

MANAGEMENT LETTER 2023

Gemeente Tynaarlo

Aanbiedingsbrief

Aan:

het college van B&W en het auditcomité van
Gemeente Tynaarlo
Postbus 5
9480 AA VRIES

Groningen, 11 maart 2024

Kenmerk: EJJ/JW/AMT/1044604/001

Ter informatie

De digitale versie van dit document is vanaf de inhouds-opgave 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 Tynaarlo 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 management letter is een samenvatting opgenomen van onze bevindingen naar aanleiding van de uitgevoerde interim-controle bij de gemeente Tynaarlo. Daarbij wordt ingegaan op de beheersing van een aantal financiële processen die zijn onderzocht in het kader van de controle van de jaarrekening en daarmee samenhangende IT-systemen. 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.

Met vriendelijke groet,

BDO Audit & Assurance B.V.
namens deze,

E.J. Jongsma RA
Partner en extern accountant gemeente Tynaarlo

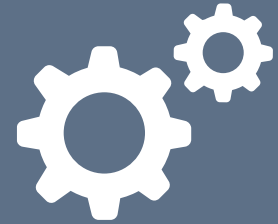
Inhoudsopgave



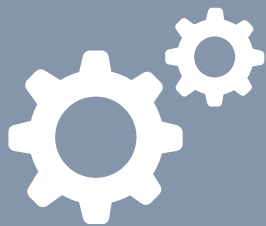
1. DASHBOARD INTERIM-CONTROLE



2. ONTWIKKELINGEN & AANDACHTSPUNTEN



3. BEVINDINGEN SIGNIFICANTE PROCESSEN



4. IT-BEHEERSING



BIJLAGEN

1. Dashboard interim-controlle

1.1 Dashboard interim-controlle

1.1 Toelichting dashboard interim-controle

Ons beeld bij de gemeente Tynaarlo over 2023

Belangrijkste aanbevelingen in deze management letter

We zien bij de gemeente Tynaarlo, net zoals bij veel andere gemeenten, dat er steeds meer taken bij de gemeente worden belegd. Maar ook dat er slechts in beperkte mate sprake is van structureel door het Rijk beschikbaar gestelde middelen. De gemeente Tynaarlo verwacht (zo blijkt uit de meerjarenbegroting 2024) ook tekorten. Hierdoor ontstaat een onbalans tussen taken en middelen: de taken en opgaven nemen toe, terwijl de structurele middelen juist afnemen. Dit bedreigt de slagkracht van gemeenten.

We stellen in deze management letter vast dat eerder gerapporteerde aandachtsgebieden op het gebied van bedrijfsvoering en (financiële) werkprocessen voor een belangrijk deel op hetzelfde niveau zijn gebleven in 2023. De belangrijkste aanbevelingen (op basis van een inschatting van kans x impact) zien toe op naleving van Europese aanbestedingsregels en rechtmatigheid van verstrekkingen op grond van de Jeugdwet en WMO. Van belang is om te vermelden dat er tot nu toe, op basis van de werkzaamheden van de VIC, geen nieuwe onrechtmatigheden of onduidelijkheden zijn geconstateerd ten opzichte van voorgaand jaar. Op IT-gebied geldt dat nog stappen gezet kunnen worden op het gebied van autorisatiebeheer en het beperken van administrator en supersuser accounts.

Gezien de omvang van de organisatie en de (personele) uitdagingen begrijpen wij dat het niet altijd realistisch is om de (eerstelijns) processen voldoende preventieve IB-maatregelen te treffen. In dat geval kan er bijvoorbeeld voor gekozen worden om achteraf (repressief) meer controles uit te voeren om vast te stellen dat rechtmatig is gehandeld. Daar waar realistisch kunnen bepaalde (rest)risico's ook weloverwogen worden geaccepteerd.

Wij adviseren daarin een afgewogen keuze te maken ten aanzien van ambitie en mogelijkheden en hiervoor een plan van aanpak op te stellen en deze met het MT, het college én de audit-commissie af stemmen. Ons advies is om daarbij ook rekening te houden met het volwassenheidsniveau van de verschillende domeinen en afdelingen. Bij afdelingen waarbij de procesgang goed is ingeregeld en waarbij sprake is van weinig verloop zijn achteraf minder controles nodig. Daarentegen kan het bij afdelingen waarbij de procesgang minder goed voor elkaar is en een hoger verloop is nodig zijn om meer controles achteraf uit te voeren.

De belangrijkste bevindingen en aanbevelingen in deze management letter zien verder toe op de volgende zaken:

- ▶ Het verder formaliseren, aanscherpen én periodiek op de agenda van onder andere het MT en het college houden van de in 2023 opgestelde frauderisicoanalyse.
- ▶ Het verder focussen en door ontwikkelen van de I-Visie met bijbehorende ontwikkelingen in strategische plannen en jaarplannen.
- ▶ De invoering van de rechtmatigheidsverantwoording is nieuw voor 2023 en onderhanden bij de organisatie. Op dit moment worden bij de gemeente Tynaarlo geen issues verwacht in het verantwoordingsproces. Wel geldt dat het wetgevingstraject nog niet definitief is afgewikkeld.
- ▶ Positief vinden wij dat de gemeente Tynaarlo de afgelopen periode druk bezig is geweest met het vernieuwen en doordachter inrichten van de P&C-cyclus, teneinde beter en tijdiger te kunnen (bij)sturen.
- ▶ Het belang van specifieke uitkeringen en de verantwoording daaromtrent (SiSa) neemt toe. Bij de gemeente Tynaarlo was in 2020 nog sprake van 11 te verantwoorden regelingen en over 2023 zijn dit totaal 30 regelingen. Vanwege dit toenemende belang wordt het ook belangrijker om als organisatie een proces in te regelen omtrent de beheersing hiervan. Dit is nu 'aan de voorkant' veelal nog niet structureel en zichtbaar geregeld en hierin kan de organisatie nog stappen zetten.

1.1 Dashboard interim-controle

UW INTERNE BEHEERSING		IT-BEHEER		ONZE BEVINDINGEN (HOOFDSTUK 3.3.)	
▶ In voorgaande jaren hebben wij uitgebreid en gedetailleerd gerapporteerd over de effectiviteit van de voor onze controle relevante bedrijfsprocessen. Gezien de omvang van de organisatie en de vele uitdagingen snappen wij dat het voor Tynaarlo niet altijd realistisch is om in processen voldoende IB-maatregelen te treffen. Wij adviseren daarom een afgewogen keuze te maken ten aanzien van ambitie en mogelijkheden en hiervoor een plan van aanpak op te stellen. ▶ De (interim) Vakmanager Financiën heeft aangegeven dat hiervoor een plan van aanpak zal worden opgesteld. In dit plan zal de prioritering van de bevindingen, de bijbehorende risico's en de te plannen acties worden opgenomen.		▶ De automatiseringsomgeving is van groot belang voor de kwaliteit van de interne beheersing. De basis van de zogenaamde IT General Controls (ITGC's) dient op orde te zijn. Daarom vormt dit een belangrijk onderdeel van onze werkzaamheden. ▶ In het verleden hebben wij vastgesteld dat voornamelijk het autorisatiebeheer en accounts met beheerrechten risico's vormen. ▶ Tijdens onze IT-controle hebben wij vastgesteld dat er sprake is van enkele verbeteringen met betrekking tot IT-beheer. ▶ Om de belangrijkste risico's van informatie-beveiliging te mitigeren en door te groeien naar een adequaat volwassenheidsniveau kunnen nog diverse stappen gezet worden. In hoofdstuk 4 zijn daarvoor een aantal aanbevelingen opgenomen.			
ONTWIKKELINGEN		VERBIJZONDERDE INTERNE CONTROLE (VIC)		OVERZICHT VAN ONZE BEVINDINGEN (BIJLAGEN)	
▶ In de jaarrekening 2023 zal het college middels een rechtmatigheidsverantwoording voor het eerst zelfstandig verantwoording aan de gemeenteraad afleggen over de financiële rechtmatigheid. De gemeente kiest hierbij voor de minimale variant. ▶ Er is de afgelopen jaren sprake van een significante stijging van SiSa-regelingen waarover via de jaarrekening expliciet verantwoording dient te worden afgelegd. ▶ Wij zullen in de controleverklaring 2023 weer rapporteren over onze werkzaamheden rondom fraude en continuïteit. Wij gaan hierover in overleg met de gemeente over de aanwezige beheersmaatregelen rondom frauderisico's. Wij hebben hiervoor via uw VIC-functionaris een concept risicoanalyse ontvangen welke nog verder dient te worden geformaliseerd.		▶ De gemeente heeft in 2023 een concept interne controleplan opgesteld en daarnaast over de uitkomsten van de verrichte werkzaamheden tot en met Q3 (in concept) gerapporteerd. ▶ De kwaliteit van de verrichte werkzaamheden is momenteel van een dusdanig niveau dat vanuit het (concept) interne controleplan er voldoende aanknopingspunten zijn voor een degelijke onderbouwing van de rechtmatigheids-verantwoording. ▶ Over de aard en timing van de gegevensgerichte werkzaamheden ten aanzien van de jaarrekeningcontrole maken wij nog definitieve afspraken met de VIC. Hierbij is het van essentieel belang dat de wijze van selectie reproduceerbaar is en dat de betrouwbaarheid van de gehanteerde brondata kan worden vastgesteld.		▶ Hierboven is een grafische weergave opgenomen van onze visie op de mate van risico en impact van de in het verleden geconstateerde bevindingen welke tevens in 2023 nog van toepassing zijn. ▶ Voor een overzicht van de reeds geconstateerde bevindingen verwijzen wij naar hoofdstuk 3 en naar bijlage A. ▶ Graag bespreken wij welke bevindingen op korte termijn prioriteit krijgen en welke (proces) bevindingen op korte termijn zullen worden geaccepteerd. ▶ In het vervolg zullen wij alleen nog rapporteren over significante bevindingen en/of bevindingen waarbij de gemeente van oordeel is dat deze prioriteit hebben en opvolging benodigd is.	
DASHBOARD	ONTWIKKELINGEN	BEVINDINGEN	IT-BEHEER	BIJLAGEN	

2. Ontwikkelingen & Aandachtspunten

2.1 Relevante ontwikkelingen

2.2 Digitale bestuurskracht

2.1 Relevante ontwikkelingen (1/4)

Geen apart oordeel
rechtmatigheid in
controleverklaring

Meer bewustwording
college
verantwoordelijkheid

Tynaarlo kiest voor de
minimale variant

Wijzigingen in de
nieuwe Kadernota
Rechtmatigheid

Invoering rechtmatigheidsverantwoording met ingang van 2023

Vanaf dit boekjaar geeft het college de rechtmatigheidsverantwoording af voor wat betreft de financiële rechtmatigheid (het begrotingscriterium, voorwaardencriterium en misbruik en oneigenlijk gebruik). 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. De SiSa-bijlage 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. In ieder geval in het accountantsverslag en mogelijk ook nog in de controleverklaring bij de jaarrekening als geheel.

De rechtmatigheidsverantwoording zorgt voor meer bewustwording bij het college 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 gemeenteraad. Deze opzet stimuleert het dualisme waarin de gemeenteraad 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. De voorgeschreven verantwoordingsgrens ligt tussen de 0% en 3% en het college heeft voorgesteld om deze op 3% van de lasten inclusief mutatie reserves vast te stellen, wat inmiddels in de aangepaste financiële verordening is geactualiseerd. Dit is meer dan de wettelijke materialiteit die in het kader van de jaarrekeningcontrole over 2023 (1% van de lasten inclusief mutatie reserves) door ons wordt gehanteerd en tevens is voorgeschreven in het controleprotocol.

Wijzigingen wet- en regelgeving

Bij het schrijven van deze management letter 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 gepubliceerd.
- ▶ De notitie van de commissie BADO 'Notitie rechtmatigheidsverantwoording' is op 6 december 2023 gepubliceerd.

Momenteel worden de aanwezige besluiten, handreikingen en notities nader bestudeerd op basis waarvan een definitief controleplan kan worden opgesteld.

Wijzigingen wet- en regelgeving (vervolg)

Vanaf boekjaar 2023 geldt de nieuwe Kadernota Rechtmatigheid. Onder andere ten aanzien van de foutenevaluatie zijn belangrijke wijzigingen doorgevoerd. In het rechtmatigheidsoordeel worden alle afwijkingen boven de verantwoordingsgrens gerapporteerd. In de nieuwe Kadernota Rechtmatigheid vallen 'afwijkingen' uiteen in fouten en onduidelijkheden. Onduidelijkheden doen zich voor in situaties 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 gegeven aan het onderscheid tussen getrouwheids- en rechtmatigheidsfouten en (mogelijk) herstel van (door de VIC) geconstateerde fouten. Wij verzoeken de gemeente om voorafgaand aan de jaarrekeningcontrole de werkzaamheden te hebben uitgevoerd en een eigen inhoudelijke analyse (inclusief rechtmatigheidsoordeel) aan te leveren.

De accountant maakt zoveel mogelijk gebruik van de uitgevoerde (verbijzonderde) interne controlewerkzaamheden van de gemeente. Wij hebben met de gemeente in het verleden diverse werkprogramma's gedeeld. Deze werkprogramma's borgen dat de gemeente volledig de benodigde stappen doorloopt die nodig zijn voor het kunnen verstrekken van de rechtmatigheidsverantwoording door het college. De werkprogramma's zijn opgebouwd uit de verwachtingen voor de gemeente en de verwachtingen voor de accountant, zodat de juiste werkzaamheden worden gedaan door beiden en wat een korte doorlooptijd van de controle bevordert.

Rechtmatigheidsverantwoording en rol van de Verbijzonderde Interne Controle (VIC)

Voor een efficiënte controle is van belang dat de aard en diepgang van de werkzaamheden van de VIC worden ingericht in lijn met de materialiteitsbepaling van de accountant.

De afgelopen periode heeft de gemeente in concept een intern controleplan opgesteld waarbij per relevant financieel proces een risicoanalyse is uitgevoerd en de aard en omvang van de door de VIC uit te voeren controles is opgenomen. Tevens hebben wij vastgesteld dat de VIC een concept VIC-rapportage over de periode januari tot en met september heeft opgesteld waarin de door de VIC geconstateerde bevindingen zijn opgenomen.

Wij hebben kennis genomen van het concept interne controleplan en de VIC-rapportage en stellen vast dat de gemeente hiermee verdere stappen heeft gezet bij het professionaliseren van de VIC-werkzaamheden en hierbij aansluit bij de vereisten uit het door de gemeenteraad vastgestelde controleprotocol. Wij adviseren u om het interne controleplan verder te concretiseren door tevens aandacht te hebben voor relevante balansmutaties en actuele ontwikkelingen (bijvoorbeeld energietoeslag). Daarnaast is het van belang dat de wijze van selectie reproduceerbaar is en dat de betrouwbaarheid van de gehanteerde brondata kan worden vastgesteld.

Graag gaan wij met u in gesprek of het ambitieniveau welke in uw eigen interne controleplan is opgenomen, een systeemgerichte controle in 2025, realistisch is en op welke wijze BDO de gemeente hierbij kan faciliteren.

2.1 Relevante ontwikkelingen (3/4)

De gemeente voldoet aan de minimale vereisten voor de rechtmatigheidsverantwoording

Status invoering rechtmatigheidsverantwoording

Status rechtmatigheidsverantwoording

De gemeente Tynaarlo heeft de afgelopen periode gewerkt om de benodigde stappen te zetten in aanloop naar de rechtmatigheidsverantwoording. De gemeente Tynaarlo heeft reeds op 13 juli 2023 bij het vaststellen van de Financiële verordening gemeente Tynaarlo 2023 de verantwoordingsgrens vastgesteld op 3%. Daarin is tevens opgenomen dat de gemeente een rapporteringsgrens van € 100.000 hanteert. Wij stellen vast dat de gemeente met deze verantwoordings- en rapportagegrens voldoet aan de minimale vereisten maar wel aan de bovenkant van de benchmark van 0 tot 3% zit.

Naast de geactualiseerde financiële verordening is tevens de controleverordening en het normenkader geactualiseerd en zijn deze inmiddels door de gemeenteraad vastgesteld. Hierin zijn afspraken opgenomen met betrekking tot het toetsingskader en hoe om te gaan met begrotingsonrechtmatigheden.

Hieronder hebben wij de voortgang van de stappen ten aanzien van de rechtmatigheidsverantwoording inzichtelijk gemaakt. Hieruit wordt duidelijk dat de gemeente Tynaarlo diverse stappen heeft gezet, maar dat ook een gedeelte van de documentatie nog nader uitgewerkt en geformaliseerd dient te worden.

TE ZETTEN STAPPEN	AFSPRAKEN COLLEGE GEMAAKT?
De verantwoordingsgrens voor 2023 is bepaald	●
De verantwoordingsgrens voor 2023 is vastgesteld door de raad	●
Het normenkader 2023 is gereed en door de raad vastgesteld	●
De financiële verordening is herzien	●
De financiële verordening bevat op welke wijze wordt omgegaan met begrotingsonrechtmatigheden	●
Het interne controleplan van de gemeente bevat:	
1. scoping van de processen en balansposten	●
2. risicoanalyses per proces en post	●
3. controleaanpak	●

● ja ● onderhanden ● n.v.t.

Verhoogde aandacht voor fraude en non-compliance

Verhoogde aandacht voor fraude en non-compliance

Onze controle is niet specifiek gericht op het ontdekken van fraude. Bij de planning voor de jaarrekeningcontrole, houden wij echter wel rekening met het risico dat de jaarrekening als gevolg van fraude en onregelmatigheden onjuistheden van materieel belang zou kunnen bevatten. Tevens dienen wij vanaf het boekjaar 2022 expliciet te rapporteren over de belangrijkste frauderisico's die door de gemeente en ons zijn geïdentificeerd. Na afloop van de interim-controle hebben wij een eerste aanzet van een door de VIC opgestelde (interne) frauderisicoanalyse/register ontvangen. Wij hebben kennis genomen van deze frauderisicoanalyse en vastgesteld dat deze nog in concept is, maar reeds op domeinniveau een inschatting van de meest relevante frauderisico's bevat die op basis van de mogelijke kans en impact zijn ingeschaald. Vanuit deze analyse blijken geen risico's met zowel een verhoogde kans als impact. Wij adviseren u om deze frauderisicoanalyse breder binnen de organisatie te bespreken en daarna te formaliseren.

Sterke toename aantal SiSa-regelingen

Toename inkomende gelden SiSa-regelingen

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 uw gemeente, is daardoor exponentieel toegenomen. De SiSa-regelingen gaan gepaard met aanvullende administratieve vereisten en een uitgebreide instructie (invalwijzer van 439 pagina's). Dit geeft een hoge druk op de organisatie binnen de gemeente en leidt tot een extra piek in de controle van de jaarrekening.

Beheersing 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 Tynaarlo, is daardoor sterk toegenomen. Dit geeft een hoge druk op uw organisatie en in de breedte bij gemeenten en provincies en de betrokken accountantskantoren. Jaarlijks publiceert het Ministerie per decentrale overheid een overzicht van de van toepassing zijnde SiSa-regelingen. Tevens geven Ministeries in de beschikkingen, waarmee de subsidie wordt verstrekt, aan dat verantwoording via SiSa plaats dient te vinden. Bij de gemeente Tynaarlo was in 2020 nog sprake van 11 te verantwoorden regelingen (waarvan 4 met een zogenaamde 0-verantwoording) waarbij dit naar verwachting voor 2023 30 regelingen (inclusief 0-verantwoordingen) betreffen.

Gezien de grote hoeveelheid is het van belang om als organisatie een proces in te regelen omtrent de beheersing van specifieke uitkeringen en de verantwoording daarover. Hierbij zijn onder andere de volgende aandachtspunten van belang:

- ▶ Is het eigenaarschap voor het totaaloverzicht aan specifieke uitkeringen binnen de organisatie belegd?
- ▶ Is de projectleider zich voldoende bewust van de (financiële) verantwoordingsplicht via de SiSa?
- ▶ Wordt een specifiek grootboek/kostenplaats aangemaakt voor het betreffende project, zodat alle gemaakte kosten/uren juist en volledig in de administratie worden geregistreerd?
- ▶ Hoe waarborgt de organisatie dat geschreven projecturen ook daadwerkelijk aan het project zijn besteed?
- ▶ Heeft de organisatie een proces omtrent review/beoordeling ingeregeld aan de hand waarvan wordt vastgesteld dat kosten/uren ook subsidiabel zijn kijkend naar de geldende wet- en regelgeving (waaronder de beschikking) en daarom ook in de SiSa-bijlage verantwoord mogen worden?

Digitale Bestuurskracht gemeente Tynaarlo

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. Dit 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 Tynaarlo

Op basis van de hierboven benoemde werkzaamheden valt het ons op dat gemeente Tynaarlo drukdoende is met het onderwerp Informatievoorziening (IV). Gedurende 2023 is een I-Visie opgesteld welke eind 2023 is geformaliseerd. De vervolgstap is het concretiseren van de I-Visie met bijbehorende ontwikkelingen in strategische plannen en jaarplannen. Wij hebben begrepen dat momenteel uitvoering wordt gegeven aan deze actie en onderschrijven de inspanning om de I-Visie op korte termijn door te vertalen.

Data management

Een wendbare organisatie is alleen mogelijk met de vierde bouwsteen; de basis van processen en data op orde hebben. Dit gaat verder dan het beschrijven van processen en het inrichten van werkprocessen in systemen. Het gaat er hierbij om dat organisaties het eigenaarschap van processen hebben ingericht en actief gebruikmaken van data om tot stuurinformatie te komen. Stuurinformatie voor de beleidsontwikkeling, die toegankelijk en begrijpelijk is voor medewerkers, bestuurders en raadsleden. Data-gedreven werken en data-gestuurde beleidsontwikkeling betekenen een verandering van werken in de organisatie. Wij merken op dat de gemeente Tynaarlo nog geen data-strategie heeft beschreven. Momenteel wordt IT nog primair gebruikt voor registrerende doeleinden. Wel heeft de gemeente een data-specialist aangenomen om te focussen op data-gedreven werken. De échte stap naar data-gedreven werken, ofwel: het werken met voorspellende data die ter input dient voor de verschillende beleidskaders, moet nog gezet worden. Wij vragen hier aandacht voor, temeer omdat dit in de toekomst steeds belangrijker gaat worden.

Financiële randvoorwaarden

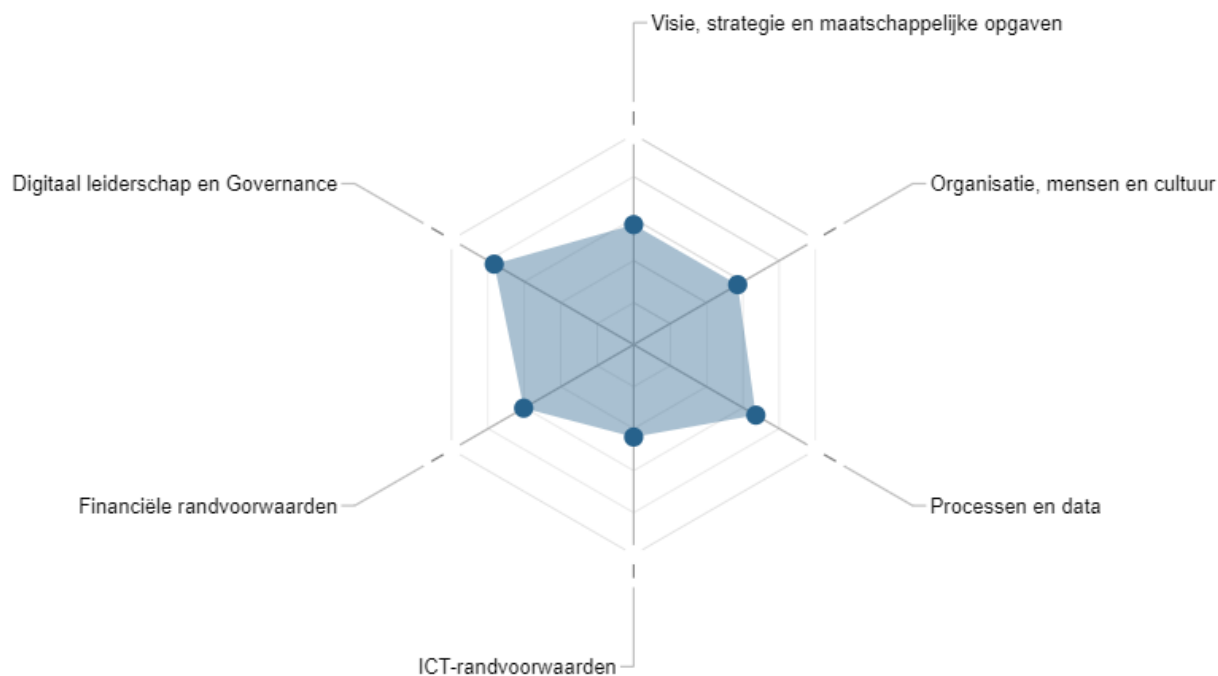
De bouwsteen financiële randvoorwaarden richt zich op benodigde investeringen. De kosten voor informatievoorziening zullen de komende jaren alleen maar toenemen, dat is naar onze mening een onomkeerbaar proces. De uitdaging is de toenemende uitgaven zodanig in te zetten dat gemeenten de voordelen van 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 Tynaarlo de huidige investeringen momenteel afdoende zijn om de informatievoorzieningsprojecten te bekostigen. Wel verwachten wij zoals genoemd een toename van de benodigde investeringen, gelet op de razendsnelle ontwikkelingen in de markt. Daarom adviseren wij om zoveel als mogelijk de komende jaren rekening te houden met deze verwachte toename van investeringen.

2.2 Digitale Bestuurskracht (2/2)

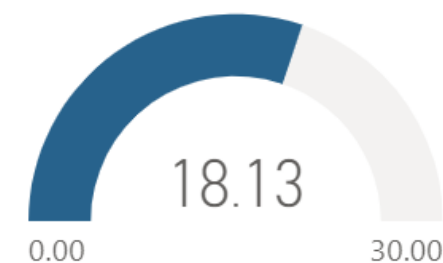
Resultaten Basisscan
Digitale Bestuurskracht
gemeente Tynaarlo

Verdeling punten over bouwstenen

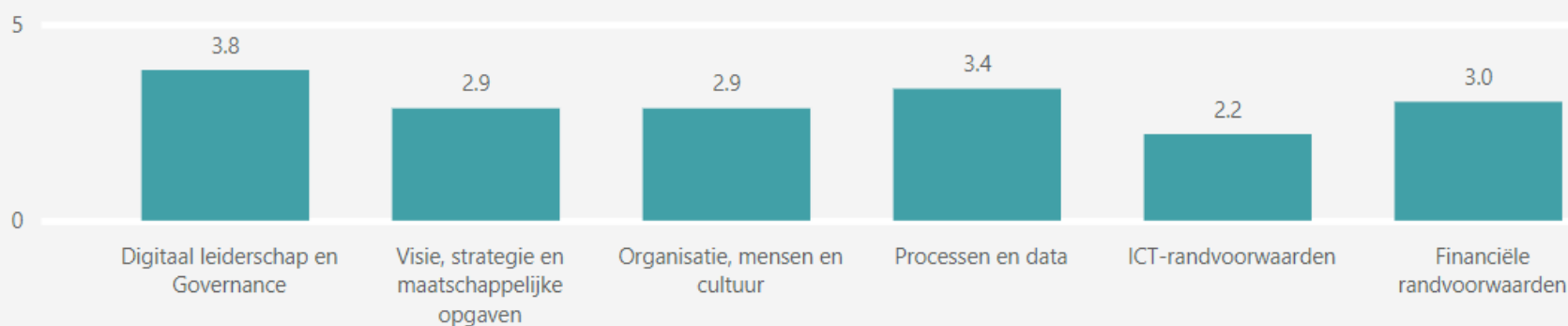
● Punten per bouwsteen



Totaal aantal punten



Punten per bouwsteen



3. Bevindingen significante processen

- 3.1 Onze controle nog transparanter
- 3.2 Effectiviteit processen
- 3.3 Overzicht van de bevindingen

3.1 Onze controle nog transparanter

- Belangrijkste onderkende risico's:
- ▶ Oneigenlijke beïnvloeding cijfers door het management
 - ▶ Onjuist oordeel rechtmatigheidsverantwoording
 - ▶ Waardering voorraad gronden

Wij beoordelen de volgende processen

Inleiding

Zoals afgelopen jaren 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 Tynaarlo. In deze management letter hebben wij daarom in lijn met voorgaande jaren 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.

Onze inschatting van de risico's en belangrijkste processen

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 potentiële risico's in de controle van de jaarrekening van de gemeente Tynaarlo:

- ▶ 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. 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, uitermate beperkt zijn. Om het resterende risico te beperken beoordelen wij schattingsprocessen en bijzondere journaalposten in detail.
- ▶ Een onjuist oordeel in de rechtmatigheidsverantwoording.
- ▶ Onjuiste waardering bouwgronden in exploitatie (materiële post met verschillende schattingselementen met verhoogde aandacht voor het woningbouwcomplex Ter Borch en Businesspark Ter Borch).

In onze aanpak is in principe de insteek, daar waar mogelijk te steunen op de interne beheersing in de significante processen van de gemeente Tynaarlo. Dit noemen wij een zogenaamde systeemgerichte aanpak, waarbij wij kunnen steunen op toereikende maatregelen in uw processen en systemen. Het voordeel hiervan is dat ook uw risico's beperkt worden en de organisatie zich kan verbeteren. Daarbij maken wij, indien mogelijk, gebruik van uw eigen verbijzonderde interne controle (VIC). Omdat de gemeente Tynaarlo heeft aangegeven een (groot) aantal niet te kunnen opvolgen, zal de controle voornamelijk gegevensgericht zijn.

In het kader van onze controle hebben wij de volgende processen beoordeeld:

- | | |
|---|---|
| ▶ het planning-en-control proces | ▶ het proces grondexploitatie |
| ▶ het inkoopproces (incl. aanbestedingen) | ▶ het proces Jeugd |
| ▶ het personeelsproces | ▶ het proces WMO |
| ▶ het proces omgevingsvergunningen | ▶ het proces omtrent verbonden partijen |
| ▶ het subsidieproces | ▶ het proces omtrent IT/automatisering |

Natuurlijk zijn er meerdere processen te onderkennen, ook met een financiële gevolgen. De uitkomsten hiervan zijn in het kader van onze risicoanalyse echter niet in deze management letter opgenomen.

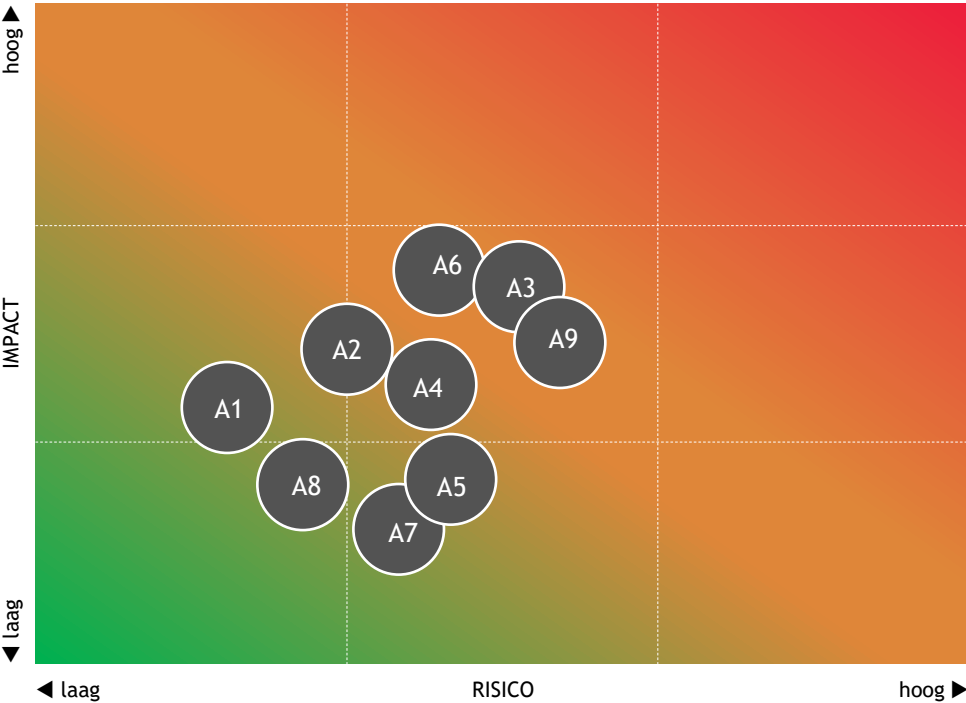
3.2 Effectiviteit processen

In het volgende overzicht geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook hoofdstuk 4 t.a.v. IT). Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat de beheersorganisatie van de gemeente (voor zover relevant voor de controle van de jaarrekening) in opzet voldoende tot goed scoort, rekening houdend met de uitkomsten van de werkzaamheden van de VIC. Voor een aantal processen geldt daarbij wel dat één of meerdere beheersmaatregelen niet of onvoldoende zichtbaar zijn. Daarom kunnen wij voor wat betreft de insteek van onze controle nog niet altijd op de processen steunen.

PROCES	OPZET AO/IB	WERKING AO/IB	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Planning & Control	●	Onderhanden	n.v.t.	Er is sprake van een adequaat functionerende planning & control-cyclus. De zichtbaarheid van controles in de P&C-cyclus kan wel verbeterd worden. Daarnaast adviseren wij de concept frauderisicoanalyse breder in de organisatie te bespreken en te formaliseren.
Inkopen	●	Onderhanden	●	Proces omtrent inkopen is adequaat. Borging van de prestatielevering blijft een aandachtspunt.
Aanbestedingen	●	n.v.t.	n.v.t.	De naleving van de aanbestedingsregels ten aanzien van verlengen en uitbreiden van contracten wordt in het proces niet geborgd.
Personeel	●	n.v.t.	●	Het proces personeelskosten is adequaat.
Omgevingsvergunningen	●	n.v.t.	●	De volledigheid van de gefactureerde omgevingsvergunningen wordt in het proces niet geborgd.
Subsidiebeheer	●	n.v.t.	●	Er is geen sluitend subsidieregister.
Grondexploitaties	●	Onderhanden	●	Het proces grondexploitaties is in opzet adequaat. Gezien er sprake is van een gegevensgerichte controle zal bij de eindejaarscontrole de aanvaarbaarheid van de gehanteerde schattingen worden vastgesteld.
Jeugd	●	n.v.t.	●	Een zichtbare controle op het woonplaatsbeginsel, de crediteurenstamgegevens en op de prestatielevering zijn belangrijke aandachtspunten.
WMO	●	n.v.t.	●	Een zichtbare controle op de crediteurenstamgegevens en op de prestatielevering zijn belangrijke aandachtspunten. Tevens is het van belang dat er sprake is van een zichtbare aansluiting tussen de FA en de uitkeringsadministratie. Dit wordt nu slechts 1x per jaar bij de jaarrekening gedaan.
Verbonden partijen en uitbesteden diensten	●	n.v.t.	n.v.t.	De processen belastingopbrengsten, facturatie (o.a. verhuur) en uitvoering Participatiewet zijn uitbesteed. Wij zullen een review uitvoeren op de werkzaamheden van de accountant van de Belasting samenwerking Drentsche Aa en Werkplein Drentsche Aa.

● proces is ontoereikend
 ● proces is toereikend, maar één of meerdere beheersmaatregelen bestaan in de praktijk niet
 ● proces is adequaat/beheersmaatregelen bestaan

3.3 Overzicht van de bevindingen



Hierboven is een grafische weergave opgenomen van onze visie op de mate van risico en impact van de geconstateerde bevindingen in relatie tot de maatregelen van interne beheersing in de relevante processen. In de bijlagen hebben wij de bevindingen nader toegelicht waarin wij ingaan op de bevinding, het risico voor de gemeente Tynaarlo, mogelijke oplossingen ter adressering van de bevindingen en de eventuele gevolgen voor onze accountantscontrole.

Voor de bevindingen die belangrijk zijn én een hoge impact hebben adviseren wij u deze zo spoedig mogelijk te adresseren. Daarnaast adviseren wij u om per detailbevinding een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd.

OVERZICHT DETAILBEVINDINGEN	
A	Detailbevindingen processen
A1	Planning & control: De zichtbaarheid van controles in de P&C-cyclus kan verbeterd worden.
A2	Planning & control: Een actuele frauderisicoanalyse ontbreekt.
A3	Inkopen: controle prestatielevering en juiste verwerking factuur (Btw, kosten of investering) niet altijd gewaarborgd.
A4	Subsidieverstrekkings: Geen sluitend subsidieregister aanwezig.
A5	Omgevingsvergunningen: Volledigheid opgelegde facturen niet geborgd.
A6	Jeugdwet/WMO: Controle op prestatielevering niet altijd aanwezig.
A7	Jeugdwet/WMO: Controle op crediteurenstamgegevens betaalbestand niet consequent uitgevoerd.
A8	Jeugdwet: Controle op woonplaatsbeginsel niet zichtbaar.
A9	Aanbestedingen: Naleven aanbestedingsregels niet geborgd.

4. IT-beheersing

- 4.1 [IT-beheersing](#)
- 4.2 [Bevindingen IT-beheersing | Civision Middelen](#)
- 4.3 [Bevindingen IT-beheersing | Mozard](#)
- 4.4 [Bevindingen IT-beheersing | Spend Cloud](#)
- 4.5 [Bevindingen IT-beheersing | Youforce](#)
- 4.6 [Actuele IT-ontwikkelingen en onze natuurlijke adviesrol](#)
- 4.7 [Informatiebeveiliging en cybersecurity](#)

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

Beoordeelde systemen:

- Civision Middelen
- Mozard
- Spend Cloud
- Youforce

Detailbevindingen
IT weergegeven in
Bijlage B

IT-werkzaamheden en onze controlerende rol

Ingevolge artikel 2:393, lid 4 BW, dient de accountant in zijn verslag aandacht te besteden aan de bevindingen die naar voren zijn gekomen uit de beoordeling van de automatiseringsomgeving wat betreft de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Wij benadrukken dat onze jaarrekeningcontrole gericht is op het geven van een oordeel omtrent de jaarrekening zelf en zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan. De IT-auditwerkzaamheden zijn geïntegreerd in de controleaanpak van de jaarrekening.

Het inzicht in de betrouwbare werking van IT-systemen en applicaties en het gebruik daarvan door de organisatie, vormen een onderdeel van de kwaliteit van de interne beheersing en de administratieve organisatie. Algemene IT-beheersmaatregelen rond uw kritieke systemen leveren daarnaast een belangrijke bijdrage aan het mitigeren van de risico's op ongeautoriseerde handelingen en het optreden van verstoringen met 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. Wij hebben in samenwerking met onze IT-auditors een aantal van deze maatregelen beoordeeld voor het financiële systeem Civision Middelen, het systeem voor sociaal domein Mozard, het systeem voor goedkeuringen op facturen Spend Cloud en het systeem voor de salarisadministratie Youforce.

De IT-audit is uitgevoerd om de impact van de risico's van ongeautoriseerde handelingen en verstoringen te kunnen vaststellen voor die systemen die gekoppeld zijn aan de voor ons relevante processen en posten (zie hoofdstuk 3). Aangezien in het huidige boekjaar geen verstoringen met dataverlies hebben plaatsgevonden, is het risico op het niet voldoen aan continuïteitsmaatregelen beperkt. Wij hebben derhalve deze maatregelen niet opnieuw beoordeeld.

In dit hoofdstuk geven wij een samenvatting van onze bevindingen voor de genoemde applicaties. De detailbevindingen rondom deze systemen zijn opgenomen in Bijlage B.

Op dit moment zijn de intern getroffen algemene IT-beheersmaatregelen rondom de applicaties in scope niet (bewijsbaar) voldoende aanwezig, waardoor in het kader van de controle van de jaarrekening 2023 aanvullende (gegevensgerichte) werkzaamheden noodzakelijk zijn om aan te tonen dat er zich geen risico's of fouten hebben voorgedaan.

Logische toegangs-beveiliging (criteria 1-5) grotendeels toereikend

Change management (criteria 6) niet beoordeeld

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

PROCES	2022	2023
1. Procedure autorisatiebeheer	verbeterpunten	voldoende
2. Periodieke controle op juistheid ingerichte autorisaties	voldoende	voldoende
3. Identificatie van gebruikers voor toegang tot systemen en data	voldoende	voldoende
4. Wachtwoordbeleid (authenticatie)	voldoende	voldoende
5. Administrators en superusers	verbeterpunten	verbeterpunten
6. Wijzigingenbeheer & Gescheiden omgevingen	Niet beoordeeld	Niet beoordeeld

KORTE OMSCHRIJVING RESULTATEN	
1	Een verbetering is doorgevoerd aan het autorisatiebeheer proces door gebruik te maken van een geformaliseerde autorisatiematrix voor het toekennen en wijzigen van autorisaties.
2	Voor Civision Middelen is een zichtbare review uitgevoerd op de actualiteit van gebruikers en de juistheid van toegewezen autorisaties.
3	Alle aanwezige generieke accounts zijn verklaarbaar.
4	De wachtwoordeisen in Civision Middelen voldoen aan de minimale eisen van BDO.
5	In Civision Middelen zijn gebruikers met beheerrechten actief die formeel werkzaam zijn vanuit de lijnorganisatie. Het aantal accounts is echter wel beperkt tot het noodzakelijk minimum.
6	Leverancier van de applicatie, PinkRoccade, verstrekt jaarlijks een ISAE3402 type II rapport na afloop van het boekjaar, inzake de getroffen beheersmaatregelen omtrent wijzigingsbeheer. Gemeente Tynaarlo heeft nog geen proces ingevuld om deze assurance-rapportages jaarlijks te beoordelen.

Legend: onvoldoende verbeterpunten voldoende Niet beoordeeld

Logische toegangs-
beveiliging (criteria 1-
5) nog
deels ontoereikend

Change management
(criteria 6) niet
beoordeeld

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

PROCES	2022	2023
1. Procedure autorisatiebeheer		
2. Periodieke controle op juistheid ingerichte autorisaties		
3. Identificatie van gebruikers voor toegang tot systemen en data		
4. Wachtwoordbeleid (authenticatie)		
5. Administrators en superusers		
6. Wijzigingenbeheer & Gescheiden omgevingen		

KORTE OMSCHRIJVING RESULTATEN	
1	De organisatie beschikt over een verouderde procedure autorisatiebeheer. Daarnaast beschikt de organisatie over een (concept) autorisatiematrix, echter is deze nog niet formeel bekrachtigd. Bovendien worden rechten toegekend op basis van voorbeeldgebruikers.
2	Een periodieke review op de actualiteit van gebruikers is uitgevoerd, echter zijn de ingerichte autorisaties per gebruiker niet zichtbaar beoordeeld.
3	Alle aanwezige generieke accounts zijn verklaarbaar.
4	Enkele eindgebruikers hebben een wachtwoord dat niet verloopt op Windows AD. Echter is vastgesteld dat zij geen toegang hebben tot Mozard.
5	De gebruikers met beheerrechten zijn op basis van functie verklaarbaar.
6	Mozard betreft een standaard-applicatie; updates worden ontwikkeld en aangeleverd door de leverancier. Begrepen dat maandelijks updates doorgevoerd worden door de leverancier. Vanwege het feit dat Mozard geen maatwerk applicatie betreft, is deze beheersmaatregel niet in bestaan beoordeeld.

onvoldoende
 verbeterpunten
 voldoende
 Niet beoordeeld

4.4 Bevindingen IT-beheersing | Spend Cloud

Logische toegangs-
beveiliging (criteria 1-
5) nog
deels ontoereikend

Change management
(criteria 6) nog niet
beoordeeld

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

PROCES	2022	2023
1. Procedure autorisatiebeheer		
2. Periodieke controle op juistheid ingerichte autorisaties		
3. Identificatie van gebruikers voor toegang tot systemen en data		
4. Wachtwoordbeleid (authenticatie)		
5. Administrators en superusers		
6. Wijzigingenbeheer & Gescheiden omgevingen		

KORTE OMSCHRIJVING RESULTATEN	
1	De organisatie beschikt over een verouderde procedure autorisatiebeheer. Daarnaast beschikt de organisatie over een (concept) autorisatiematrix, echter is deze nog niet formeel bekrachtigd. Uitdiensttreding wordt niet structureel tijdig gemeld bij de functioneel beheerders.
2	Voor Spend Cloud is een zichtbare review uitgevoerd op de actualiteit van gebruikers en de juistheid van toegewezen autorisaties.
3	Er bestaan geen generieke accounts in Spend Cloud.
4	Enkele eindgebruikers hebben een wachtwoord dat niet verloopt op Windows AD. Echter is vastgesteld dat zij geen toegang hebben tot Spend Cloud.
5	In Spend Cloud zijn gebruikers met beheerrechten actief die formeel werkzaam zijn vanuit de lijnorganisatie. Het aantal accounts is echter wel beperkt tot het noodzakelijk minimum.
6	Spend Cloud verstrekt jaarlijks een ISAE3402 type II rapport na afloop van het boekjaar, inzake de getroffen beheersmaatregelen omtrent wijzigingsbeheer. De organisatie heeft nog geen proces ingevuld om deze assurance-rapportages jaarlijks te beoordelen.

onvoldoende verbeterpunten voldoende Niet beoordeeld

Logische toegangs-
beveiliging (criteria 1-
5) nog
deels ontoereikend

Change management
(criteria 6) nog niet
beoordeeld

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

PROCES	2022	2023
1. Procedure autorisatiebeheer		
2. Periodieke controle op juistheid ingerichte autorisaties		
3. Identificatie van gebruikers voor toegang tot systemen en data		
4. Wachtwoordbeleid (authenticatie)		
5. Administrators en superusers		
6. Wijzigingenbeheer & Gescheiden omgevingen		

KORTE OMSCHRIJVING RESULTATEN	
1	De organisatie beschikt over een verouderde procedure autorisatiebeheer. Het autorisatiebeheerproces voor Youforce wordt echter wel volgens een controleerbaar proces uitgevoerd waarbij is vastgesteld dat gebruikers aan de juiste rechten zijn toegekend en rechten tijdig worden onttrokken.
2	Een periodieke review wordt uitgevoerd, echter is deze niet zichtbaar vastgelegd, waardoor onvoldoende controleerbaar is op welke aspecten de controle is uitgevoerd.
3	Alle aanwezige generieke accounts zijn verklaarbaar.
4	Enkele eindgebruikers hebben een wachtwoord dat niet verloopt op Windows AD. Echter is vastgesteld dat zij geen toegang hebben tot Youforce.
5	In Youforce zijn gebruikers met beheerrechten actief die formeel werkzaam zijn vanuit de lijnorganisatie. Het aantal accounts is echter wel beperkt tot het noodzakelijk minimum.
6	Raet (leverancier Youforce) verstrekt jaarlijks een ISAE3402 type II rapport na afloop van het boekjaar, inzake de getroffen beheersmaatregelen omtrent wijzigingsbeheer. De organisatie heeft nog geen proces ingevuld om deze assurance-rapportages jaarlijks te beoordelen.

voldoende
 verbeterpunten
 voldoende
 Niet beoordeeld

Relevante IT-ontwikkelingen bij gemeente Tynaarlo

Vanuit onze natuurlijke adviesrol zien wij een aantal belangrijke ICT-ontwikkelingen die (op termijn) effect kunnen hebben op de interne beheersing en de controle van de jaarrekening.

Gemeente Tynaarlo is voornemens om het applicatielandschap en de infrastructuur te moderniseren. Hiertoe behoort het aanbesteden van de applicaties Civision Middelen en Youforce waardoor het financieel- en HR-systeem (respectievelijk) mogelijk wordt vervangen.

Vanuit de jaarrekeningcontrole is bij applicatie implementatietrajecten de juistheid en volledigheid van een eventuele dataconversie van (historische) gegevens van belang. Hierbij adviseren wij om (1) op basis van een risicoanalyse maatregelen te nemen binnen het conversietraject en (2) controles op juistheid en volledigheid onderdeel te laten zijn van het conversietraject. Tevens adviseren wij om de controleresultaten aantoonbaar te documenteren in een conversiedossier en onderdeel te maken van de beslissing tot livegang.

Een conversiedossier bevat tenminste de volgende stukken:

- Projectplan of document waaruit de inrichting van de projectorganisatie rondom de conversie blijkt.
- Resultaten van een uitgevoerde risicoanalyse en daarop ontworpen conversiecontroles.
- Conversieplan of blauwdruk, waaruit de conversiestrategie, planning, beoogde controles, toleranties, verwachte (controleerbare) vastleggingen blijkt.
- Resultaten van een uitgevoerde analyse op te converteren data (scope en omvang van data, conversiemethodieken, mapping van oude naar nieuwe situatie, opschoningen en/of verrijkingen etc.).
- Procesregistraties waaruit blijkt dat geplande opschoningen en verrijkingen gecontroleerd hebben plaatsgevonden.
- Procesregistraties waaruit blijkt dat geplande proefconversies zijn beoordeeld en opgevolgd.
- Controleregistraties gericht op het vaststellen van juistheid en volledigheid van de finale conversie, en eventuele overige controles (acceptatietesten, sanity checks etc.).
- Controleregistraties waaruit blijkt dat geconstateerde afwijkingen zijn geëvalueerd en correcties zijn doorgevoerd en zijn gecontroleerd.
- Conversieverslag inclusief eventueel vrijgave-advies en benoeming nazorgactiviteiten.

4.7 Informatiebeveiliging en cybersecurity (1/2)

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

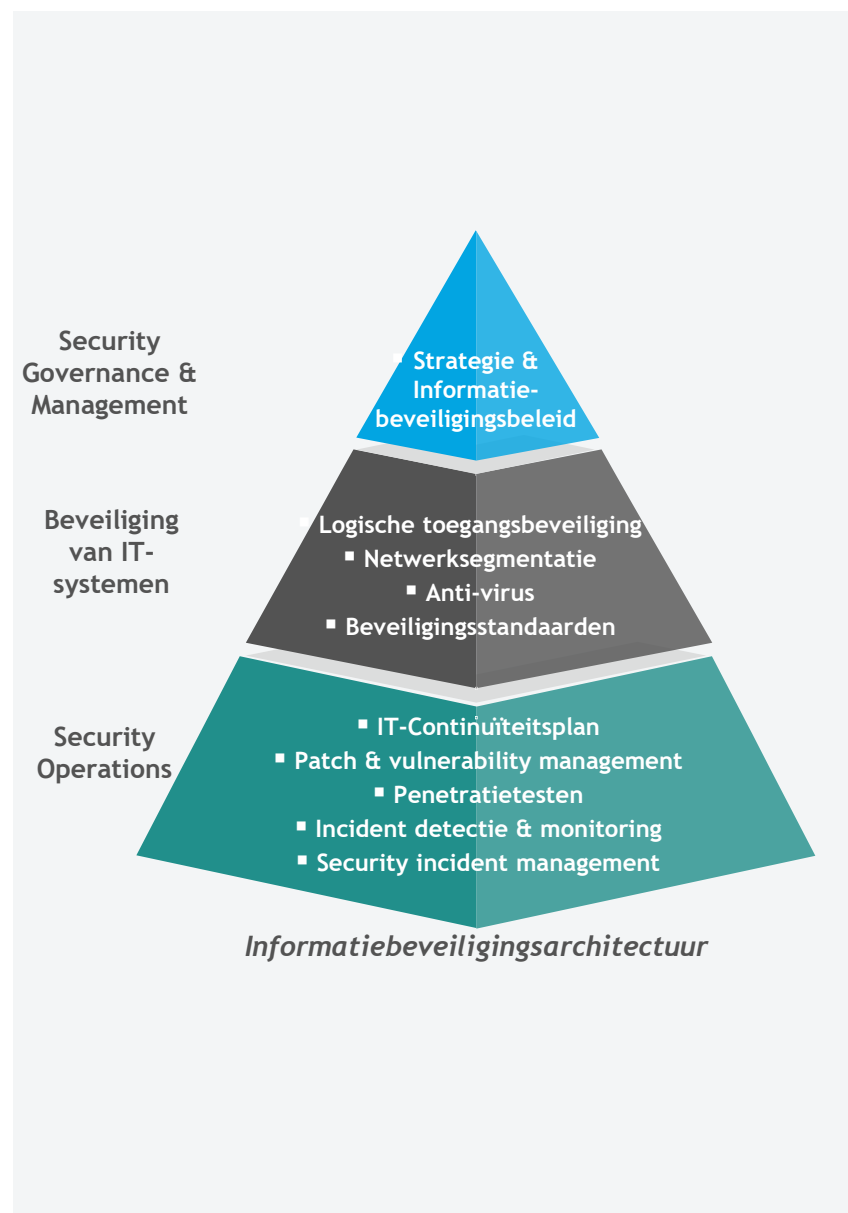
Vanuit onze natuurlijke adviesrol attenderen wij u graag op een aantal ontwikkelingen op het gebied van IT. Afgelopen jaren is er meer aandacht voor cybersecurity risico's ontstaan, mede door verhoogde (media)aandacht voor cybersecurity incidenten. Deze toegenomen aandacht voor cybersecurity risico's 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.



Informatiebeveiliging bij uw gemeente

Informatiebeveiliging bij gemeente Tynaarlo

Om de maatregelen ten aanzien van informatiebeveiliging te beoordelen hebben wij een interview gehouden met de Informatiemanager I&A en Vakgroep manager van dezelfde afdeling. Aanvullend hebben wij ontvangen documentatie geïnspecteerd. Op basis hiervan hebben wij begrepen dat de organisatie een informatiebeveiligingsbeleid heeft opgesteld. Momenteel wordt dit strategische beleid herzien door de CISO zodat binnenkort een nieuwe versie beschikbaar is. Voor de overige beleidsstukken zoals een procedure autorisatiebeheer, incidenten-procedure en wachtwoordbeleid geldt dat de gemeente veel heeft vastgelegd in werkafspraken, maar hier nog niet in alle gevallen een formeel beschreven procedure aan ten grondslag ligt.

In 2023 heeft de gemeente een cyber crisis oefening gehad. Hierbij waren onder andere de CISO, Vakgroep Manager I&A en enkele relevante stakeholders uit de organisatie betrokken. Wij hebben begrepen dat de organisatie hier relevante leerpunten uit heeft getrokken om zichzelf beter voor te bereiden op een echte cyber aanval.

Security awareness

Voor security awareness wordt momenteel door de CISO en de FG periodiek een post gemaakt op het intranet. Een interactieve training voor informatiebeveiliging wordt nog niet aangeboden. Wij zouden adviseren hier meer aandacht aan te besteden aangezien wij in de praktijk merken dat de mensen die het minst bekend zijn met informatiebeveiliging deze posts op het intranet niet, of beperkt, lezen. Deze doelgroep vormt juist de zwakste schakel van de organisatie en is kwetsbaar voor dreigingen van buitenaf. Wij hebben begrepen dat de CISO bij de introductie van nieuwe medewerkers wel een presentatie geeft over informatiebeveiliging, maar het speelveld is continu in ontwikkeling en het blijft belangrijk om hier doorlopend aandacht aan te schenken.

Bijlagen

- A Detailbevindingen processen
- B Detailbevindingen IT-beheer

A. Detailbevindingen processen

Bevinding	DE ZICHTBAARHEID VAN CONTROLES IN DE PLANNING & CONTROLCYCLUS KAN VERBETERD WORDEN	KANS: middel
Jaar van constatering	2019	IMPACT: middel
Onze bevinding/ constatering uit 2019	In het algemeen constateren wij dat de gemeente Tynaarlo een uitgebreid, maar niet volledig zichtbaar systeem van interne beheersing heeft omtrent begroting, tussentijdse rapportages en jaarrekening. Wij hebben de volgende bevindingen: - o Er is geen procesbeschrijving die ingaat op de totstandkoming van de begroting en rapportages. - o Bij het opstellen van tussentijdse rapportages is het van belang om vast te stellen dat deze aansluiten bij de financiële administratie en dat afwijkingen inhoudelijk afdoende zijn verklaard en aansluiten met de onderliggende berekeningen. Wij hebben vastgesteld dat de gemeente Tynaarlo een systeem van budgetbewaking heeft, waarbij op basis van diverse correspondentie zichtbaar is dat budgethouders daarbij betrokken zijn. Financieel consulenten geven aandachtspunten en bijzonderheden mee die de budgethouders dienen te verklaren. Er is geen totaaloverzicht waarin zichtbaar is of wordt bijgehouden dat alle aandachtspunten opgevolgd zijn. - o Uit de analyse van begrotingsafwijkingen in de jaarrekening van de afgelopen jaren blijkt dat met name baten en lasten in het sociaal domein en het grondbedrijf niet altijd goed te voorspellen zijn. - o Balansposten worden tussentijds niet zichtbaar geanalyseerd.	
Advies 2019	- o Wij adviseren een procesbeschrijving voor de totstandkoming van de programmabegroting en voortgangsrapportage op te stellen. - o Wij adviseren de controles of (diepgaande) analyse van de programmabegroting, de voortgangsrapportage en begrotingswijzigingen door zowel de afdeling financiën als de concerncontroller en het MT zichtbaar te maken. - o Wij raden de afdeling financiën aan gestructureerd en gecentraliseerd tussentijdse monitoring uit te voeren op de voortgang van budgetten (realisatie versus begroting). - o Wij raden aan om te analyseren voor welke baten en lasten de voorspelbaarheid beperkt is en hoe dit verbeterd kan worden. Ook raden wij aan om tussentijds balansposten te analyseren.	
Opvolging voorgaande jaren	U heeft geen opvolging gegeven aan deze bevinding in voorgaande jaren. Wij hebben voorgaande jaren aanvullend geconstateerd dat balansposities in de jaarrekening sterk af kunnen wijken van de begroting voor het betreffende jaar. Risico hiervan is dat geen goed inzicht is in onder meer de financieringsbehoefte en de financiële ratio's. Wij adviseren om investeringsplannen versus realisatie beter te monitoren en de uitkomsten hiervan te verwerken in de (balansposten zoals opgenomen in de) begroting. Naar verwachting van het college kunnen met de voorgenomen investeringen in een nieuw financieel pakket de verbeteringen in de P&C cyclus worden gerealiseerd.	
Opvolging 2023	Tijdens onze interim-controle hebben wij vastgesteld dat er slechts in beperkte mate opvolging aan deze bevinding is gegeven.	
Risico/gevolg	De basis van het proces "begroten en verantwoorden" van de gemeente is goed, echter als gevolg van de constatering hierboven is de mate van nauwkeurigheid niet altijd vast te stellen. Het risico bestaat dat de programmabegroting, de voortgangsrapportages en begrotingswijzigingen niet juist of volledig tot stand zijn gekomen en dat afwijkingen ten opzichte van de begroting niet tijdig signaleerd worden. Het risico hiervan is dat gestuurd wordt op basis van onjuiste, onvolledige of verouderde informatie.	
Ons advies 2023	Wij adviseren u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren.	

Bevinding	EEN ACTUELE FRAUDERISICO ANALYSE ONTBREEKT	KANS: middel
Jaar van constatering	2020	IMPACT: middel
Onze bevinding/ constatering uit 2020	Alle organisaties hebben te maken met risico's die een negatieve invloed kunnen hebben op haar financiële positie, haar reputatie en/of de mogelijkheid de gestelde beleidsdoelstellingen te realiseren. De primaire verantwoordelijkheid voor het beheersen van deze risico's berust bij het college en de gemeenteraad. Zij zijn onder andere verantwoordelijk voor het uitvoeren van een gedegen risicoanalyse, waaronder een frauderisicoanalyse. De gemeente Tynaarlo voert diverse risicoanalyses uit, maar een actuele frauderisicoanalyse ontbreekt.	
Advies 2020	Wij adviseren u een frauderisicoanalyse op te stellen en deze jaarlijks te bespreken en te updaten. Bij een frauderisicoanalyse worden fraudescenario's (manieren waarop fraude plaats kan vinden binnen uw organisatie) alsook de elementen van de fraudedriehoek (gelegenheid, druk en rationalisatie) betrokken.	
Opvolging voorgaande jaren	U heeft voorgaande jaren geen opvolging gegeven aan deze bevinding.	
Opvolging 2023	Wij hebben vastgesteld dat u in 2023 een concept frauderisicoanalyse/register hebt opgesteld. Deze analyse bevat een inschatting van de meest relevante frauderisico's die op basis van de mogelijke kans en impact zijn ingeschaald. Wij hebben vastgesteld dat de door u opgestelde frauderisicoanalyse in de basis voldoende diepgang heeft.	
Risico/Gevolg	Een frauderisicoanalyse heeft ten doel de frauderisico's in kaart te brengen, zodat de organisatie adequate maatregelen kan nemen die deze risico's kunnen mitigeren. Indien een (actuele) frauderisicoanalyse niet aanwezig is, bestaat het risico dat niet voldoende maatregelen zijn getroffen om een mogelijke fraude te voorkomen.	
Ons advies 2023	Wij adviseren om de concept analyse breder binnen de gemeente te bespreken en daarna te formaliseren. Daarnaast adviseren wij om de opgestelde frauderisicoanalyse jaarlijks te actualiseren. Gezien het belang, voor zowel uw organisatie als ook de accountantscontrole, van de frauderisicoanalyse gaan wij graag met u in gesprek om de door u opgestelde frauderisicoanalyse nader te spreken. Wij zullen op (korte) termijn hier een afspraak voor initiëren.	

Bevinding	PRESTATIELEVERING INKOPEN NIET ALTIJD GEWAARBORGD, CONTROLE OP BTW NIET ZICHTBAAR	KANS: middel
Jaar van constatering	2016	IMPACT: middel
Onze bevinding/ constatering uit 2016	Wij hebben geconstateerd dat in het inkoopproces de prestatielevering, de controle op juiste BTW-boeking en verwerking als kosten of investering niet als afzonderlijke processtappen wordt afgedwongen dan wel zichtbaar worden vastgesteld en vastgelegd.	
Advies 2016	In het inkoopproces onderscheiden wij de volgende activiteiten die met elkaar verbonden zijn welke wij adviseren in het proces op te nemen: - o De bestelling: het uitvaardigen van de opdracht aan de leverancier, wat tot een verplichting leidt (verplichtingenregistratie). - o De prestatielevering: het moment dat de leverancier goederen levert c.q. dienst verricht conform de bestelling (zichtbaar middels pakbon/rapportage/urenregistratie/proces verbaal/etc.). Dit leidt tot een afname van de uitstaande verplichting en tot een toename van de kosten. - o De factuur: nadat is vastgesteld dat de factuur conform de bestelling is en dat de prestatie ook daadwerkelijk is geleverd, kan de factuur betaalbaar worden gesteld.	
Opvolging voorgaande jaren	U geeft aan dat de budgethouder bij facturen > € 1.500 de prestatielevering vaststelt en dit zichtbaar maakt door middel van zijn digitale autorisatie. Dit blijkt niet expliciet uit de autorisatie (die voor meerdere toetspunten geldt) of uit de procesbeschrijving. De onderbouwing van de prestatielevering wordt niet vastgelegd. Als gevolg hiervan is niet in alle gevallen aantoonbaar dat de prestatielevering, de verwerking van de BTW en de verwerking als investering of kosten gecontroleerd is.	
Opvolging 2023	Wij hebben geconstateerd dat er nog onvoldoende opvolging is gegeven aan deze bevindingen.	
Risico/gevolg	Het risico bestaat dat bij de gemeente onterecht declaraties in rekening worden gebracht waarvoor geen/onvolledige/onjuiste prestatie verricht c.q. geleverd is door de wederpartij. Het risico bestaat dat, indien prestatielevering niet wordt vastgesteld, facturen onterecht geautoriseerd worden voor akkoord. Daarnaast bestaat het risico dat de BTW niet juist geboekt wordt en dat de factuur niet op de juiste grootboekrekening wordt verantwoord.	
Ons advies en onze aanvullende werkzaamheden	We adviseren de controle op prestatielevering, de verwerking van de BTW en de verwerking als investering of kosten zichtbaar vast te leggen. Daarnaast adviseren wij u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren.	

A.4 Subsidieverstrekingen | Geen sluitend subsidieregister

Bevinding	GEEN SLUITEND SUBSIDIeregISTER	KANS: midden
Jaar van constatering	2018	IMPACT: midden
Onze bevinding/ constatering uit 2018	Wij hebben geconstateerd dat de gemeente Tynaarlo niet over één sluitend subsidieregister beschikt. Hierdoor wordt niet in alle gevallen afgedwongen dat de interne procedures omtrent subsidieverstrekingen worden nageleefd.	
Advies 2018	Wij adviseren om tot één sluitend subsidieregister te komen en de subsidielasten onder één separate kostenplaats te verantwoorden.	
Opvolging voorgaande jaren	Wij hebben bij onze controles van eerdere boekjaren vastgesteld dat tot 2023 geen opvolging is gegeven aan de bevinding.	
Opvolging 2023	Wij hebben geconstateerd dat er nog onvoldoende opvolging is gegeven aan deze bevindingen.	
Risico/gevolg	Het risico bestaat dat subsidies worden verstrekt buiten de bevoegdheid van medewerkers om en mogelijk boven het subsidieplafond. Daarnaast bestaat het risico dat subsidies niet juist en tijdig worden vastgesteld.	
Ons advies en onze aanvullende werkzaamheden	Wij adviseren om tot één sluitend subsidieregister te komen en de subsidielasten onder één separate kostenplaats te verantwoorden. Daarnaast adviseren wij u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren. Deze aanvullende gegevensgerichte werkzaamheden betreffen onder andere het maken van een totaalaansluiting tussen de verstrekte subsidies vanuit de subadministratie en de verantwoorde subsidielasten in de financiële administratie. Daarnaast dient te worden beoordeeld of de verstrekte subsidies juist en tijdig zijn vastgesteld.	

Bevinding	VOLLEDIGHEID OPGELEGDE FACTUREN NIET GEBORGD	KANS: midden
Jaar van constatering	2018	IMPACT: laag
Onze bevinding/ constatering uit 2018	In 2018 is het heffings- en inningsproces omtrent de vergunningen overgegaan van de gemeente Tynaarlo naar de Belastingssamenwerking Drentsche Aa. Hiertoe levert de gemeente Tynaarlo periodiek een lijst met te factureren vergunningen aan bij de Belastingssamenwerking Drentsche Aa, die vervolgens verantwoordelijk is voor het heffen en innen van deze bedragen. Wij hebben tijdens de interim-controle geconstateerd dat er geen zichtbare aansluiting wordt gelegd door de gemeente Tynaarlo tussen de te factureren vergunningen, de werkelijk gefactureerde bedragen en de financieel verantwoorde en ontvangen bedragen.	
Advies 2018	Wij adviseren om periodiek (minimaal elk kwartaal) zichtbaar de aansluiting te leggen tussen de te factureren vergunningen en de daadwerkelijk gefactureerde vergunningen door de Belastingssamenwerking Drentsche Aa.	
Opvolging voorgaande jaren	U heeft in het verleden aangegeven voornemens te zijn periodiek (per kwartaal) zichtbaar de aansluiting vast te stellen tussen de te factureren vergunningen en de daadwerkelijk gefactureerde vergunningen.	
Opvolging 2023	De huidige situatie is ongewijzigd. Er vindt nog geen periodieke zichtbare aansluiting plaats tussen de subadministratie en de financiële administratie in het proces van omgevingsvergunningen.	
Risico/gevolg	Het risico bestaat dat de opbrengsten onvolledig worden verantwoord, wanneer de Belastingssamenwerking Drentsche Aa deze niet volledig factureert.	
Ons advies	Wij adviseren om periodiek (minimaal elk kwartaal) zichtbaar de aansluiting te leggen tussen de te factureren vergunningen en de daadwerkelijk gefactureerde vergunningen door de Belastingssamenwerking Drentsche Aa. Daarnaast adviseren wij u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren.	

A.6 Jeugd en WMO | Controle prestatielevering

Bevinding	Controle prestatielevering sociaal domein niet altijd aanwezig	KANS: midden
Jaar van constatering	2016	IMPACT: midden
Onze bevinding/ constatering uit 2016	Wij hebben vastgesteld dat bij her-aanvragen met betrekking tot zorg in natura een zichtbare controle plaatsvindt op de prestatielevering. Echter vindt deze controle niet plaats voor nieuwe cliënten/aanvragen en bij alle PGB-verstrekkings.	
Advies 2016	Tijdens de interim-controle 2016 is dit met u besproken waarbij vanaf 2017 de prestatielevering zal worden gewaarborgd bij herverstrekkings in de bespreekverslagen met de cliënten waarbij zichtbaar een evaluatie wordt opgenomen van eerder geleverde zorg.	
Geconstateerde opvolging in 2022	U heeft aangegeven de bevinding op te volgen als onderdeel van het verbetertraject van het Maatregelenpakket sociaal domein. U bent voornemens om steekproefgewijs cliënten aan te schrijven om vast te stellen of de geleverde zorg ook daadwerkelijk wordt geleverd. Echter vindt momenteel nog geen zichtbare controle op de prestatielevering plaats.	
Opvolging en aangescherpte bevinding 2023	Uw voornemens hebben nog niet geleid tot wijzigingen in het proces ten aanzien van controle op prestatielevering. Daarnaast hebben wij bij onze dossiercontroles vastgesteld dat bij herverstrekkings ook niet altijd sprake is van een zichtbare evaluatie van de prestatielevering.	
Risico/gevolg	Het risico bestaat dat er onterecht declaraties bij de gemeente in rekening worden gebracht, waarvoor geen/onvolledige/onjuiste prestatie is verricht c.q. geleverd door de wederpartij.	
Ons advies/ en onze aanvullende werkzaamheden	Wij adviseren om voor ieder dossier de prestatielevering zichtbaar te controleren door in de bespreekverslagen een evaluatie van de geleverde zorg op te nemen en uw voornemens voor controle op prestatielevering tijdens de looptijd van de verstrekking te realiseren. Daarnaast adviseren wij u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren.	

Bevinding	Controle wijziging crediteurenstamgegevens sociaal domein niet consequent uitgevoerd	KANS: laag
Jaar van constatering	2021	IMPACT: midden
Onze bevinding/ constatering uit 2021	Wij hebben geconstateerd dat de medewerkers die de betaalbestanden voor het sociaal domein (WMO en Jeugd) klaarzetten, ook rechten hebben om crediteurenstamgegevens te wijzigen. Wij hebben aanvullend daarop vastgesteld dat de controle op de wijziging van de crediteurenstamgegevens in het softwarepakket voor het sociaal domein (Aeolus) gedurende het boekjaar niet heeft plaatsgevonden.	
Advies 2021	Wij adviseren u de controle op de wijziging van de crediteurenstamgegevens in het softwarepakket voor het sociaal domein opnieuw in te richten. Tevens adviseren wij u de software zo in te richten dat de administratief medewerkers sociaal domein die de betaalbestanden klaarzetten, geen rechten meer hebben om de crediteurenstamgegevens te wijzigen.	
Opvolging voorgaande jaren	U heeft aangegeven dat uw VIC per jaareinde een integrale controle uit zal voeren op de doorgevoerde wijzigingen crediteurenstamgegevens. Dit betreft een controle achteraf, waardoor het geschetste risico reeds plaats heeft kunnen vinden. U bent voornemens om op korte termijn de controle op crediteurenstamgegevens in het proces in te regelen. De controle door de VIC is in tegenstelling tot de controle zoals deze tot 2021 bestond echter niet zichtbaar achteraf, waardoor voor ons niet is vast te stellen dat de controle plaats heeft gevonden.	
Opvolging 2023	In 2023 heeft u zoals voorgaand jaar aangegeven de controle op de crediteurenstamgegevens in het sociaal domein opnieuw ingericht. Vanaf september 2023 worden de mutaties in de crediteurenstamgegevens binnen Aeolus gecontroleerd. Deze controle heeft met terugwerkende kracht vanaf 1 januari 2023 plaatsgevonden. Over deze controle hebben wij de volgende op- en aanmerkingen: ○ De controle wordt niet systematisch afgedwongen en wordt uitgevoerd nadat de mutatie in Aeolus al is verwerkt. Hierdoor heeft de controle geen preventieve werking. ○ Door de manier waarop de controle wordt vastgesteld (in een Excelbestand), is voor ons en voor uw VIC-functionaris niet vast te stellen wie op welk moment de controle heeft uitgevoerd. ○ De controle wordt in opzet uitgevoerd door de medewerkers die ook de betaalbestanden klaarzetten. Hoewel de mutatie door medewerkers buiten het betalingsproces plaatsvindt, is hierdoor nog steeds geen sprake van volledige functiescheiding tussen het beheer van de crediteurenstamgegevens en de betalingen.	
Risico/gevolg	Het risico bestaat dat er facturen worden betaald aan een verkeerd rekeningnummer, met als gevolg dat crediteuren ten onrechte worden afgeboekt in uw administratie en een onrechtmatige uitstroom van middelen plaatsvindt.	
Ons advies en onze aanvullende werkzaamheden	Wij adviseren u de controle op de wijziging van de crediteurenstamgegevens in het softwarepakket voor het sociaal domein opnieuw in te richten. Tevens adviseren wij u Aeolus zo in te richten dat de administratief medewerkers sociaal domein die de betaalbestanden klaarzetten, geen rechten meer hebben om de crediteurenstamgegevens te wijzigen. Daarnaast adviseren wij u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren.	

Bevinding	Controle woonplaatsbeginsel	KANS: laag
Jaar van constatering	2016	IMPACT: laag
Onze bevinding/ constatering uit 2016	Wij hebben vastgesteld dat er geen zichtbare controle op het woonplaatsbeginsel plaatsvindt. Er vindt wel een zichtbare collegiale toetsing plaats op de beschikking en bij akkoord van de jurist gaat de beschikking naar de vakmanager voor ondertekening.	
Advies 2016	Wij adviseren om de controle van het woonplaatsbeginsel zichtbaar vast te leggen op het bespreekverslag. Deze toetsing dient zichtbaar plaats te vinden door een andere medewerker dan de consultant die het plan van aanpak heeft opgesteld.	
Opvolging voorgaande jaren	U geeft aan voornemens te zijn de controle op het woonplaatsbeginsel, als onderdeel van het verbetertraject als onderdeel van het Maatregelenpakket sociaal domein, uit te voeren. Echter vindt momenteel nog geen zichtbare controle op het woonplaatsbeginsel plaats. Achteraf wordt een controle op de het woonplaatsbeginsel uitgevoerd middels de GBA-overzichten.	
Opvolging 2023	U bent nog steeds voornemens om deze bevinding als onderdeel van het verbetertraject Maatregelenpakket sociaal domein op te pakken.	
Risico/gevolg	Het risico bestaat dat beschikkingen onrechtmatig worden verstrekt.	
Ons advies en onze aanvullende werkzaamheden	Wij adviseren om de controle van het woonplaatsbeginsel zichtbaar vast te leggen in het bespreekverslag. Deze toetsing dient zichtbaar plaats te vinden door een andere medewerker dan de consultant die het plan van aanpak heeft opgesteld. Daarnaast adviseren wij u om een onderbouwde keuze te maken of deze bevinding opvolging behoeft of dat het resterende restrisico en de aanvullende gegevensgerichte werkzaamheden door de gemeente zullen worden geaccepteerd. Indien de gemeente van mening is dat het restrisico kan worden geaccepteerd dan zullen wij hier in het vervolg niet meer over rapporteren en aanvullende gegevensgerichte werkzaamheden voor uitvoeren. Deze aanvullende gegevensgerichte werkzaamheden betreffen onder andere een detailcontrole op de rechtmatige totstandkoming van verstrekte uitkeringen sociaal domein.	

A.9 Aanbestedingen | Naleven aanbestedingsregels

Bevinding	Naleven aanbestedingsregels niet geborgd	KANS: midden
Jaar van constatering	2022	IMPACT: midden
Onze bevinding/ constatering uit 2022	Bij iedere bestelling > € 10.000 dient een inkoopmeldformulier ingevuld te worden door de afdeling waarbij de inkoper een begeleidingsformulier invult en aangeeft welke aanbestedingsvorm gekozen dient te worden. In 2021 heeft u dit in de herziene mandaatregeling opgenomen. Achteraf monitort de afdeling inkoop op de naleving hiervan middels de spendanalyse. Voor verlengingen en uitbreidingen van opdrachten wordt door de afdelingen niet in alle gevallen een inkoop gemeld middels het inkoopmeldformulier. Voor boekjaar 2021 heeft dit geleid tot onrechtmatigheden. Daarmee is er geen sprake van een sluitend systeem waarmee wordt geborgd dat vooraf de juiste aanbestedingsvorm wordt gekozen / de inkoper tijdig kan signaleren of verlengingen en uitbreidingen van opdrachten onder de gehanteerde aanbestedingsvorm hebben plaatsgevonden.	
Advies 2022	Wij adviseren om de workflow rondom de inkopen en aanbestedingen zodanig in te richten dat verplichte consultatie van Team Inkoop ook voor verlengingen en uitbreidingen van opdrachten kan worden afgedwongen. Daarnaast adviseren wij u om tijdig spendanalyses uit te voeren om mogelijke issues inzake het interne aanbestedingsbeleid alsook EU-aanbestedingen tijdig te signaleren.	
Opvolging 2023	Wij hebben geconstateerd dat er nog onvoldoende opvolging is gegeven aan deze bevindingen.	
Risico/gevolg	Naar onze inschatting is niet geborgd dat de beheersmaatregelen volg- en controleerbaar 'sluitend' zijn en zijn de beheersmaatregelen niet preventief van aard. Wij kunnen om deze redenen vanuit onze controlerende rol niet zonder meer steunen op de beheersmaatregelen in het proces ten aanzien van aanbestedingen. Hierdoor ontstaat het risico dat de gemeente Tynaarlo niet voldoet aan de Europese Aanbestedingsregels en de eigen interne spelregels.	
Ons advies en onze aanvullende werkzaamheden	Wij adviseren om de workflow rondom de inkopen en aanbestedingen zodanig in te richten dat verplichte consultatie van Team Inkoop ook voor verlengingen en uitbreidingen van opdrachten kan worden afgedwongen. Daarnaast adviseren wij u om tijdig spendanalyses uit te voeren om mogelijke issues inzake het interne aanbestedingsbeleid alsook EU-aanbestedingen tijdig te signaleren. In het kader van onze controle van de jaarrekening 2023 zijn aanvullende gegevensgerichte maatregelen in de vorm van een spendanalyse noodzakelijk.	

B. Detailbevindingen IT-Beheer

Bevinding	LOGISCHE TOEGANGSBEVEILIGING - AUTORISATIEBEHEER EN PERIODIEKE REVIEW	Gerelateerde BIO normen: 9.2.1 9.2.2.1 9.2.5.1 9.2.2.2 9.2.3.1	KANS: midden
Jaar van constatering	2021		IMPACT: midden
Applicaties	Mozard, Spend Cloud en Youforce		
Bevindingen	De gemeente beschikt inmiddels meerdere jaren over een verouderde procedure autorisatiebeheer. De organisatie beschikt voor Mozard en Spend Cloud over een (concept) autorisatiematrix, welke niet structureel gehanteerd wordt bij de toekenning van autorisaties. Specifiek voor Youforce geldt dat een dergelijke matrix voor het toekennen van autorisaties nog niet is opgesteld, buiten het systeem. Daarnaast worden autorisaties binnen Mozard toegekend op basis van voorbeeldgebruikers. Voor Civision Middelen is een verbetering doorgevoerd en voldoet het proces autorisatiebeheer nu aan de daaraan te stellen eisen. Om een adequaat autorisatiebeheerproces te borgen, dient periodiek een gebruikersreview op basis van een autorisatiematrix plaats te vinden. Voor Civision Middelen en Spend Cloud zijn dergelijke reviews zichtbaar uitgevoerd. Voor Mozard geldt dat een review op de actualiteit van gebruikers is uitgevoerd, echter zijn de ingerichte autorisaties per gebruiker niet zichtbaar beoordeeld. Eveneens hebben wij voor Youforce vastgesteld dat een zichtbare vastlegging van de periodiek beoordeling aanwezig is.		
Risico/Gevolg	Door het ontbreken van actuele procedures, autorisatiematrices en reviews bestaat het risico dat gebruikers te hoge/onjuiste autorisaties bezitten en hierdoor de functiescheidingsprincipes van de gemeente mogelijk doorbroken kunnen worden met het risico op ongeautoriseerde handelingen.		
Ons advies/ Uw aanvullende werkzaamheden	Wij adviseren de bestaande autorisatiebeheerprocedure en autorisatiematrices te actualiseren conform het vernieuwde autorisatiebeheerproces en de eisen die in de BIO worden gesteld. Aan de hand van de autorisatiematrices dienen de gebruikersreviews minimaal jaarlijks zichtbaar en controleerbaar plaats te vinden waarbij alle gebruikers en toegewezen autorisaties gecontroleerd dienen te worden. Deze reviews dienen uitgevoerd te worden door functionarissen die zelf niet over de bevoegdheden beschikken om gebruikers en/of autorisaties te beheren.		
Reactie management/ Opvolging			

Bevinding	LOGISCHE TOEGANGSBEVEILIGING - AUTHENTICATIE EN GEBRUIKERS MET BEHEERRECHTEN	Gerelateerde BIO normen: 9.4.3.1 9.4.3.5 9.2.3	KANS: laag
Jaar van constatering	2021		IMPACT: midden
Applicaties	Civision Middelen, Mozard, Spend Cloud en Youforce		
Bevindingen	De applicaties Mozard, Spend Cloud en Youforce maken gebruik van single sign-on op basis van Windows AD. Voor Youforce geldt dat tevens via de webomgeving kan worden ingelogd middels een geldige combinatie van gebruikersnaam en wachtwoord. Wij hebben een analyse van de Windows AD omgeving gedaan. Op basis hiervan is vastgesteld dat enkele gebruikersaccounts zijn uitgezonderd van het verplicht periodiek wachtwoord wijzigen. Deze gebruikersaccounts hebben niet direct toegang tot de applicaties relevant voor de jaarrekeningcontrole, maar dit kan verbeterd worden. Voor de applicaties Civision Middelen, Spend Cloud en Youforce geldt dat meerdere gebruikers met beheerrechten actief zijn die formeel werkzaam zijn vanuit de lijnorganisatie. Het aantal accounts met beheerrechten is echter wel per applicatie beperkt tot het noodzakelijk minimum.		
Risico/Gevolg	Door het uitzonderen van gebruikers bestaat het risico dat wachtwoorden door onbevoegden worden achterhaald en kunnen worden misbruikt. Hierdoor zouden eveneens de functiescheidingsprincipes doorbroken kunnen worden en ongeautoriseerde handelingen worden uitgevoerd. 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.		
Ons advies/ Uw aanvullende werkzaamheden	Ondanks dat dit niet direct een risico voor de jaarrekeningcontrole vormt adviseren wij een controle uit te voeren op de persoonlijke Windows AD accounts van eindgebruikers, zodat iedereen aan hetzelfde (sterke) wachtwoordbeleid dient te voldoen. Wij adviseren een duidelijke functiescheiding aan te brengen tussen het gebruik en het beheer van applicaties. 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-afdeling. Mocht dit vanuit organisatorisch oogpunt niet haalbaar zijn dan adviseren wij om zichtbaar aan te tonen dat de gebruikers met beheerrechten geen werkzaamheden in de lijnorganisatie hebben uitgevoerd (o.b.v. logging o.i.d.).		
Reactie management/ Opvolging			

Bevinding	WIJZIGINGENBEHEER	Gerelateerde BIO normen: 11.2 12.1.2 12.3.1.1 - 12.3.1.4 12.3.1.5	KANS: middel
Jaar van constatering	2021		IMPACT: middel
Applicaties	Civision Middelen, Spend Cloud en Youforce		
Bevindingen	De maatregelen inzake wijzigingsbeheer voor Civision Middelen, Spend Cloud en Youforce vallen onder verantwoordelijkheid van de leveranciers. De leveranciers verantwoorden zich jaarlijks middels een ISAE 3402 type II assurance-verklaring. De assurance-rapportages over 2023 zijn ten tijde van de IT-audit nog niet beschikbaar. Wij hebben daarnaast begrepen dat de gemeente nog geen proces heeft ingericht om deze assurance-rapportages te beoordelen en opvolging te geven aan de gebruikersverantwoordelijkheden.		
Risico/Gevolg	Indien geen zichtbare beoordeling wordt uitgevoerd op de assurance-rapportages bestaat het risico dat het wijzigingenbeheer proces of infrastructuur in de ogen van de gemeente niet adequaat wordt beheerd en mogelijk ongeautoriseerde handelingen worden doorgevoerd in de systemen. Eveneens bestaat het risico dat mogelijk aanvullende maatregelen die door de gebruikersorganisatie uitgevoerd dienen te worden, niet bekend zijn bij de organisatie.		
Ons advies/ Uw aanvullende werkzaamheden	Wij adviseren afspraken te maken welke functionaris verantwoordelijk is voor management van de leverancier. Vervolgens adviseren wij de assurance-rapportages, zodra deze beschikbaar zijn, op te vragen en deze kritisch te beoordelen teneinde vast te stellen of de getroffen maatregelen in lijn zijn met het beleid van de gemeente en in hoeverre de gemeente voldoet aan de in de assurance-rapportage gestelde gebruikersmaatregelen. Bij laatst genoemde kunt u denken aan beoordelen van release notes, of uitvoeren van (acceptatie) testwerkzaamheden.		
Reactie management/ Opvolging			