtbaar worden gecontroleerd door de VIC als onderbouwing van de rechtmatigheidsverantwoording.*
- De organisatie maakt een verbijzonderd intern controleplan (VIC-plan) met hierin de aspecten vanuit het toetsingskader



## 2.1 Rechtmatigheidsverantwoording (3/3)

Belangrijke  
coördinerende rol ligt  
bij de VIC

De tijdigheid van de  
werkzaamheden van  
concern control/ VIC  
zijn van groot belang

Status rechtmatigheids-  
verantwoording bij de  
gemeente Weert

### Mogelijke doorontwikkeling VIC in het kader van de rechtmatigheidsverantwoording

Er is een belangrijke coördinerende rol voor de VIC weggelegd ten aanzien van de rechtmatigheidsverantwoording. Bij de gemeente Weert zijn de processen zo ingericht dat met name de VIC werkzaamheden, vastleggingen en uitkomsten de basis zijn voor de onderbouwing van de rechtmatigheidsverantwoording. De verantwoordelijkheden voor de rechtmatigheidsverantwoording liggen veel breder, alle organisatieonderdelen en het voltallige college 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. Dan kan de VIC 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'. Dit is een ontwikkeling die de gemeente Weert in de toekomst nog kan maken.

### Samenwerking VIC

De accountant maakt zoveel mogelijk gebruik van de uitgevoerde (verbijzonderde) interne controlewerkzaamheden van de gemeente Weert. Hierover zijn wij reeds met de VIC in overleg getreden, zodat de juiste werkzaamheden worden gedaan door beiden en wat een korte doorlooptijd van de controle bevordert. De tijdigheid van de werkzaamheden van de VIC zijn hierbij enorm van belang. In het kader van een goede samenwerking hebben wij o.a. onze werkprogramma's ten aanzien van SiSa en aanbestedingsrechtmatigheid met de gemeente Weert gedeeld. Wij adviseren in het kader van de aanbestedingsrechtmatigheid de VIC werkzaamheden explicieter vast te leggen conform de SDO notitie.

### Status rechtmatigheidsverantwoording bij de gemeente Weert

Binnen de organisatie is voldoende bewustzijn over de impact van de rechtmatigheidsverantwoording op de inrichting van interne beheersingsmaatregelen in de processen. De organisatie heeft de nodige voorbereidende acties uitgevoerd. In het interne controleplan 2023 van de gemeente Weert is aandacht voor de kaders, tolerantie, risico's en criteria. Het interne controleplan 2023 geeft een nadere invulling van de interne controle en omvat naast een beschrijving van de belangrijkste ontwikkelingen ook de gesignaleerde (fraude) risico's. In de werkplannen per proces zijn de interne beheersingsmaatregelen en de controlewerkzaamheden van de VIC gedetailleerd weergegeven. De opvolging van de actiepunten uit de VIC-controle dienen vastgelegd te worden en indien mogelijk worden gecorrigeerd. Hierbij adviseren wij om de beslisboom als bijlage (6) van Kadernota Rechtmatigheid 2023 te raadplegen om vast te stellen of de bevinding toeziet op een getrouwheids- of rechtmatigheidsfout. Onder andere ten aanzien van de foutenevaluatie zijn belangrijke wijzigingen doorgevoerd. In de rechtmatigheidsverantwoording worden alle afwijkingen boven de verantwoordingsgrens gerapporteerd. In de nieuwe Kadernota rechtmatigheid vallen 'afwijkingen' uiteen in fouten en onduidelijkheden. Onduidelijkheden doen zich voor in een situatie met complexe wet- en regelgeving, waarin de normstelling niet eenduidig uitlegbaar is. De Kadernota rechtmatigheid bevat geen mogelijkheid om afwijkingen als onzekerheid op te nemen. Daarnaast wordt in de nieuwe Kadernota rechtmatigheid nadere duiding aan het onderscheid tussen getrouwheids- en rechtmatigheidsfouten en (mogelijk) herstel van (door de VIC) geconstateerde fouten gegeven. De beslisboom in bijlage 6 van de Kadernota rechtmatigheid biedt handvatten om vast te stellen of een bevinding op een getrouwheids- of rechtmatigheidsfout toeziet.

Fraude en het vermogen om risico's vanuit de reguliere bedrijfsvoering financieel op te vangen

Jaarlijks frauderisicoanalyse

Transparantie over fraude en continuïteit vraag dialoog

### Onze controle gaat uit van de fraudepreventie door de gemeente

In onze managementletter 2022 hebben wij reeds aandacht gevraagd voor dit onderwerp. Onze beroepsorganisatie, de NBA, heeft een notitie uitgebracht 'best practice maatregelen fraude(risico)beheersing voor bestuurders en toezichthouders'. In deze notitie komt nadrukkelijk de rol van bestuurders en toezichthoudende organen, zoals de raad, bij het voorkomen en detecteren van fraude aan de orde. Door de nadruk te leggen op het voorkomen van fraude, kunnen de gelegenheden die tot fraude leiden, afnemen. Dit vraagt om actief toezicht op risico's en beheersmaatregelen ter voorkoming van fraude. Ook de accountant heeft hierin een belangrijke rol.

### Frauderisicoanalyse en het frauderesponseplan

Wij hebben in onze managementletter 2022 gerapporteerd over het belang van frauderisicobeheersing en het frauderesponseplan. De frauderisicoanalyse is in 2023 voorzien van een update en is besproken met de auditcommissie d.d. 5 oktober 2023. De frauderisicoanalyse omvat naast de risico's per proces ook de getroffen beheersingsmaatregelen. De toetsing van het adequaat functioneren van de beheersingsmaatregelen in het kader van frauderisicobeheersing vindt plaats via de interne controle. Daarnaast heeft de gemeente Weert in de fraude risico analyse opvolging gegeven aan het advies voor het opzetten van een fraude responsplan. In de Gedragscode ambtenaren gemeente Weert 2022, en Meldregeling vermoedens van misstanden en inbreuken gemeente Weert 2022 is uitgewerkt 'hoe te handelen' bij (vermoedens van) fraude.

Het vergroten van de rol van de raad ten aanzien van frauderisicobeheersing kan door bijvoorbeeld jaarlijks één of meerdere onderkende frauderisico's (en indien van toepassing de interne beheersings-maatregelen die zijn genomen om deze frauderisico's te mitigeren) nader te laten onderzoeken door de (verbijzonderde) interne controle, een accountant of een gespecialiseerde (fraude)onderzoeker.

Sterke toename aantal SiSa-regelingen

Procedure specifieke uitkeringen opgesteld

Het proces ten aanzien van de beheersing van specifieke uitkeringen

### Beheersing specifieke uitkeringen

Onderdeel van de jaarrekeningcontrole betreft de controle van de specifieke regelingen die in de SiSa-bijlage worden verantwoord. Wij zien een landelijke trend dat ministeries steeds vaker een specifieke regeling kiezen voor het verstrekken van subsidies aan decentrale overheden. Het aantal SiSa-regelingen, ook voor de gemeente Weert, is daardoor sterk toegenomen. Dit geeft een hoge druk op de organisatie binnen de gemeente, andere decentrale overheden en de accountantskantoren.

Jaarlijks publiceert het ministerie per decentrale overheid een overzicht van de van toepassing zijnde SiSa-regelingen. Tevens geven ministeries in de toekenningsbeschikkingen aan dat verantwoording via SiSa plaats dient te vinden. Gezien het hoge aantal regelingen en de omvang van de subsidiebedragen is het van belang om als organisatie een proces in te regelen omtrent de beheersing van specifieke uitkeringen en de verantwoording daarover. Wij hebben geconstateerd dat reeds een aantal stappen zijn gezet ten aanzien van de opzet van de interne beheersing, maar dat eveneens nog verdere stappen gemaakt kunnen worden.

Binnen organisatie zijn de volgende functies betrokken bij het proces met betrekking tot de Sisa: vak-ambtenaren, financieel adviseurs, teamleider financieel beheer en de coördinator interne controle. De coördinator interne controle zet de verschillende regelingen uit bij de vak-ambtenaar en houdt periodiek contact met deze personen aangaande de voortgang van het project, mede voor verantwoording in de SiSa. De teamleider financieel beheer voert jaarlijks bij het opstellen van de SiSa-bijlage, ten behoeve van de jaarrekening, per regeling een controle uit om de juiste, rechtmatige en volledige verwerking in de SiSa-bijlage te waarborgen.

De gemeente Weert heeft in de basis een goed proces voor beheersing van specifieke uitkeringen. In de bijlage is een actueel overzicht opgenomen van de SiSa-regelingen. Vanaf 2023 behoort de Sisa-bijlage bij de rechtmatigheidsverantwoording. De raad dient derhalve expliciet verantwoording af te leggen over de bestedingen in de Sisa-bijlage.

### Begrotingsrechtmatigheid

De commissie BBV publiceerde begin november een nadere duiding van de Kadernota rechtmatigheid 2023. Deze duiding heeft betrekking op:

1. Het al dan niet tijdig melden van afwijkingen van de begroting voor zowel baten, lasten als kredieten. Wat ‘niet tijdig’ concreet betekent wordt bepaald door de ‘spelregels’ tussen de Gemeenteraad en het College van B&W over het informeren en vaststellen van begrotingswijzigingen bij overschrijdingen van lasten of investeringsbudgetten en/of lagere of hogere baten dan begroot. Deze spelregels zijn veelal in de financiële verordening art. 212 Gemeentewet opgenomen.
2. Met de invoering van de rechtmatigheidsverantwoording, waarbij het toelichten en verantwoorden meer centraal staat, is het mogelijk om vóóraf afspraken te maken tussen de gemeenteraad en het college van B&W welke begrotingsonrechtmatigheden als acceptabel worden beschouwd (dus wel onrechtmatig, maar acceptabel). Deze afspraken kunnen in de financiële verordening art. 212 Gemeentewet worden opgenomen.

Wij vragen u voorafgaand aan de jaarrekeningcontrole 2023 een analyse op te stellen van de begrotingsrechtmatigheid waarbij bijlage 3 van de Kadernota rechtmatigheid 2023 een handreiking kan bieden.

# 3. Bevindingen significante processen

## 3.1 Inrichting van onze controle

## 3.1 Inrichting van onze controle (1/2)

### Inleiding

Zoals afgelopen jaar aangegeven, nemen de eisen die worden gesteld aan de accountantscontrole toe. Wij vinden het daarom van groot belang dat wij inzicht geven in de normen en verwachtingen ten aanzien van onze controle en de vertaling hiervan specifiek voor de gemeente Weert. Alleen dan gaat de discussie niet alleen over de kwaliteit van de accountantscontrole, maar vooral ook over de wijze waarop de gemeente hiervan kan profiteren. In deze management letter hebben wij daarom meer in detail uitgelegd op welke wijze wij de controle hebben ingericht en welke afwegingen wij daarbij maken. Wij doen dat door in deze paragraaf onze risico-inschatting, belangrijkste processen, controleaanpak en afwegingen te beschrijven. Voor ons totaalbeeld van de belangrijkste processen en bevindingen c.q. aandachtspunten verwijzen we naar bijlage A.



### Belangrijkste aandachtspunten:

- ▶ Management override
- ▶ Ongeautoriseerde handelingen in Coda en Xworks
- ▶ Waardering risicovolle grondexploitaties
- ▶ Getrouwheid rechtmatigheidsverantwoording

### Onze inschatting van de belangrijkste aandachtspunten

In het kader van de controle van de jaarrekening 2023 en onze aanpak hebben wij een zogenaamde initiële risico-inschatting gemaakt. Wij zien de volgende aandachtspunten in de controle van de jaarrekening van de gemeente Weert:

- ▶ In onze controlestandaarden (NV COS) wordt expliciet management override (bewuste beïnvloeding door bestuur of management van de jaarcijfers) als belangrijk aandachtspunt onderkend. Als accountant moeten wij in onze werkzaamheden hier specifiek aandacht aan besteden. Wij zijn van mening dat binnen de gemeente de mogelijkheden, om buiten de getroffen interne beheersmaatregelen invloed uit te oefenen op de in de jaarrekening gepresenteerde uitkomsten beperkt zijn. Het verrichten van een onjuiste/fictieve memoriaalboeking in de laatste maand van een tussentijdse rapportageperiode of het boekjaar dan wel bij het opstellen van de tussentijdse rapportage of de jaarrekening zien wij als enige mogelijkheid. Derhalve controleren wij deze memoriaalboekingen in detail.
- ▶ Om te voorkomen dat functionarissen handelingen verrichten die buiten hun functieomschrijving vallen en potentieel schadelijke gevolgen kunnen hebben voor gemeente Weert is het essentieel dat de logische toegangsbeveiliging goed is ingericht. Tijdens onze controle beoordelen wij de opzet en het bestaan van de logische toegangsbeveiliging van Coda en Xworks en controleren wij of handelingen in deze systemen zijn verricht door de juiste functionarissen. Hierbij zullen wij ons met name richten op de juiste autorisatie van inkoopfacturen en uitkeringen en IBAN-wijzigingen. Dit zijn de handelingen die volgens ons het meest waarschijnlijk ongeautoriseerd kunnen worden uitgevoerd door uw functionarissen, met name de functionarissen met super-userrechten.
- ▶ Tijdens de jaarrekeningcontrole besteden we specifiek aandacht aan de juiste waardering van de meest risicovolle projecten van de gemeente Weert. Dit omvat de schattingselementen in de exploitatieopzetten van grondexploitaties met een hoog risicoprofiel. Projecten worden als risicovol aangemerkt als sprake is van een hoge mate van schattingonzekerheid hetgeen zich uit in de aanzienlijke omvang van de nog te maken kosten en de nog te realiseren opbrengsten. Vanuit de audit 2022 zijn dit Laarveld, Kampershoek 2.0, Beekpoort-Noord en de Kempen Uitbreiding geweest. Op basis van de gesprekken gedurende de interim-controle met de verantwoordelijke planeconomen verwachten wij dat de selectie risicovolle grondexploitaties voor de audit 2023 ongewijzigd zal blijven daar geen nieuwe grondexploitaties zijn geopend in 2023. De definitieve selectie zullen wij bepalen zodra we de meest recente tussentijdse cijfers ontvangen. Hierover zijn afspraken gemaakt met de planeconomen en de coördinator interne controle.
- ▶ Getrouwheid van de rechtmatigheidsverantwoording. In de jaarrekening 2023 zal de gemeente Weert voor het eerst een rechtmatigheidsverantwoording opnemen. Dit als gevolg van een landelijke wetswijziging.

# 4. Bevindingen interim-controle

- 4.1 Informatiebeveiliging en cybersecurity
- 4.2 IT-beheersmaatregelen
- 4.3 Bevindingen IT-beheer | CODA
- 4.4 Bevindingen IT-beheer | Xworks
- 4.5 Digitale bestuurskracht



Verhoogde aandacht voor cybersecurity bij management en de toezichthouder

Ransomware kan de bedrijfscontinuïteit in gevaar brengen

Veranderingen in het digitale domein vragen van uw organisatie dat cybersecurity risico's periodiek worden geëvalueerd om vast te stellen of deze voldoende worden geadresseerd

### Informatiebeveiliging en cybersecurity

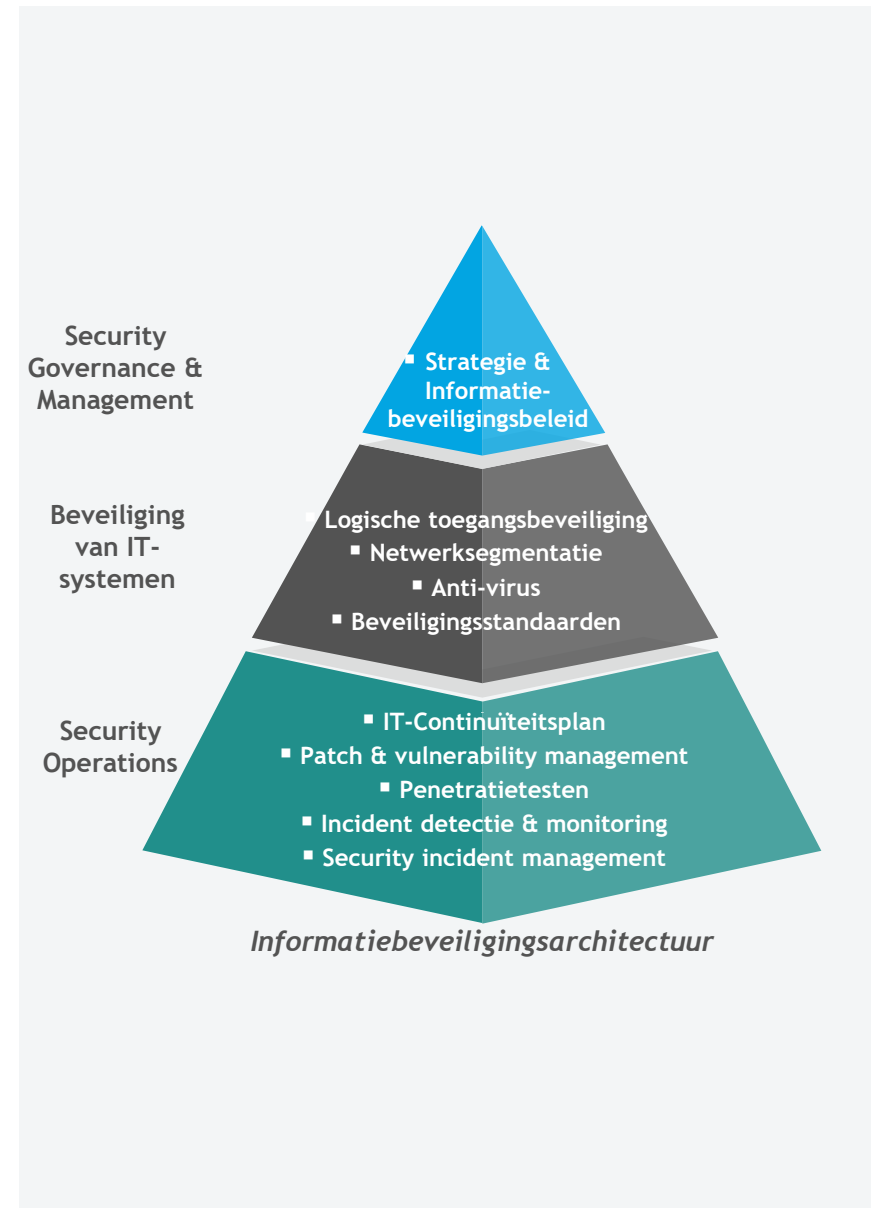
Vanuit onze natuurlijke adviesrol attenderen wij u graag op een aantal ontwikkelingen op het gebied van IT. Afgelopen jaren is er meer aandacht voor cybersecurity risico's ontstaan, mede door verhoogde (media)aandacht voor cybersecurity incidenten. Deze toegenomen aandacht voor cybersecurity risico's leeft bij zowel management, toezichthouders als ook het maatschappelijk verkeer. Organisaties zijn in sterke en toenemende mate afhankelijk van de continuïteit van IT-systemen. Zelfs zodanig dat bij het uitvallen of gijzeling (via ransomware) van de IT-systemen de bedrijfscontinuïteit geraakt kan worden. Dit kan daarmee een continuïteitsrisico in het kader van de jaarrekening met zich meebrengen.

Daarnaast is het van belang om te voldoen aan de aanstaande (vanaf 17 oktober 2024) Europese richtlijn NIS 2 (Netwerk- en Informatiesystemen 2) voor cybersecurity. Ook kan een cybersecurity incident leiden tot ongeautoriseerde toegang tot gevoelige gegevens waardoor er niet voldaan wordt aan de privacywetgeving (AVG).

Een cybersecurity incident, een incident als gevolg van activiteiten/ calamiteiten in het cyberdomein (digitale domein) kan resulteren in:

- ▶ Verstoringen in bedrijfsvoering (en daarmee eventueel continuïteit);
- ▶ Datalekken door ongeautoriseerde toegang tot gegevens;
- ▶ Fraude (beïnvloeding/manipulatie van gegevens);
- ▶ Aanzienlijke reputatieschade;
- ▶ Diefstal.

Als gevolg van de snelheid waarmee het digitale (cyber)domein zich ontwikkelt is het zeer belangrijk om continu en grondig te evalueren of cybersecurity risico's nog passend (juist en volledig) worden geadresseerd. Dit kunt u doen door veranderingen in dreigingen of kwetsbaarheden te identificeren en de effectiviteit van getroffen maatregelen periodiek te toetsen.



### Inventarisering

Tijdens de audit hebben we de getroffen maatregelen m.b.t. Informatiebeveiliging en cybersecurity geïnventariseerd en bewijsstukken geïnspecteerd. Hiermee hebben wij geïnventariseerd dat de Gemeente Weert:

- ▶ Beschikt over een specifiek belegde CISO functie;
- ▶ Inzicht heeft in het IT-landschap via ICT-NML waardoor cyber risicobereidheid effectief kan worden ingericht;
- ▶ De technische informatiebeveiligingsmaatregelen grotendeels heeft uitbesteed aan serviceorganisatie ICT-NML en jaarlijks middels TPM inzicht krijgt in de kwaliteit van de beheersing hieromtrent;
- ▶ Beschikt over gedocumenteerde procedures en beleidsstukken waaronder, maar niet beperkt tot Identity & Access Management, Incidenten management en Uitwijktesten;
- ▶ Beschikt over een actueel informatiebeveiligingsbeleid met daarin verwerkt de beveiligingsstrategie en taken en verantwoordelijkheden die hiermee samenhangen;
- ▶ Via ICT-NML wekelijkse vulnerability scans uitgevoerd krijgt;
- ▶ Phishingtests heeft uitgevoerd onder haar medewerkers ter bewustwording van social engineering risico's;
- ▶ Via ICT-NML beschikt over een SIEM/SOC oplossing van Ilionx.

### Aanbeveling

Op basis van de geïnventariseerde maatregelen adviseren we u jaarlijks als klant van serviceorganisaties een beoordeling te doen op de scoping van de relevante assurance verklaringen dit ter controle of de in de assurance-verklaring gebruikte scope en behaalde doelstellingen nog in lijn zijn met de behoefte cq verwachtingen van de gemeente.

Wij beoordelen de betrouwbaarheid en continuïteit IT voor zover relevant voor de controle van de jaarrekening

### IT-audit algemeen

In het kader van de jaarrekeningcontrole is een IT-audit uitgevoerd. De IT-audit is primair gericht op de betrouwbaarheid van de gegevensverwerking ten behoeve van de totstandkoming van de jaarrekening. Dit betekent dat de uitkomsten van de IT-audit geïnterpreteerd moeten worden met de uitkomsten van de andere werkzaamheden van de accountant en de IT-audit zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan.

Het inzicht in de betrouwbare werking van ICT-systemen en applicaties en het gebruik daarvan door de Gemeente Weert, vormen een onderdeel van de kwaliteit van de interne beheersing en de administratieve organisatie. Algemene IT-beheersmaatregelen (hierna: IT General Controls) rond uw kritieke systemen leveren daarnaast onder meer een belangrijke bijdrage aan het mitigeren van de risico's op onbeheerste wijzigingen, ongeautoriseerde handelingen en het optreden van verstoringen en het beperken van de impact op de gegevensverwerking.

De bevindingen zoals gerapporteerd in deze management letter zijn gericht geweest op het beoordelen van de opzet en het vaststellen van het bestaan van algemene IT-beheersmaatregelen voor zover relevant voor de jaarrekeningcontrole. Wij hebben in samenwerking met onze IT-auditors deze maatregelen beoordeeld om de impact van de risico's vanuit IT te kunnen vaststellen voor die systemen en applicaties die gekoppeld zijn aan de voor ons relevante processen en posten.

Op het moment dat de intern getroffen IT General Controls rondom de applicaties in scope niet (bewijsbaar) voldoende aanwezig zijn, dan heeft dit mogelijk invloed op interne beheersingsmaatregelen in de applicaties en rapportages vanuit de applicaties. De impact van de bevindingen met betrekking tot de IT General Controls zal bij de betreffende processen worden behandeld.

### Toelichting status IT General Controls

Het hierna opgenomen schema bevat een weergave van de status van de opzet en het bestaan van de door ons in het kader van de jaarrekeningcontrole onderzochte IT General Controls in het huidig jaar en in voorgaand jaar binnen de onderzochte systemen, zijnde Coda en Xworks. Onze relevante bevindingen met betrekking tot de IT General Controls en overige IT-gerelateerde bevindingen treft u hierna en in bijlage B aan.

Op de volgende pagina's zijn vervolgens onze bevindingen met betrekking tot de IT General Controls tekstueel nader toegelicht. Tenslotte zijn onze overige IT-gerelateerde bevindingen uiteengezet. De scope van relevante IT General Controls wordt jaarlijks beoordeeld en kan hierdoor afwijken van de scope van voorgaande jaren.

Beoordeelde systemen:

- ▶ CODA
- ▶ Xworks

Detailbevindingen  
IT weergegeven in  
bijlage B

Logische toegangsbeveiliging nog deels ontoereikend

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar bijlage B

PROCES	2022	2023	KORTE OMSCHRIJVING BEVINDINGEN
Logische toegangsbeveiliging			
1. Procedure autorisatiebeheer BIO norm: 9.2.1 & 9.2.2.1 & 9.2.2.2 & 9.2.3.1	●	●	<b>Indienst:</b> Voor één willekeurige gebruiker vastgesteld dat er een gedocumenteerde aanvraag is gedaan en rechten in lijn met de aanvraag zijn toegekend. Rechtenoekenning gebeurd op basis van kopiegebruiker waarmee er een restrisico bestaat dat de verkeerde rechten worden toegekend. <b>Uitdienst:</b> Voor één willekeurige uitdiensttreder vastgesteld dat toegang tot de applicatie tijdig is ontnomen.
2. Periodieke controle op toegang en juistheid ingerichte autorisaties BIO norm: 9.2.5	●	●	De coördinator interne controle heeft een review uitgevoerd op de juistheid van autorisaties middels een vergelijking tussen rechten en huidige functies zonder gebruik van een normpositie. Actualiteit van gebruikers is geen inzichtelijk onderdeel van de review geweest.
3. Identificatie van gebruikers voor toegang tot applicaties BIO norm: 9.2.1.1 & 9.2.1.2	●	●	Generieke accounts zijn verklaarbaar vanuit gebruiksdoeleinden.
4. Authenticatie (SSO via AD) BIO norm: 9.4.3.1 - 9.4.3.5	●	●	Wachtwoordmaatregelen voldoen in de basis aan de BDO minimum-practice. Active Directory beheer ligt bij partij Syntrophos die vanuit Privacy en Security overwegingen geen volledig inzicht geven in de totale AD-inrichting. Hiermee bestaat er door beperkt inzicht een restrisico dat gebruikers uitgezonderd zijn van wachtwoord wijzigen. Dit wordt als beperkt ingeschat door de overige sterkere maatregelen.
5. Administrator- en superuser-accounts BIO norm: 9.2.3	●	●	Één gebruiker met een dubbelfunctie in zowel de lijn- als IT-organisatie beschikt over superuser-rechten, waarmee functiescheiding wordt doorbroken.
Change management			
6. Wijzigingsbeheer BIO norm: 12.1.2 & 12.1.4	●	○	Er is in 2021 vastgesteld dat er een wijzigingsbeheerproces door de Gemeente Weert is ingericht, waarbij updates worden getest voordat ze worden doorgevoerd. Wij hebben het proces dit jaar niet vastgesteld, omdat het niet in scope is van de audit.
Continuïteit			
7. Back-up en restore BIO norm: 11.2 & 12.3.1.1 - 12.3.1.4 & 12.3.1.5	●	○	We hebben in 2021 vastgesteld dat er back-ups voldoende zijn ingericht en dat er een restoretest is uitgevoerd. Wij hebben het proces dit jaar niet vastgesteld, omdat het niet in scope is van de audit.

● onvoldoende ● verbeterpunten ● voldoende ● geen waarneming ○ niet onderzocht

Logische toegangsbeveiliging deels ontoereikend

Continuïteit deels ontoereikend

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar bijlage B

PROCES	2023	KORTE OMSCHRIJVING BEVINDINGEN
Logische toegangsbeveiliging		
1. Procedure autorisatiebeheer BIO norm: 9.2.1 & 9.2.2.1 & 9.2.2.2 & 9.2.3.1	●	<b>Indienst:</b> Voor één willekeurige gebruiker vastgesteld dat er een gedocumenteerde aanvraag is gedaan en rechten in lijn met de aanvraag zijn toegekend. Rechtenoekenning gebeurt op basis van kopiegebruiker waarmee er een restrisico bestaat dat de verkeerde rechten worden toegekend. <b>Uitdienst:</b> Voor één willekeurige uitdiensttreder vastgesteld dat toegang tot de applicatie tijdig toegang is ontnomen.
2. Periodieke controle op toegang en juistheid ingerichte autorisaties BIO norm: 9.2.5	●	Er heeft ten tijde van de audit nog geen gedocumenteerde controle plaatsgevonden op de juistheid van autorisaties en actualiteit van gebruikers.
3. Identificatie van gebruikers voor toegang tot applicaties BIO norm: 9.2.1.1 & 9.2.1.2	●	Generieke accounts zijn verklaarbaar vanuit gebruiksdoeleinden.
4. Authenticatie (SSO via AD) BIO norm: 9.4.3.1 - 9.4.3.5	●	Wachtwoordmaatregelen voldoen in de basis aan de BDO minimum-practice. Active Directory beheer ligt bij partij Syntrophos die vanuit Privacy en Security overwegingen geen volledig inzicht geven in de totale AD-inrichting. Hiermee bestaat er door beperkt inzicht een restrisico dat gebruikers uitgezonderd zijn van wachtwoord wijzigen. Dit wordt als beperkt ingeschat door de overige sterkere maatregelen.
5. Administrator- en superuser-accounts BIO norm: 9.2.3	●	Drie gebruikers uit lijnorganisatie beschikken over superuser-rechten, waarmee functiescheiding wordt doorbroken.
Change management		
6. Wijzigingsbeheer BIO norm: 12.1.2 & 12.1.4	○	Er is in 2021 vastgesteld dat er een wijzigingsbeheerproces door de Gemeente Weert is ingericht, waarbij updates worden getest voordat ze worden doorgevoerd. Wij hebben het proces dit jaar niet vastgesteld, omdat het niet in scope is van de audit.
Continuïteit		
7. Back-up en restore BIO norm: 11.2 & 12.3.1.1 - 12.3.1.4 & 12.3.1.5	●	Continuïteitsmaatregelen zijn belegd bij serviceorganisatie Blinqt. Blinqt heeft nog geen assurance beschikbaar ter controle van de specifieke maatregelen hieromtrent.

● onvoldoende
 ● verbeterpunten
 ● voldoende
 ● geen waarneming
 ○ niet onderzocht

### Digitale Bestuurskracht gemeente Weert

Vanwege het toenemende belang van digitalisering hebben wij een inventarisatie gedaan naar het volwassenheidsniveau van de Digitale Bestuurskracht van uw organisatie. Deze inventarisatie maakt inzichtelijk wat het vermogen van uw organisatie is om door middel van digitalisering uw opgaven uit te kunnen voeren en wat hierin geoptimaliseerd kan worden. Dit is geen uitgebreid onderzoek geweest, maar een inventarisatie op basis van een vragenlijst, aangevuld met interviews. De volwassenheidsscan heeft ten doel om vanuit onze natuurlijke adviesfunctie mee te denken over dit belangrijke onderwerp, onze observaties te delen, de uitkomsten in de branche te benchmarken en ervaringen te delen. Vanzelfsprekend zijn wij graag bereid met u hierover verder van gedachten te wisselen. De resultaten van de volwassenheidsscan zijn op de volgende pagina weergegeven. Hieronder hebben wij de belangrijkste observaties beknopt uitgewerkt.

### Overall beeld gemeente Weert

Op basis van de hierboven benoemde werkzaamheden valt het ons op dat gemeente Weert vergevorderd is met de uitrol van het traject 'Sturen op Effecten'. Met de invoering van "Sturen op Effecten" wordt een transitie doorlopen van sturen op "input" (taken die uitgevoerd worden) via "output" (prestatie die geleverd is) naar "outcome" (het effect dat in de maatschappij zichtbaar wordt). Daarmee wordt het maken van keuzes transparant en gekoppeld aan de inzet van middelen. Op strategisch en operationeel niveau zijn KPI's gedefinieerd en daarop wordt gestuurd. Het definiëren van KPI's op tactisch niveau staat op de planning. Wij onderschrijven deze inspanning om op alle niveaus in de organisatie transparantie op de gemaakte keuzes, met bijbehorende middelen, te creëren. Daarnaast merken wij op dat in deze fase meestal niet de techniek maar vooral de digitale vaardigheid en digitale weerbaarheid van medewerkers en inwoners een grote uitdaging is. Medewerkers moeten immers de techniek op een veilige manier bedienen en inwoners moeten vaardig om kunnen gaan met digitale informatie en gemeentelijk digitale diensten en producten. Daarom adviseren wij om concern-breed en integraal voldoende aandacht te schenken aan het verhogen van de digitale vaardigheid en -weerbaarheid door bijvoorbeeld een apart trainingsplan op te stellen, gericht op de integratie van informatievoorziening in de bedrijfsvoering en samenleving.

### Externe ontwikkelingen

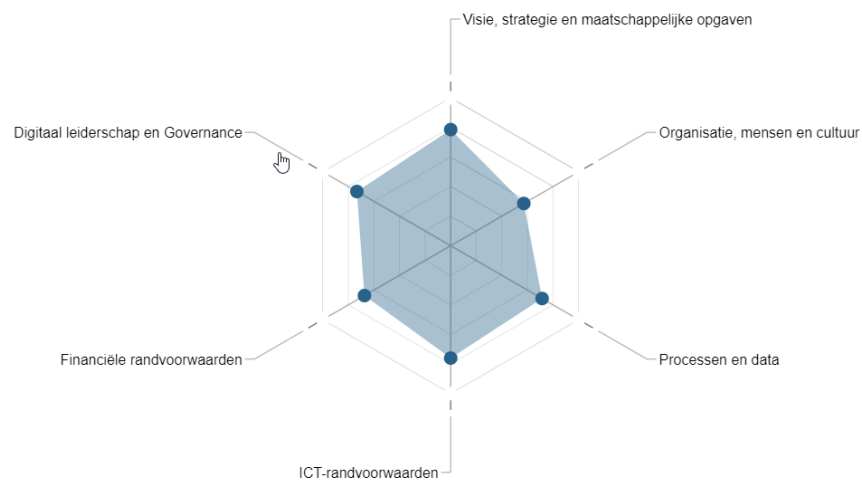
In ons dagelijks leven is de vergaande digitalisering niet meer weg te denken en volgen deze ontwikkelingen elkaar razendsnel op. Waar het hebben van een iPad destijds nog nieuw was, bestaan nu al AI-programma's zoals Chat GPT die zelf rapportages kunnen schrijven. Nu zijn niet alle ontwikkelingen even relevant voor de gemeente Weert, maar het is wel belangrijk deze ontwikkelingen te volgen en te verkennen wat deze ontwikkelingen in potentie voor de gemeente kunnen betekenen. Wij adviseren daarbij eveneens aandacht te houden voor een gezonde balans tussen innovatie en de basis op orde houden alsook het tempo waarmee de ontwikkeling al dan niet omarmt wordt.

## Financiële randvoorwaarden

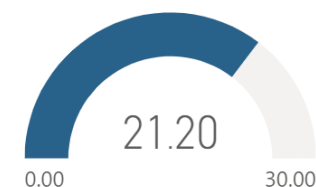
De bouwsteen financiële randvoorwaarden richt zich op benodigde investeringen. De kosten voor Informatievoorziening zullen de komende jaren alleen maar toenemen, dat is naar onze mening een onomkeerbaar proces. De uitdaging is de toenemende uitgaven zodanig in te zetten dat gemeenten de voordelen van de digitalisering, innovatie en het data-gedreven werken kunnen benutten. Dan is dit geen steeds hoger wordende kostenpost, maar een bewuste investering in een betere digitale sturing en beheersing van de organisatie. Wij hebben begrepen dat bij de gemeente Weert structurele middelen beschikbaar zijn gesteld om reguliere en innovatieve Informatievoorzieningsprojecten te bekostigen. Wij onderschrijven de toekenning van deze structurele middelen, temeer omdat wij een toename van de benodigde investeringen, gelet op de razendsnelle ontwikkelingen in de markt verwachten. Daarom adviseren wij ook om zoveel als mogelijk de komende jaren rekening te houden met deze verwachte toename van investeringen.

Verdeling punten over bouwstenen

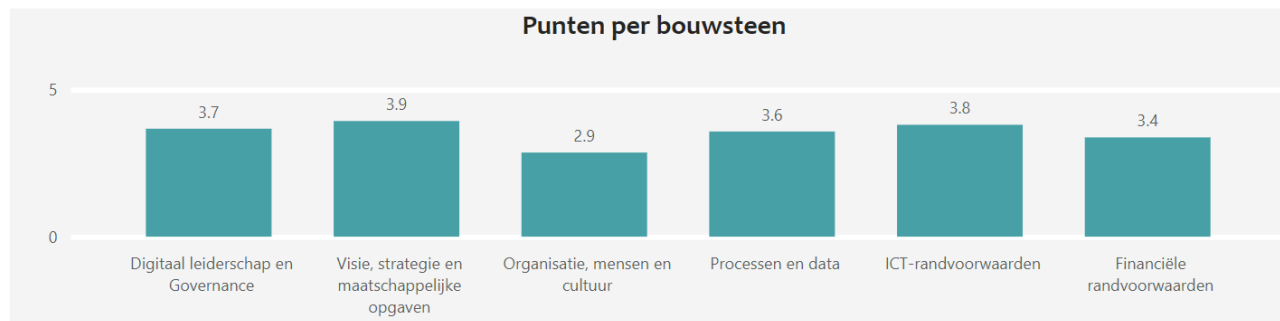
Punten per bouwsteen



Totaal aantal punten



Punten per bouwsteen



# 5. Vooruitblik jaarrekening 2023

## 5.1 Vooruitblik jaarrekening 2023



## Gemaakte afspraken voor jaarrekeningcontrole 2023

We hebben afgesproken om net als vorig jaar voorafgaand aan de accountantscontrole een scan uit te voeren op het (digitale) jaarrekeningdossier om te beoordelen of de opgevraagde controledocumentatie tijdig is opgeleverd en een solide basis vormt voor onze werkzaamheden.

Wij onderkennen de volgende aandachtspunten voor de jaarrekeningcontrole 2023:

- ▶ Zichtbare follow-up van de bevindingen en aanbevelingen uit deze managementletter (hoofdstuk 2 tot en met 4);
- ▶ Actualisatie van de grondexploitatieopzetten per 31-12-2023 inclusief financiële doorrekeningen en zichtbare follow-up van de aandachtspunten uit deze managementletter (hoofdstuk 3.2);
- ▶ Aanlevering van de spendanalyse over de gehele vierjaarsperiode 2020-2023 met een interne toetsing op de naleving van de Europese aanbestedingsregels. Hierbij dient rekening te worden gehouden met de aandachtspunten uit de notitie 'Uitvoering van controle op aanbestedingsrechtmatigheid bij jaarrekeningcontrole van decentrale overheden' van de NBA-SDO. Verder vragen wij uw specifieke aandacht voor de betrouwbaarheid van het gehanteerde lijstwerk om de volledigheid van de uitgevoerde spendanalyse te waarborgen;
- ▶ Aanlevering van een overzicht van de lasten Wmo per zorgaanbieder met de onderliggende productieverantwoordingen en bijbehorende controleverklaringen inclusief een verschillenanalyse. In dit kader hebben wij uw organisatie voorgaande jaren reeds gefaciliteerd met een format met de juiste documentatievereisten;
- ▶ Aanlevering van de WNT-verantwoording en onderliggende brondocumentatie;
- ▶ Aanlevering van een kwalitatief en kwantitatief goed balansdossier waarop intern een zichtbare 'kwaliteitscheck' is verricht;
- ▶ Aanlevering van standaardbankverklaringen en advocatenbrieven per 31-12-2023. Daarnaast aanlevering van de 'tax letter' waarin de relevante informatie rondom de fiscaliteiten (Vpb, btw en LB) wordt vermeld. Wij zullen u hiervoor de template nog aanreiken.
- ▶ Aandacht voor de frauderisico's in de programmarekening en de programmaverantwoording.
- ▶ Betrouwbare export van de geboekte inkoopfacturen 2023 uit Coda waarbij zichtbaar is op regelniveau welke functionaris de inkoopfactuur heeft aangemaakt en welke budgethouder deze heeft geautoriseerd.

Mede gezien de ervaringen is het van essentieel belang met derde partijen afspraken te maken dat de verantwoordingsinformatie voor de vaststelling van de jaarrekening door het college van B&W beschikbaar is. Dit betreft met name:

- ▶ De dossiercontrole op de zorgtoekenningen door het Centrum voor Jeugd en Gezin;
  - ▶ De productieverantwoordingen (inclusief bijbehorende controleverklaringen) van de zorgaanbieders Wmo en Jeugdzorg;
  - ▶ De verantwoordingsinformatie inzake de jeugdzorglasten vanuit centrumgemeente Roermond;
  - ▶ De verantwoordingsinformatie inzake de gemeentelijke belastingen/heffingen vanuit de gemeenschappelijke regeling BsGW.
- Het is van belang dat uw organisatie stuurt op een tijdige realisatie van bovengenoemde afspraken. Dit komt ten goede aan de efficiëntie van het jaarrekeningproces en de jaarrekeningcontrole.

# Bijlagen

- A Effectiviteit processen
- B Detailbevindingen IT-beheer
- c Indicatie omvang Sisa-verantwoording 2023

# A. Effectiviteit processen

## 3.2 Effectiviteit processen (1/2)

PROCES	CTFS	OPZET AO/IB	VIC	T.o.v. 2022	GEWIJZIGDE CONCLUSIE T.A.V. DE CONTROLEAANPAK (t.o.v. voorgaand jaar)?
Planning & Control (incl. memorialen)	●	●	●	→	Er is sprake van een adequaat functionerende planning-en-controlcyclus. Binnen dit proces is sprake van interne beheersmaatregelen. Als voorbeeld noemen we de onafhankelijke toets op de juistheid en rechtmatigheid van memoriaalboekingen, de WNT-verantwoording en de SiSa-verantwoording en de interne kwaliteitscheck op de jaarstukken. Deze maatregelen worden echter niet altijd toereikend genoeg vastgelegd, waardoor achteraf niet toetsbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd.
Inkoop- en betalingsproces	●	●	●	↓	<p>Wij hebben geconstateerd dat twee medewerkers van de afdeling Financiën beide zelfstandige betaalbevoegdheden hebben in de Rabobank applicatie om iDeal betalingen te verrichten tot 10.000 euro. Voor dit deelproces is een procedure aanwezig waarbij iDeal betalingen via een formulier worden aangevraagd en dienen te worden geautoriseerd door de budgethouder voordat de iDeal betaling mag plaatsvinden. Achteraf wordt door medewerker FA per bankafschrift alle betalingen gecodeerd, waarbij betalingen zonder onderliggende documentatie op een tussenrekening worden verantwoord om verder uitgezocht te worden. Ondanks de aanwezige interne beheersingsmaatregelen blijft het theoretisch risico aanwezig dat iDeal betalingen kunnen plaatsvinden zonder goedkeuring van de budgethouder.</p> <p>Verder is (nog) geen deugdelijke interne beheersing aanwezig op (de volledigheid van het) het contractenregister. Daarnaast zijn de IT-beheersmaatregelen omtrent logische toegangsbeveiliging ontoereikend (als gevolg van superusers) om de betrouwbaarheid van geautomatiseerde gegevensverwerking te waarborgen. Verdere details zijn beschikbaar in hoofdstuk 4 en bijlage B van deze managementletter.</p>
Aanbestedingen	●	●	●	→	<p>Wij hebben de tussentijdse spendanalyse 2023 t/m Q2 beoordeeld en hierbij terugkoppeling gegeven aan de coördinator interne controle voor aanvullende onderbouwing (correspondentie en/of inlichtingen) voor de gegeven (tussentijdse) conclusies ten aanzien van de aanbestedingsrechtmatigheid.</p> <p>Aandachtspunt hierbij is om in de spendanalyse per crediteur de punten uit de SDO-notitie expliciet te laten vastleggen waarbij een conclusie wordt gevormd over de aanbestedingsrechtmatigheid. Aangezien deze analyse niet zichtbaar is uitgevoerd in de tussentijdse spendanalyse t/m 2023 Q2 hebben wij dit niet kunnen beoordelen. We verwachten deze analyse te ontvangen voordat de jaarrekeningcontrole begint. Aandachtspunt is dat alle toetspunten uit de SDO-notitie zichtbaar worden gecontroleerd door de VIC als onderbouwing van de rechtmatigheidsverantwoording.</p> <p>Aandachtspunt blijft de (zichtbare) controle op de actualisatie en parameters in de exploitaties. Ook voor 2023 dient bij de actualisatie rekening gehouden te worden met het hoge inflatiecijfer in 2023. Ter volledigheid vermelden wij het aandachtspunt om gewijzigde prognoses in exploitatieopzetten tussen jaar T en T-1 adequaat te onderbouwen, waarbij de financieel specialist grondexploitatie zichtbaar de aansluiting maakt tussen de herziene exploitatie opzet uit jaar T met en de financiële administratie. Deze werkzaamheden vinden plaats na de jaarwisseling aangezien de grondexploitatie één keer per jaar worden geactualiseerd.</p>
Grondexploitatie	●	●	●	→	Er zijn interne beheersmaatregelen aanwezig op het declaratieproces, zoals de onafhankelijke toets op de juistheid en rechtmatigheid van declaraties inclusief uitbetalingen. Deze controlemaatregelen worden niet zichtbaar vastgelegd waardoor het achteraf niet mogelijk is om te toetsen of de controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd.
Personeel	●	●	●	→	Vastgesteld dat ten opzichte van voorgaand jaar functiescheiding wordt afgedwongen in XWorks tussen de opvoer en autorisatie van bankrekeningnummers van cliënten. Echter is sprake van ontoereikende IT-beheersmaatregelen (logische toegangsbeveiliging: autorisatiebeheer en drie accounts met superuserrechten) om een betrouwbare gegevensverwerking te waarborgen (zie hoofdstuk 4 in deze managementletter). De accounts met superuserrechten zijn tevens betrokken bij het proces inzake opvoer en autorisatie bankrekeningnummers.
Uitkeringen in geld en natura	●	●	●	→	BsGW is verantwoordelijk voor het belastingproces. Het is echter een blijvend aandachtspunt om grip te hebben en te houden op een correcte en volledige aanlevering van gegevens, zoals omgevingsvergunningen, aan BsGW aangezien dit onder de verantwoordelijkheid van de gemeente Weert valt.
Gemeentelijke belastingen en heffingen	●	●	●	→	

● ontoereikend  
 ● toereikend, met verbeterpunten  
 ● toereikend  
 ● geen waarneming  
   niet onderzocht

→ geen verandering ten opzichte van voorgaand jaar  
 ↓ verslechterd ten opzichte van voorgaand jaar  
 ↑ verbeterd ten opzichte van voorgaand jaar

## 3.2 Effectiviteit processen (2/2)

PROCES	CTFS	OPZET AO/IB	VIC	T.o.v. 2022	GEWIJZIGDE CONCLUSIE T.A.V. DE CONTROLEAANPAK (t.o.v. voorgaand jaar)?
Parkeeropbrengsten	●	●	●	→	Proces inzake parkeeropbrengsten is adequaat en de volledigheid van de opbrengsten is gewaarborgd.
Omgevingsvergunningen Huren en pachten Treasury	●	●	●	→	Binnen het proces is sprake van interne beheersmaatregelen. Deze maatregelen worden echter niet altijd toereikend genoeg vastgelegd, waardoor achteraf niet toetsbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd. Volledigheidshalve vermelden we dat ten tijde van de interim-controle 2023 geen nieuwe leningen zijn afgesloten (treasury).
Uitkering gemeentefonds Verbonden partijen Subsidieverstrekingen en inkomensoverdrachten tussen overheden	●	●	●	→	Er zijn interne beheersmaatregelen van toepassing op het proces echter worden deze maatregelen niet altijd adequaat vastgelegd waardoor het achteraf niet mogelijk is om te toetsen of de controlemaatregelen zijn uitgevoerd en op welke wijze deze zijn uitgevoerd.

● ontoereikend  
 ● toereikend, met verbeterpunten  
 ● toereikend  
 ● geen waarneming  
 ○ niet onderzocht

→ geen verandering ten opzichte van voorgaand jaar  
 ↓ verslechterd ten opzichte van voorgaand jaar  
 ↑ verbeterd ten opzichte van voorgaand jaar

## B. Detailbevindingen IT-beheer

Bevinding	Indienst	RISICO: gemiddeld
Jaar van constatering	2023	IMPACT: gemiddeld
Onze bevinding	<p><b>Indienst - Coda &amp; Xworks</b></p> <ul style="list-style-type: none"> <li>▶ Aanvraag voor rechtentoeakening gebeurd door een daarvoor bevoegde medewerker middels ticket met medewerkersinformatie;</li> <li>▶ Rechtentoeakening gebeurd op basis van kopie van een bestaande gebruiker zonder gebruik van een normpositie;</li> </ul> <p><u>Conclusie:</u> Door het ontbreken van een eenduidige koppeling tussen functie en autorisaties bestaat het risico op foutieve rechtentoeakening.</p>	
Risico	<p>Door het ontbreken van adequate naleving op gebruikersbeheerprocedures bestaat het risico dat personen teveel of onterechte rollen/rechten bezitten en hierdoor de functiescheidingsprincipes mogelijk doorbroken kunnen worden met het risico op ongeautoriseerde handelingen. Tevens bestaat het risico dat een medewerker na uitdiensttreding toegang behoudt tot de betreffende applicaties en hierin transacties kan uitvoeren. Het intrekken van toegangsrechten per applicaties heeft als risico dat dit niet tijdig voor elke applicatie wordt gedaan.</p>	
Onze aanbeveling	<p>Het verdient de aanbeveling om een formele normpositie voor Coda en Xworks op te stellen zodat de belangrijkste gewenste functiescheidingsprincipes zichtbaar zijn gemaakt. In navolging hierop raden we aan om dit jaarlijks vooraf door het management te laten goedkeuren, zodat dit organisatie-breed wordt gedragen en baseline biedt. Aan de hand van deze normpositie dienen de verzoeken tot het aanvragen en muteren van gebruikers met rollen en rechten beoordeeld te worden alvorens deze autorisatiegroep/rechten worden toegekend.</p>	
Reactie management		

Bevinding	Periodieke review op juistheid van autorisaties en actualiteit van gebruikers	RISICO: laag
Jaar van constatering	2023	IMPACT: laag
Onze bevinding	<p>Voor Xworks is niet inzichtelijk een controle uitgevoerd op de juistheid van toegekende autorisaties. Voor applicaties Xworks en Coda is geen inzichtelijke controle uitgevoerd op de actualiteit van gebruikers.</p> <p>Hiermee bestaat het risico dat incorrecte toekenning van rechten en/of de niet tijdige blokkering van gebruikers onopgemerkt blijft.</p>	
Risico	<p>Door het ontbreken van adequate naleving op gebruikersbeheerprocedures bestaat het risico dat personen teveel of onterechte rollen/rechten bezitten en hierdoor de functiescheidingsprincipes mogelijk doorbroken kunnen worden met het risico op ongeautoriseerde handelingen. Tevens bestaat het risico dat een medewerker na uitdiensttreding toegang behoudt tot de betreffende applicaties en hierin transacties kan uitvoeren. Het intrekken van toegangsrechten per applicaties heeft als risico dat dit niet tijdig voor elke applicatie wordt gedaan.</p>	
Onze aanbeveling	<p>De periodieke reviews worden voor de relevante applicaties niet tot ongedocumenteerd uitgevoerd. Hierbij verdient het de aanbeveling de controle op juistheid van autorisaties en actualiteit tenminste jaarlijks te documenteren. Als onderdeel van deze controle wordt aangeraden structureel controle-elementen op te nemen in de beoordeling ten behoeven van de navolgbaarheid van de werkzaamheden. Denk hierbij aan:</p> <ol style="list-style-type: none"> <li>1. Doeleinden (juistheid en actualiteit);</li> <li>2. Vastlegging van werkzaamheden en bevindingen;</li> <li>3. Duidelijk inzicht in welke middelen zijn gebruikt voor de controle (bijv. normpositie en lijst van actuele dienstverbanden);</li> <li>4. Eventuele opvolging bij bevindingen;</li> <li>5. Akkoord door een geautoriseerde.</li> </ol>	
Reactie management		



Bevinding	<b>Superusers</b>	RISICO: gemiddeld
Jaar van constatering	2023	IMPACT: gemiddeld
Onze bevinding	<p><b>Coda &amp; Xworks</b>                  Wij hebben vastgesteld dat in de genoemde applicaties eindgebruikers beschikken over rollen/rechten om autorisaties toe te kennen (superuser-rechten):</p> <p>In Coda is 1 eindgebruikers die beschikt over superuser-rechten, namelijk:</p> <ul style="list-style-type: none"> <li>▶ 1 Financieel medewerkers (die gebruikers kunnen verwijderen en autorisaties toe kunnen kennen, maar geen gebruikers aan kunnen maken)</li> </ul> <p>In Xworks zijn 3 eindgebruikers die beschikken over superuser-rechten, namelijk:</p> <ul style="list-style-type: none"> <li>▶ 2 Kwaliteitsmedewerkers</li> <li>▶ 1 WMO backoffice consulent</li> </ul>	
Risico	<p>Accounts met beheerrechten bezitten alle rechten en kunnen hiermee gewenste functiescheidingen doorbreken en eventueel ongeautoriseerde wijzigingen (bijvoorbeeld stamgegevens of financiële transacties) doorvoeren. Dit is een inherent risico van beheeraccounts. Echter wordt dit risico aanzienlijk verhoogd door deze accounts te beleggen in de lijnorganisatie. Tevens bestaat het risico op generiek en/of verouderde genaamde accounts dat met deze accounts ongeautoriseerde wijzigingen worden doorgevoerd, waarnaar op basis van naamgeving niet te achterhalen is wie deze wijzigingen heeft doorgevoerd.</p>	
Onze aanbeveling	<p>Het verdient de aanbeveling om een duidelijke functiescheiding aan te brengen tussen het gebruik en het (IT-)beheer. Dit bijvoorbeeld door de kritische applicatiebeheer processen (zoals o.a. het aanmaken, verwijderen, wijzigen van gebruikers en rechten, het wijzigen van systeeminstellingen zoals wachtwoordinstellingen, logininstellingen, het installeren van updates) te centraliseren bij de IT-organisatie</p>	
Reactie management		

# C. Indicatie omvang Sisa- verantwoording 2023

## C. Indicatie omvang SiSa-verantwoording 2023

NR.	SPECIFIEKE UITKERING OF OVERIG	2022	2023*
A16	Bekostigingsregeling opvang ontheemden Oekraïne	Ja	Ja
B2	Regeling specifieke uitkering gemeentelijke hulp aan gedupeerden kinderopvangtoeslagproblematiek 2021	Ja	Ja
C209	Meerjarige regeling specifieke uitkeringen voor huisvesting aandachtsgroepen (RHA 2022)	Ja	Ja
C31	Regeling vaststelling regels verstrekken eenmalige specifieke uitkering aan gemeenten huisvesting kwetsbare doelgroepen	Ja	Ja
C55	Aanpak energiearmoede	Ja	Ja
C56	Regeling specifieke uitkeringen voor huisvesting aandachtsgroepen (RHA 2021)	Ja	Ja
C62	Regeling specifieke uitkering kwijtschelding gemeentelijke belastingen	Ja	Ja
D92	Regeling specifieke uitkering Informatiepunten Digitale Overheid	Nee	Ja
D8	Specifieke uitkering Onderwijsachterstandenbeleid	Ja	Ja
D14	Middelen inhalen COVID-19 gerelateerde onderwijsvertragingen	Ja	Ja
D19	Specifieke uitkering tijdelijke onderwijs huisvesting Oekraïne	Ja	Ja
E20	Regeling stimulering verkeersveiligheidsmaatregelen	Ja	Ja
F11	Regeling specifieke uitkering MKB-deals	Ja	Ja
F28	Tijdelijke regeling capaciteit decentrale overheden voor klimaat-.en energiebeleid (CDOKE)	Nee	Ja
G2	Gebundelde uitkering op grond van artikel 69 Participatiewet	Ja	Ja
G3	Besluit bijstandsverlening zelfstandigen 2004	Ja	Ja
G4	Tijdelijke overbruggingsregeling zelfstandig ondernemers	Ja	Ja
G10	Wet inburgering 2021	Ja	Ja
G12	Kwijtschelden publieke schulden SZW domein hersteloperatie kinderopvangtoeslagenaffaire	Ja	Ja
G13	Onderwijsroute	Ja	Ja
H4	Regeling specifieke uitkering stimulering sport	Ja	Ja
H8	Regeling sportakkoord 2020-2022	Ja	Ja
H12	Specifieke uitkering lokale preventieakkoorden of preventieaanpakken	Ja	Ja
H25	Regeling Specifieke uitkering IJsbanen en zwembaden	Ja	Ja
H30	Specifieke uitkering sport en bewegen, gezondheidsbevordering, cultuurparticipatie en de sociale basis 2023-2026	Nee	Ja
H31	Specifieke uitkering noodfonds energie amateursportverenigingen (SPUK NEAS)	Nee	Ja
H32	Specifieke uitkering Meerkosten Energie Openbare Zwembaden	Nee	Ja

\*) Verwachting d.d. 24-11-2023 op basis van Concept verantwoordingsoverzicht SiSa 2023, bron: <https://teverantwoordenregelingen.rijksoverheid.nl>. Waarschijnlijk volgen nog enkele aanvullende beschikkingen die op dit moment nog niet bekend zijn.

bdo.nl