- CONCEPT - 25 NOVEMBER 2022

MANAGEMENT LETTER 2022

Gemeente Bernheze

BDO

Aanbiedingsbrief

Gemeente Bernheze
T.a.v. het college van B&W
De Misse 6
5384 BZ HEESCH

Eindhoven, 25 november 2022

Kenmerk: XXXXXX/XXX/XX/XX

Geacht college,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2022 van de gemeente Bernheze 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 2022 van dienst te zijn geweest. Wij willen de organisatie bedanken voor de prettige samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,

BDO Audit & Assurance B.V.
namens deze,

drs. D.O. Meeuwissen RA
Partner en extern accountant gemeente Bernheze

VORIGE PAGINA
VOLGENDE PAGINA
INHOUDSOPGAVE
SAMENVATTING

Inhoudsopgave

1. Dashboard interim-controle

1.1 Dashboard interim-controle

FRAUDERISICOBEHEER

- Vanaf boekjaar 2022 zij aanpassingen doorgevoerd inzake het verplicht rapporteren over onze controleaanpak ten aanzien van fraude- en vermogensrisico's in onze controleverklaring. Dit vraagt om een zorgvuldig proces, dat wij samen met u zullen doorlopen
- De gemeente heeft in het kader van fraude diverse kaders en regelingen opgesteld gebaseerd op modelhandreikingen zoals ook gerapporteerd in de managementletter 2021. De frauderisicoanalyse van uw gemeente wordt eind 2022 geactualiseerd. Bij het actualiseren van de frauderisicoanalyse is het aan te bevelen aandacht te besteden aan onder meer de verantwoordelijkheden en termijnen voor de opvolging van aanbevelingen.

RECHTMATIGHEIDSVERANTWOORDING 2023

- De invoering van de rechtmatigheidsverantwoording geldt vanaf het verslagjaar 2023.
- De gemeenteraad dient zelf een aantal keuzes te maken, waaronder het vaststellen van het grensbedrag (0%-3%) en de rapporteringstolerantie. Wij adviseren het grensbedrag gelijk te stellen aan de materialiteit voor de jaarrekeningcontrole (1%) en de rapporteringstolerantie op 5% van de materialiteit.
- De terminologie en inhoud van de financiële verordening zijn nog niet in overeenstemming met de rechtmatigheidsverantwoording. Gemeente Bernheze wacht hierbij op het beschikbaar komen van diverse notities en uitingen.
- Met de publicatie van de notities van SDO en de BADO kan de organisatie verdere invulling geven aan de rechtmatigheidsverantwoording.

AANDACHTSPUNTEN JAARREKENING 2022

- Door de hoge inflatiecijfers (circa 12% volgens het CBS) lopen gemeenten het risico dat (offertes voor) bestedingen die onderhands zijn gegund toch de drempel overschrijden voor het verplicht moeten doorlopen van een Europese aanbestedingsprocedure.
- Er is geen intern proces om de status van de bestedingen en SiSa-regelingen tussentijds te monitoren. Gezien de flinke toename van de aantal SiSa-regelingen in de afgelopen jaren zullen wij in overleg treden met de organisatie om tijdig inzicht te krijgen voor het huidig boekjaar.

BEVINDINGEN SIGNIFICANTE PROCESSEN

- Wij kwalificeren de interne beheersing over het algemeen in opzet voldoende en binnen de primaire processen is sprake van minimaal noodzakelijke primaire functiescheiding. Deze functiescheiding ontbreekt echter bij de processen memoriaalboekingen en omgevingsvergunningen.
- Ten opzichte van voorgaand jaar zijn de processen in grote lijnen gelijk gebleven.
- Verbeteringen zijn met name te behalen in het opstellen of actualiseren van procesbeschrijvingen, mede met het oog op de invoering van de rechtmatigheidsverantwoording. Met de krapte op de arbeidsmarkt kan uitval van medewerkers impact hebben op de uitvoering van (primaire) processen binnen de gemeente.

BEHEERSING IT

- Gemeente Bernheze is per 1 januari 2022 overgestapt naar een nieuwe applicatie voor de financiële administratie.
- De belangrijkste verbeterpunten met betrekking tot de financiële administratie zien toe op periodiek beoordelen van de ingerichte autorisaties, accounts met superuser rechten en het wachtwoordbeleid.
- Er zijn twee belangrijke aandachtspunten voor het uitbesteden van IT-applicaties, te weten periodiek beoordelen van de contracten en het periodiek beoordelen van de aanwezige leveranciersaccounts.

VERBIJZONDERE INTERNE CONTROLE

- De Interne Controles worden door de financieel beleidsmedewerkers en medewerkers financiële administratie uitgevoerd. Alle interne controles worden door één functionaris, de coördinator interne controles, gereviewed.
- De VIC bij Bernheze kwalificeert als Variant 2; VIC werkt samen met de accountant en voert gegevensgerichte controles uit.
- Onze conclusie in relatie tot de verbijzonderde interne controle is ongewijzigd. Net als in 2021 kwalificeren wij de VIC niet als interne beheersmaatregel, maar als instrument voor de aanlevering van stukken.
- Vanwege het uitvallen van personeel is de VIC controle voor 2022 slechts voor 5 relevante processen uitgevoerd. U heef actie ondernomen om deze achterstand in te halen.

2. Ontwikkelingen & Aandachtspunten

2.1 Rapporteren over fraude en continuïteit in de controleverklaring

Verplicht rapporteren in de controleverklaring over fraude en het vermogen om risico's vanuit de reguliere bedrijfsvoering financieel op te vangen

Verplicht rapporteren in de controleverklaring over fraude en het vermogen om risico's vanuit de reguliere bedrijfsvoering financieel op te vangen

Vanaf boekjaar 2022 worden door de Nederlandse Beroepsorganisatie van Accountants (NBA) enkele aanpassingen in de controleverklaring doorgevoerd. Deze aanpassingen zien op het verplicht rapporteren over onze controleaanpak frauderisico's en onze controleaanpak ten aanzien van het vermogen om risico's vanuit de reguliere bedrijfsvoering financieel op te vangen in de controleverklaring. Deze verplichting geldt voor wettelijke controles (gemeenten, provincies en waterschappen). Voor niet wettelijke controles kan in overleg de nieuwe uitgebreide controleverklaring vrijwillig worden toegepast. Met het verplicht rapporteren over deze onderwerpen wordt tegemoet gekomen aan een veel gehoorde wens van stakeholders om transparanter te zijn over welke werkzaamheden wij als uw accountant hebben uitgevoerd om frauderisico's en het vermogen om de risico's vanuit de bedrijfsvoering financieel op te vangen alsmede de bedrijfsvoering zonder tussenkomst van de provinciale toezichthouder voort te zetten. Per onderwerp zullen wij voortaan, in alle gevallen, gaan rapporteren over wat de meest belangrijke frauderisico's zijn, over de inschatting van het college om de risico's vanuit de bedrijfsvoering financieel op te vangen en hoe op beide thema's in de controle is ingespeeld.

Uiteraard hebben de onderwerpen fraude en het vermogen om financiële risico's op te vangen altijd al de aandacht tijdens de accountantscontrole, maar door deze zaken nu te gaan beschrijven in de controleverklaring wordt die aandacht ook expliciet gemaakt. Wij zullen in de controleverklaring 2022 rapporteren over onze werkzaamheden rondom fraude en continuïteit. Wij zijn ons er van bewust dat dit om een zorgvuldig proces vraagt, wat wij samen met u zullen doorlopen en waarover wij tijdig met u van gedachten zullen wisselen. Dit proces vraagt namelijk ook iets van u, bijvoorbeeld over úw aandacht voor genoemde risico's en over de door u gewenste mate van transparantie in de programmarekening en de programmaverantwoording over zowel fraude als het vermogen om financiële risico's op te vangen. Wij gaan daarover graag met u in gesprek.

Transparantie over fraude en continuïteit vraagt dialoog

Onze controle gaat uit van de fraudepreventie door de gemeente Bernheze

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 gemeenteraad, 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. De landelijke pilots waar in de controleverklaring 2020 van de accountant uitgebreider wordt gerapporteerd over het thema fraude (o.a. Gemeente Breda) hebben bijgedragen aan de best practices. De best practices van de NBA zijn erop gericht het fraudebewustzijn en de frauderisicobeheersing te vergroten.

Graag gaan wij met u in overleg over het vergroten van de actieve rol van de gemeenteraad/auditcommissie ten aanzien van frauderisico-beheersing. Bijvoorbeeld door 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 controller, een accountant of een gespecialiseerde (fraude)onderzoeker. Uw gemeente heeft diverse kaders en regelingen opgesteld die zijn gebaseerd op modelhandreikingen zoals ook is gerapporteerd in het managementletter 2021. Wij hebben begrepen dat de frauderisicoanalyse eind 2022 nog wordt geactualiseerd.

2.2 Rechtmatigheidsverantwoording (1/2)

Mededeling doen omtrent de naleving van de rechtmatigheid door het college

De SiSa-verantwoording wordt mogelijk ook een onderdeel van de rechtmatigheidsverant woording

Invoering rechtmatigheidsverantwoording met ingang van 2023

In onze management letter van 2021 hebben wij aangegeven dat de rechtmatigheidsverantwoording ingevoerd wordt voor gemeenten. Dit besluit is nu door de tweede kamer aangenomen, de rechtmatigheidsverantwoording wordt ingevoerd met ingang van 2023. Deze invoering heeft gevolgen voor de (interne) beheersing van de organisatie en ook de rol van de accountant verandert hierdoor. Wij verwachten dat dit een aanzienlijke uitdaging is, maar ook een kans voor uw organisatie en interne beheersing. Met ingang van verslagjaar 2023 wordt de gemeente Bernheze zelf verantwoordelijk voor de rechtmatigheidsverantwoording en moet het college een (onderbouwde) mededeling doen omtrent de naleving van de rechtmatigheid. De wetswijziging is niet alleen een technische verandering maar ook een cultuurverandering die effect heeft op de bedrijfsvoering van de organisatie.

Een belangrijke recente ontwikkeling is dat de SiSa-verantwoording mogelijk ook onderdeel van de rechtmatigheidsverantwoording wordt. De interne beheersing rondom het aanvragen, besteden en verantwoorden van specifieke uitkeringen is daarmee een relatief nieuw proces dat aandacht van de organisatie behoeft en van incidentele activiteiten bij de jaarafsluiting naar een continu beheerst proces kan worden opgeschaald. Hierbij merken we op dat de verwachting is dat het aantal SiSa-regelingen de komende jaren verder zal toenemen en tot extra werkzaamheden zal leiden.

Uit de kadernota rechtmatigheid 2023 van de commissie BBV blijkt dat er een standaard model van de verklaring komt, de rechtmatigheid wordt beperkt tot drie rechtmatigheidsaspecten, het algemeen bestuur kan de tolerantiegrenzen zelf bepalen (tot 3%) en bevindingen moeten worden opgenomen in de paragraaf bedrijfsvoering. Wij bevelen u aan om het grensbedrag gelijk te stellen aan de materialiteit voor de jaarrekeningcontrole (1%) en de rapporteringstolerantie op 5% van de materialiteit conform de BADO.

In alle gevallen zal de komende periode gebruikt moeten worden om voorbereidingen te treffen voor de invoering van de rechtmatigheids-verantwoording. De wijziging in de verantwoordelijkheden ten aanzien van rechtmatigheid betekent niet dat er minder rechtmatigheidscontroles moeten worden uitgevoerd, maar dat het college deze zelfstandig/intern moet inrichten, uitvoeren, controleren en rapporteren. Als accountant zullen wij die werkzaamheden vervolgens toetsen, teneinde te kunnen controleren en verklaren dat de rechtmatigheidsverklaring van het college een getrouw beeld geeft.

Onze observaties over de voortgang van de voorbereidingen hebben we in de tabel op de volgende pagina gegeven. Wij ondersteunen graag op de punten waar dit gewenst is.

2.2 Rechtmatigheidsverantwoording (2/2)

TE ZETTEN STAPPEN	AFSPRAKEN COLLEGE GEMAAKT?			
	ja	onderhanden	n.v.t.	Toelichting
De normenkader en verantwoordingsgrens blijven gelijk aan 2022 en zijn nog niet vastgesteld door de raad				
De verantwoordingsgrens voor 2023 is bepaald	●			De verantwoordingsgrens blijft hetzelfde als in 2022.
De verantwoordingsgrens voor 2023 is vastgesteld door de raad		●		De verantwoordingsgrens is nog niet vastgesteld.
Het normenkader 2022/2023 is gereed, datum vaststelling door de raad is gepland		●		Het huidige normenkader is de basis en wordt samen met de toetsingskader jaarlijks geüpdatet. De raad wordt middels een notitie geïnformeerd. De actualisatie wordt in december 2022 door het college vastgesteld.
De financiële verordening wordt bewust pas in 2023 vastgesteld om de meest actuele informatie mee te nemen				
De financiële verordening is herzien		●		De vaststelling van de financiële verordening is uitgesteld naar 2023 i.v.m. de invoer van de rechtmatigheidsverantwoording.
De financiële verordening bevat op welke wijze wordt omgegaan met begrotingsonrechtmatigheden		●		De financiële verordening wordt bewust uitgesteld naar 2023 om de meest actuele informatie (inclusief het omgaan met begrotingsrechtmatigheid) wordt meegenomen.
Het college en de raad hebben overeenstemming over de inhoud van de paragraaf Bedrijfsvoering		●		Zie eerdere toelichting. Dit is uitgesteld naar 2023.
In het jaarlijks controleplan wordt rekening gehouden met zowel materiële als politiek gevoelige onderdelen				
Het interne controleplan van de gemeente bevat:				
1. scoping van de processen en balansposten	●			In het controleplan wordt rekening gehouden met zowel processen en posten van materiele aard als proces- of politiek gevoelige onderdelen.
2. risico-analyses per proces en post	●			Het controleplan richt zich op onderdelen binnen de organisatie met een hoger risico.
3. controleaanpak	●			Er wordt jaarlijks een interne controleplan geschreven waar per onderdeel een stappenplan wordt uitgeschreven.

2.3 Aandachtspunten jaarrekening 2022 (1/2)

Documentatie van ramingen bij aankondiging of inleiding procedure aanbesteding essentieel

Inflatie en aanbestedingsprocedure

Het inflatiecijfer is in 2022 uitzonderlijk hoog. In augustus meldde het CBS een inflatiecijfer tot meer dan 12%. Veel gemeenten hebben, voordat de hoge inflatie bekend werd, ramingen opgesteld voor overheidsopdrachten en vaste prijsafspraken gemaakt. Door de inflatie loopt men nu het risico dat (offertes voor) bestedingen, waarvoor een reële raming is afgegeven, en onderhands zijn gegund, toch de drempel overschrijden voor het verplicht doorlopen van een Europese aanbestedingsprocedure. In een dergelijk geval hoeft de gemeente niet alsnog Europees aan te besteden.

Belangrijk hierin is dat:

- de raming reëel was op het tijdstip van verzending van de aankondiging of het moment van inleiden van de procedure voor gunning van de opdracht;
- de raming goed gedocumenteerd moet zijn met inbegrip van opties van het contract;
- een eventuele wijziging goed wordt gemotiveerd, wordt onderbouwd met bewijsstukken en de wijziging dient gedocumenteerd te worden in het inkoopdossier. Dat kan met een afwijkingennotitie.

Inflatiecorrectie buiten afspraken mogelijk binnen wetgeving EU-aanbestedingen

Inflatie en wezenlijke wijziging

Wij zien dat veel opdrachtnemers een beroep doen op de opdrachtgevers om de contractwaarde aan te passen naar de huidige marktomstandigheden, terwijl dit buiten contractuele voorwaarden gaat. Door sterk stijgende kosten van grondstoffen en loon kunnen contracten niet nageleefd worden zonder grote financiële- en continuïteitrisico's voor de opdrachtnemer en daarmee de opdracht. De aanbestedingswet biedt een tweetal opties om contractafspraken aan te passen.

- Een bagatelwijziging (de wijziging is minder dan 10 procent van de totale opdrachtwaarde inclusief opties en verlengingen, bij diensten of leveringen, 15% van de opdrachtwaarde bij werken);
- Een onvoorziene omstandigheid (2.163e Aw).

Van de bagatelregeling kan eenvoudig gebruik gemaakt worden, waarbij documenteren hiervan wel belangrijk is. Als de bagatel al is gebruikt, resteert de wijzigingsgrond van de onvoorziene omstandigheid. In dat geval moet worden aangetoond dat:

1. de oorzaak van de prijsstijging niet kon worden voorzien door de opdrachtgever;
2. de wijziging minder bedraagt dan 50 procent van de totale opdrachtwaarde;
3. de algemene aard van de opdracht niet wordt gewijzigd; en
4. de omstandigheden zijn terug te voeren op een externe oorzaak.

In de jurisprudentie is een aantal voorbeelden terug te vinden waarbij deze argumentatie stand heeft gehouden. Het tekort aan grondstoffen door lockdowns in China, de sancties tegen Rusland, de oorlog in Oekraïne en het algemeen personeelstekort zijn voorbeelden van deze onvoorziene omstandigheden. Naar de jaarrekeningcontrole toe is het belangrijk om deze overwegingen vast te leggen (voor aanpassing van de overeenkomst) om het proces niet te vertragen.

2.3 Aandachtspunten jaarrekening 2022 (2/2)

Grip op jaarrekeningproces

Voor u als college is het van belang dat het jaarrekeningproces geen vertraging oploopt en u tijdig de jaarstukken vaststelt en verstrekt. Als accountant van gemeente Bernheze zien wij hierin voor ons een belangrijke rol weggelegd.

Zaken die het jaarrekeningproces kunnen vertragen moeten tijdig worden geadresseerd. Voorbeelden van dergelijke zaken betreffen:

Vanwege de toename in het aantal SiSa-regelingen verdient het de aanbeveling ook tussentijds de omvang van deze regelingen te monitoren

- De toename van het aantal SiSa-regelingen door het Rijk die een aantal jaren terug is ingezet en zowel de organisatie bij het opstellen als de accountant in de controle extra tijd en werk bezorgen. Er is geen intern proces voor tussentijdse monitoring van de SiSa-regelingen, echter wel rondom de jaarafsluiting door het doorlopen van de grootboekrekeningen samen met verantwoordelijken. Het is een aandachtspunt voor u om niet alleen per jaareinde maar ook op enig gewenst tussentijds moment een actueel en volledig inzicht in het aantal en de omvang en alle toegekende SiSa-regelingen te krijgen. Wij adviseren u om tussentijds op de hoogte te blijven van alle actualiteiten met betrekking tot de SiSa en wat de omvang is per regeling voor uw gemeente. Vlak na jaareinde zullen wij met u in overleg treden om tijdig inzicht te hebben in het aantal regelingen voor het huidige boekjaar.

Afspraken inzake (gedeeltelijk) uitbestede processen maken en monitoren

- Tijdige informatievoorziening met betrekking tot (gedeeltelijk) uitbestede processen is van belang, zoals jeugdzorg. Uitloop in de planning van deze partijen heeft daardoor extra gevolgen voor de planning van het bestuurlijk proces van gemeente Bernheze en de (tijdige) beschikbaarheid van deze informatie. Wij adviseren u met deze partijen concrete afspraken te maken en te monitoren ten behoeve van het bestuurlijk proces.

3. Bevindingen significante processen

3.1 Onze controle nog transparanter (1/2)

Kwaliteit en proces van management rapportage

Onderkende risico's:
- Management override
- EU-aanbestedingen
- Waardering grex
- Ongeautoriseerde handelingen in Key2

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 Bernheze. 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.

Onze inschatting van de risico's en belangrijkste processen

In het kader van de controle van de jaarrekening 2022 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 Bernheze:

- 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 uitoefenen op de in de jaarrekening gepresenteerde uitkomsten, beperkt zijn mede dankzij de maatregelen die gehanteerd worden per proces. Om het resterende risico te beperken beoordelen wij schattingsprocessen en bijzondere journaalposten in detail.
- Het niet naleven van de Europese aanbestedingsregels.
- Onjuiste waardering bouwgronden in exploitatie van De Erven en Zwarte Molen vanwege stijgende materiaal en/of personeelskosten.
- De gevolgen van ongeautoriseerde handelingen in Key2Financiën.

In onze aanpak is de insteek, daar waar mogelijk te steunen op de interne beheersing in de significante processen van de gemeente Bernheze. Dit noemen wij een zogenaamde systeemgerichte aanpak, waarbij wij kunnen steunen op toereikende maatregelen in uw processen en systemen. Daarbij maken wij, indien mogelijk, gebruik van uw eigen verbijzonderde interne controle (VIC).

3.1 Onze controle nog transparanter (2/2)

Per proces toetsen:
- AO/IB
- IT-maatregelen
- VIC

Uitwerking controlestrategie per proces

Voor elk proces beoordelen wij de volgende onderdelen:
- **AO/IB:** Is sprake van een actuele en toereikende procesbeschrijving met voldoende beheersmaatregelen?
- **IT-maatregelen:** Zijn in en rondom het systeem voldoende waarborgen getroffen t.a.v. de betrouwbaarheid van de gegevensverwerking?
- **VIC:** Heeft de VIC de interne beheersmaatregelen getoetst en kunnen wij daar gebruik van maken?

Op basis van de toereikendheid van de interne beheersingsmaatregelen, onze ervaring en de kwaliteit en omvang van de materiële processen voor de jaarrekening, bepalen wij of we deze procesmatig / systeemgericht toetsen of (achteraf) gegevensgerichte werkzaamheden uitvoeren in de vorm van steekproeven / deelwaarnemingen, cijferanalyses, verbandscontroles, etc. verbandscontroles, etc.

Bij een toereikende interne beheersing kunnen wij er gebruik van maken tijdens de controle

Indien bovenstaande vragen positief kunnen worden beantwoord, is de organisatie optimaal in control en kunnen wij, waar mogelijk, gebruik maken van uw eigen interne beheersing. De vaak tijdrovende en gedetailleerde gegevensgerichte werkzaamheden, kunnen dan beperkt blijven tot een minimum. Bij de voorbereiding van de jaarrekeningcontrole maken wij afspraken over de resterende werkzaamheden, aanpak en de hiervoor benodigde informatie.

Vanzelfsprekend geven wij, evenals in voorgaande jaren, vanuit onze natuurlijke adviesrol aanbevelingen op welke wijze verbeteringen in de interne beheersing mogelijk zijn. De belangrijkste bevindingen en aanbevelingen met betrekking tot de significant processen hebben wij opgenomen in de tabel in paragraaf 3.2.

Samenvatting effectiviteit van de primaire processen

In het overzicht op de volgende pagina geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook hoofdstuk 4 t.a.v. ICT).

Wij kunnen vooralsnog niet altijd steunen op de interne beheersing. Onze aanpak is daarom hoofdzakelijk gegevensgericht

Wij concluderen dat de door ons beoordeelde processen in opzet niet zijn gewijzigd ten opzichte van vorig jaar. Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat binnen de processen over het algemeen sprake is van minimaal noodzakelijke primaire functiescheiding. Tevens is binnen de processen sprake van interne beheersmaatregelen. Deze maatregelen worden echter niet toereikend vastgelegd of consequent toegepast, waardoor achteraf niet toetsbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd. Omdat de AO/IB en IT General Controls niet altijd goed zijn opgezet of goed werken, kunnen wij voor onze controle nog niet op de processen steunen en bestaat onze controleaanpak overwegend uit gegevensgerichte werkzaamheden.

3.2 Effectiviteit processen

PROCES	CTFS	AO/IB	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK	T.o.v. 2021
Planning & Control				Er is onvoldoende zichtbare functiescheiding ten aanzien van het proces rondom memoriaalboekingen. Aanlevering van een boeking en onderliggende documentatie door de budgethouder wordt niet afgedwongen. Een financieel medewerker kan dit proces zelfstandig opstarten en afronden. Daarnaast ontbreekt er een zichtbare autorisatie voor de memoriaalboeking door een budgethouder. De enige controle op de memoriaalboekingen is de controle of deze in balans is, maar er vindt geen controle op juistheid aan de hand van onderliggende bronbescheiden plaats. Ten tijde van de controle was er nog geen VIC uitgevoerd voor dit proces als gevolg van uitval van personeel.	→
Subsidies				De procesbeschrijving is in het boekjaar 2021 geactualiseerd als gevolg van het vaststellen van de nieuwe Verordening Welzijnssubsidies op 12 december 2020. Hierin zijn de gestelde termijnen voor het indienen van verantwoordingen aangepast. Tevens zijn in de subsidiebeschikking geen prestatieafspraken voor subsidieontvangers opgenomen. Het proces is ongewijzigd ten opzichte van voorgaand jaar. Ten tijde van de controle was er nog geen VIC uitgevoerd voor dit proces als gevolg van uitval van personeel.	→
Inkopen & betalingen				Er is sprake van minimaal noodzakelijke (primaire) functiescheiding, waarbij facturen worden goedgekeurd door een budgetbewaker en een budgethouder. De controle op prestatielevering wordt echter niet zichtbaar vastgelegd door de budgethouder. Dit is een bewuste keuze van de gemeente. Bij het wijzigen van crediteuren stamgegevens en het verrichten van betalingen is eveneens sprake van functiescheiding en een vierogen principe.	→
Aanbeste-dingen				Er is sprake van een minimaal noodzakelijke (primaire) functiescheiding doordat inkoopadviseurs bij aanbestedingen groter dan € 30.000 betrokken zijn bij het proces. Dit wordt echter niet afgedwongen in het proces en is ook niet zichtbaar. Wel neemt het college vooraf een besluit over de Europese aanbestedingen en bij aanbesteding van werken groter dan € 500.000 en worden achteraf ook ingelicht over de gunning. Tevens vindt er geen controle plaats op stilzwijgende verlengingen, wezenlijke wijzigingen of homogene opdrachten op basis van CPV-codes. Ten tijde van de controle was er nog geen VIC uitgevoerd voor dit proces als gevolg van uitval van personeel. Achteraf worden middels een spendanalyse eventuele onrechtmatigheden geconstateerd.	→
Personeel				Er is sprake van voldoende functiescheiding in het personeelsproces. In- en uitdiensttredingen worden op basis van een checklist door onder andere HRM en de salarisadministratie behandeld, verwerkt en door een collega financiële administratie ingeboekt in de FA. Een deel van de mutaties, zoals collectieve verhogingen, worden door de salarisverwerker Centric doorgevoerd. Maandelijks vindt een controle plaats door de salarisadministrateurs op de mutaties voordat deze naar Centric worden gestuurd. De tweede controle op de doorgevoerde mutaties vindt echter niet zichtbaar plaats. De fouten worden in de volgende ronde opnieuw gestuurd ter correctie.	→
Omgevings-vergunningen				Omgevingsvergunningen zijn voor het eerste halfjaar in Squit XO behandeld en het tweede halfjaar in RXmission. Elke standaard vergunnings-aanvraag heeft één dossiereigenaar die de vergunningaanvraag behandelt, de (volledigheid van de) aanvraag toetst aan de verordening en de beschikking verzendt. Er is daarmee geen sprake van functiescheiding binnen het primaire proces. Eventuele risico's worden achteraf door de VIC gemitigeerd. Complexe vergunningsaanvragen worden binnen het team besproken en hiervan wordt een lijst bijgehouden.	→
Verhuur				Er is sprake van voldoende functiescheiding binnen het verhuurproces tussen de het opstellen en ondertekenen van de overeenkomsten, de facturatie en het registreren van de ontvangen bedragen. Contracten kunnen niet altijd worden teruggevonden en er vindt verder geen zichtbare controle plaats op de volledigheid van de facturatie. Hierdoor is de AO/IB voor verbetering vatbaar.	→
Grond-exploitaties incl.aan- en verkopen				Binnen het proces rondom de grondexploitatie is sprake van minimaal noodzakelijke (primaire) functiescheiding tussen de planeconoom, projectmanager wonen en beleidsmedewerker financiën. Het proces is ongewijzigd ten opzichte van voorgaand jaar.	→
Sociaal domein				Er is sprake van een minimaal noodzakelijke (primaire) functiescheiding. Vorig jaar was het proces jeugdzorg belegd bij gemeente 's-Hertogenbosch. Met ingang van 1 januari 2022 is de factuurverwerking van het proces jeugdzorg, net als Wmo, belegd bij de gemeente Bernheze. Het proces uitkeringen in geld is belegd bij gemeente Meierijstad. Het RIOZ is op onderdelen nog wel betrokken binnen het proces jeugdzorg. Wij adviseren de onderlinge verantwoordelijkheden uiteen te zetten, het proces verder te formaliseren en uitgevoerde controles zichtbaar vast te leggen. Ten tijde van de controle was er nog geen VIC uitgevoerd voor dit proces als gevolg van uitval van personeel.	→
Verbonden partijen			n.v.t.	Binnen dit proces is sprake van de minimaal noodzakelijke functiescheiding. Er is geen sprake van (zichtbare) controlemaatregelen. De gemeente beschikt niet over een nota verbonden partijen en hanteert geen eigen beleid in aanvulling op de regionale kadernota. De gemeenteraad wordt middels de paragraaf verbonden partijen in de begroting en de jaarrekening geïnformeerd. Tevens besluit de gemeenteraad over toetreding van andere gemeenten tot een gemeenschappelijke regeling. Het proces is ongewijzigd ten opzichte van voorgaand jaar.	→

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

4. Bevindingen IT-beheer

4.1 IT-beheer

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

Beoordeelde systemen:
- Key2Finance

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 ICT-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 onbeheerste wijzigingen, 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 Key2Finance. Dit om de impact van de risico's van onbeheerste wijzigingen, ongeautoriseerde handelingen en verstoringen te kunnen vaststellen voor die systemen die gekoppeld zijn aan de voor ons relevantie processen en posten (zie **hoofdstuk 3**).

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

Op het moment dat de intern getroffen algemene IT-beheersmaatregelen rondom de applicaties in scope niet (bewijsbaar) voldoende aanwezig zijn, zijn in het kader van de controle van de jaarrekening 2022 aanvullende (gegevensgerichte) werkzaamheden noodzakelijk om aan te tonen dat er zich geen risico's of fouten hebben voorgedaan.

Wij hebben geen vergelijking gemaakt in hoofdstuk 4.2 met de IT General Controls van voorgaand jaar, omdat dit een andere applicatie betrof.

4.2 Bevindingen IT-beheer | Key2Finance (K2F)

Logische toegangs-beveiliging K2F (criteria 2,4,5) zijn (deels) ontoereikend

Change management is in opzet beschreven

Back-ups vinden dagelijks plaats en maandelijks volgt een full back-up van de database. Het was verder niet mogelijk om documentatie omtrent de uitgevoerde restoretest aan te leveren

PROCES	2022	2021	KORTE OMSCHRIJVING BEVINDINGEN
Logische toegangsbeveiliging			
1. Procedure autorisatiebeheer	●	n.v.t	Gezien het aantal gebruikers in K2F en de rollen die toegewezen worden (Budgethouder of kredietbeheerder) is het proces als akkoord bevonden.
2. Periodieke controle op juistheid ingerichte autorisaties	●	n.v.t	Er is geen formele en gedocumenteerde periodieke review uitgevoerd op de juistheid van autorisaties in K2F aan de hand van een gedocumenteerde normpositie. Daarbij is er geen vastlegging van eventuele uitzonderingen en follow-up documentatie beschikbaar.
3. Identificatie van gebruikers voor toegang tot systemen en data	●	n.v.t	Er is één generiek account geïdentificeerd. Dit betreft een beheeraccount van Centric.
4. Authenticatie	●	n.v.t	De wachtwoordeisen voldoen op de punten complexiteit en minimale leeftijd wachtwoord niet aan de BDO Best Practice.
5. Administrator- en Superuser-accounts	●	n.v.t	In K2F zijn gebruikers met beheerrechten actief welke formeel werkzaam zijn vanuit de lijnorganisatie. Dit betreffen de gebruikers Jeannette van Hamond (Beleidsmedewerker) en Mark van Buul (Controller). Hierdoor kan mogelijk controle technische functiescheiding worden doorbroken.
Change management			
6. Wijzigingsbeheer	●	n.v.t	Changes worden door de externe beheerder doorgezet naar de productieomgeving, ook zonder formeel akkoord na testwerkzaamheden. Hierdoor zijn er workarounds gecreëerd waarbij is vastgesteld dat dit geen invloed heeft op de controle van de jaarrekening.
7. Gescheiden IT-omgevingen	●	n.v.t	Er is een gescheiden productie- en test omgeving beschikbaar voor de applicatie K2F. De productieomgeving waarbij ontwikkelaars geen toegang hebben tot de productieomgeving.
Continuïteit			
8. Fysieke toegangscontrole	●	n.v.t	Geen bevinding.
9. Back-up maatregelen	●	n.v.t	Op dagelijkse basis worden backups uitgevoerd en maandelijks volgt er een full backup van de database. Ook wordt er gemonitord op succesvol verloop van de backups.
10. Restore-test	●	n.v.t	Er is een volledige restoretest uitgevoerd in het huidig jaar, echter is het niet mogelijk om hier vastlegging/documentatie over aan te leveren.

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

4.3 Actuele IT- ontwikkelingen en onze natuurlijke adviesrol

Veranderende vraag van leveranciers-management

Beoordeling van contracten

Aanpak van cyberrisico's

Leveranciersmanagement

Sinds enkele jaren zien wij in de markt een verschuiving naar Software-As-A-Service (SaaS) applicaties. Wij hebben tevens begrepen dat het de strategie is van de gemeente Bernheze om zoveel mogelijk IT te outsourcen. Dit vergt andere competenties dan voorheen en brengt andere risico's met zich mee. Hoe weet u bijvoorbeeld dat leveranciers hun informatiebeveiliging adequaat hebben ingericht en daar ook naar handelen? En of u voldoende beschermt bent tegen een cyberaanval? Daarnaast krijgen wij steeds vaker de vraag of leveranciers daadwerkelijk hun KPI's nakomen en of hier wel op de juiste manier over gerapporteerd wordt. In het kader hiervan willen wij u op een tweetal punten wijzen.

Actualiteit van contracten

Wij zien dat veel organisaties langlopende contracten hebben met leveranciers maar deze overeenkomsten niet in alle gevallen worden bijgewerkt naar huidige inzichten vanuit de markt. Daarom adviseren wij om een beoordeling uit te voeren op de huidige contractuele afspraken en bijbehorende servicelevel overeenkomsten en daarbij vast te stellen in hoeverre deze nog actueel zijn. Bij deze evaluatie adviseren wij eveneens te kijken naar afspraken die gemaakt zijn ten aanzien van informatiebeveiliging en de maatregelen die uw leverancier heeft ingericht om cyberaanvallen en datalekken te voorkomen. Hiervoor bestaan verschillende vormen. Een veelvoorkomende variant is een assurance verklaring (zoals ISAE of SOC2 verklaring) waarin de leverancier inzicht geeft in de door haar getroffen maatregelen. Met de veranderende eisen en toenemende wet en regelgeving, inclusief verantwoording van en aan het management is het erg belangrijk dat de afspraken met leveranciers hierin meebewegen. Het is daarom aan u als gemeente Bernheze om periodiek de contractuele afspraken te evalueren.

Afspraken t.a.v. Cyberrisico's

Aanvullend hierop is het voor uw organisatie belangrijk om na te gaan of alle koppelingen en leveranciersaccounts die u momenteel in uw systemen heeft zitten nog wel allemaal nodig zijn. Uit een recent voorbeeld bij gemeente Buren is gebleken dat hackers via leveranciersaccounts gegevens buit hebben gemaakt. Om dit te voorkomen kunt u zelf maatregelen treffen door accounts te blokkeren op het moment dat deze niet gebruikt worden en strenge wachtwoordeisen in te richten. Hierdoor wordt het risico op ongeautoriseerd gebruik verlaagd.

5. Bevindingen interne controle

5.1 Verbijzonderde interne controle

Drie varianten van VIC:
- Voldoen aan COS 610
- Gegevensgericht
- Geen VIC

VIC en Three Lines

Diverse voor- en nadelen voor inrichting VIC

Data-analyse en process mining steeds vaker toegepast

Verbijzonderde Interne Controle

De afgelopen jaren is veel discussie geweest over de eisen die gesteld moeten worden aan de onafhankelijkheid, positie en kwaliteit van de Verbijzonderde Interne Controle (VIC) en de wijze waarop organisaties en accountants hierin kunnen samenwerken. Wij onderscheiden hierbij een aantal varianten / situaties voor een organisatie:

1. De VIC voldoet aan de eisen van COS 610
2. De VIC werkt samen met de accountant in de uitvoering van gegevensgerichte controles (handmatig of op termijn via data-analyse en/of process mining)
3. De organisatie kiest er voor om geen VIC uit te voeren of besteed dit uit (accountant, derde partij)

De inhoudelijke invulling van de VIC (3e Lijn) hangt sterk samen met de vraag of de 1e en 2e lijn toereikend functioneren. Aan bovengenoemde varianten zijn diverse voor- en nadelen verbonden, die wij hier kort zullen toelichten. Daarbij is het van belang dat de gemeente Bernheze een bewuste keuze maakt, rekening houdend met de ambities, specifieke situatie / fase waarin de organisatie zich bevindt, beschikbare capaciteit, kosten versus baten, etc.

1. **AD 1) VIC voldoet aan COS 610**
   De COS 610 zijn controlestandaarden van accountants waarin de eisen / voorwaarden zijn uitgewerkt, waaraan de VIC moet voldoen teneinde hier als accountant gebruik van te kunnen maken. Hoewel dit controlestandaarden van accountants zijn, kunnen deze ook goed als norm voor de gemeente worden toegepast. De voorwaarden gaan onder meer over de onafhankelijkheid en positie in de organisatie, de kwaliteit van medewerkers, de kwaliteitsprocedures van de VIC, de communicatie en rapportages en de uitvoering van de werkzaamheden. Als een organisatie in staat is aan deze eisen te voldoen, betekent dat (zeer waarschijnlijk) ook dat de VIC zodanig is ingericht, dat deze gedurende het jaar grip houdt op het functioneren van de interne beheersing in de 1e en 2e lijn. Als accountant kunnen wij dan beperktere reviews doen op de werkzaamheden van de VIC.

2. **Ad 2) VIC werkt samen met accountant en voert gegevensgerichte controles uit**
   Indien een organisatie niet kan voldoen aan COS 610, kan nog steeds wel op een efficiënte wijze worden samengewerkt met de accountant. De VIC toetst dan, op basis van selecties en werkprogramma's van de accountant, achteraf de belangrijke beheers-maatregelen. In deze situatie moet de accountant alle werkzaamheden zelfstandig beoordelen en reperformen. Steeds vaker zien wij dat deze controles plaatsvinden op basis van data uit geautomatiseerde systemen en applicaties; de zogenaamde data-analyse en/of process mining.

3. **Ad 3) De VIC wordt uitbesteed aan een externe accountant of derde partij**
   Steeds vaker zien wij dat (kleinere) organisaties de VIC uitbesteden omdat ze de kennis of capaciteit niet hebben, de continuïteit en kwaliteit van de VIC moeilijk kunnen borgen en het ook niet als kernactiviteit zien. Daarmee verdwijnt de 3e lijn en nemen beheersmatige risico's toe, maar worden wel directe personeelskosten bespaard. In geval van een ontwikkeling naar een verantwoording omtrent de rechtmatigheid door het college is dit vanzelfsprekend geen optie meer. In dat geval worden bij deze optie de kosten van externen derhalve hoger.

5.1 Verbijzonderde interne controle

Eisen COS 610 niet realistisch

Samen met de gemeente Bernheze concluderen wij dat het op dit moment niet realistisch om te voldoen aan de eisen van de COS 610 c.q. dit op korte termijn ook niet het streven is. Wel is de kwaliteit zodanig dat in goede samenwerking in belangrijke mate gebruik kan worden gemaakt van de door de VIC (in overleg met ons) voorbereide werkzaamheden; ofwel de tweede variant. In lijn met voorgaande jaren rapporteren wij vanuit dit uitgangspunt met betrekking tot de Verbijzonderde Interne Controle (VIC) van de gemeente Bernheze als volgt:

Het interne controleplan wordt jaarlijks geactualiseerd en bevat een risicoanalyse per proces. Deze resulteert in een evaluatie met de gevonden fouten en bevindingen

- Gemeente Bernheze kent geen afzonderlijke afdeling of functionaris(sen) die als VIC worden aangemerkt. Binnen het team financiën fungeert één medewerker als coördinator interne controle. De interne controles op de verschillende processen worden gemonitord door uw financieel beleidsmedewerkers en medewerkers financiële administratie.
- De interne controles worden uitgevoerd op basis van het intern controleplan dat jaarlijks wordt geactualiseerd. In het intern controleplan is per proces een risicoanalyse opgesteld, zijn het aantal te controleren items benoemd en is per proces een werklijst aanwezig. Het aantal te controleren items is niet gebaseerd op de financiële stroom van het proces en de risicoanalyse. Verdere professionalisering kan nog plaatsvinden door de financiële stromen per proces in kaart te brengen en te koppelen aan de risicoanalyse, de processen in scope en het aantal te controleren items op basis van deze financiële stromen te definiëren en de processen te koppelen met het normenkader.
- Naar aanleiding van de uitgevoerde interne controles worden rapportages opgesteld met bevindingen en aanbevelingen op basis van het format zoals is opgenomen in het controleplan. Deze rapportages worden vervolgens gereviewed door en besproken met de coördinator interne controle. De coördinator interne controle verzorgt de verdere communicatie van de rapportages en houdt de voortgang van de uitgevoerde interne controles bij. De lijst met aanbevelingen wordt 2 maal per jaar gedeeld met het Managementteam.

Meerwaarde van de VIC voor de organisatie kan nog worden vergroot

Daarnaast geldt als constatering dat de VIC in de uitvoering van haar werkzaamheden nu primair gericht is op het uitvoeren van de in het jaarplan opgenomen (gegevensgerichte) testaantallen. In onze optiek kan de meerwaarde van de VIC voor de organisatie nog worden vergroot door ‘aan de voorkant’ nog meer expliciet aandacht te geven aan de opzet en inrichting van de AO/IB per proces alsmede de advisering daaromtrent (systeem-procesgericht).

Uitval van de VIC coördinator

Door uitval van een medewerker verantwoordelijk voor de VIC was het niet gelukt om alle interne controles uit te voeren conform planning. Voor slechts vijf materiële processen die relevant zijn voor de jaarrekeningcontrole (GREX, verhuur en pacht, personeelskosten, bouwleges en inkopen en betalingen) waren de interne controle over het eerste half jaar conform planning uitgevoerd. De VIC vormt in uw interne organisatie de laatste mogelijkheid om getrouw- en rechtmatigheidsfouten tijdig te detecteren en, waar mogelijk, te corrigeren. De gemeente loopt het risico dat fouten die niet meer gecorrigeerd kunnen worden (met name voor de rechtmatigheid) ook niet tijdig worden gesignaleerd of bijgestuurd. Vooruitkijkend naar de rechtmatigheidsverantwoording vanaf 2023 is dit een punt van aandacht binnen de gemeente Bernheze.

Kort samengevat zouden wij verwachten dat de VIC zich, alvorens over te gaan tot het uitvoeren van de testaantallen, ook richt op het vastleggen / uitwerken van de procesbeschrijvingen en het uitvoeren en documenteren van de omvattende lijncontroles per proces. De testwerkzaamheden zouden zich vervolgens liefst 1:1 moeten verhouden tot de binnen de verschillende processen geïdentificeerde ‘key-controls’ of beheersmaatregelen.

Bijlage

A. Detailbevindingen IT-beheer

A.1 Periodieke controle op juistheid ingerichte autorisaties

Bevinding	Er vindt geen zichtbaar gedocumenteerde review op juistheid en actualiteit van rechten plaats.	KANS: laag
Jaar van constatering	2022	IMPACT: middel

Onze bevinding	Op dit moment vind t er geen zichtbaar gedocumenteerde review op juistheid en actualiteit van rechten plaatst waarbij tevens een follow-up zichtbaar is gedocumenteerd.
Risico	Het risico bestaat dat er gebruikers in de applicatie aanwezig zijn die op basis van functie niet over de juiste rechten beschikken. Hierdoor kunnen (mogelijk) ongeautoriseerde handelingen worden verricht.
Onze aanbeveling	Een halfjaarlijkse controle van elke gebruiker met de daarbij behorende rechtenset. Hierbij dient dit vergeleken te worden met de rechten die volgens indienstformulier toegekend moeten worden. Daarnaast is het van belang om verschillen te documenteren en de follow-up van deze constatering vast te leggen.
Reactie management	

A.2 Authenticatie

Bevinding	Authenticatie	RISICO: middel
Jaar van constatering	2022	IMPACT: laag

Onze bevinding

Op basis van systeemwaarnemingen hebben wij vastgesteld dat de volgende wachtwoordvereisten worden afgedwongen voor Key2Finance :

WACHTWOORDINSTELLINGEN	KEY2FINANCE (via Active Directory)
Minimale wachtwoordlengte	8 karakters
Wijzigingsfrequentie	90 dagen
De laatste 5 wachtwoorden mogen niet hergebruikt worden	Ingesteld
Het account wordt na # foutieve inlogpogingen geblokkeerd	3 foutieve inlogpogingen
Wachtwoordcomplexiteit	**Nee**
Initiële wachtwoordwijziging	Afgedwongen
Minimale wachtwoordduur	Niet ingesteld

Het ingestelde wachtwoord voor K2F voldoet op de eisen wachtwoordcomplexiteit en minimale wachtwoordduur niet aan de BDO Best practice. Echter is 2FA ook ingesteld voor alle gebruikers die van buiten de organisatie verbinding maken met de omgeving van Bernheze. Hierdoor is deze bevinding als laag ingeschaald.

Risico

Gemeente Bernheze loopt op basis van het ontbreken van adequate wachtwoordinstellingen in Key2Finance het risico dat wachtwoorden makkelijk te raden zijn. Hierdoor kan (potentieel) ongeautoriseerde handelingen worden uitgevoerd.

Onze aanbeveling

Gemeente Bernheze beschikt over een gedocumenteerd wachtwoordbeleid. De wachtworodeisen beschreven in dit document zijn voldoende aan de BDO best practice. Wij raden derhalve aan om de wachtwoordinstellingen van de Active Directory gelijk te trekken aan het interne wachtwoordbeleid.

Reactie management

A.3 Administrator- en Superuser-accounts

Bevinding	ADMINISTRATOR- EN SUPERUSER-ACCOUNTS TOEGEKEND AAN EINDGEBRUIKERS	RISICO: Middel
Jaar van constatering	2022	IMPACT: Middel

Onze bevinding	Wij hebben vastgesteld dat gebruikers met beheerrechten in de applicaties Key2Finance, formeel werkzaam zijn vanuit de lijnorganisatie. ▶ Voor Key2Finance hebben wij twee beheeraccounts vastgesteld van medewerkers werkzaam in de lijnorganisatie.
Risico	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 genaamde accounts dat met deze accounts ongeautoriseerde wijzigingen worden doorgevoerd, waarnaar op basis van naamgeving niet te achterhalen is wie deze wijzigingen heeft doorgevoerd.
Onze aanbeveling	Het verdient aanbeveling om het aantal beheeraccounts accounts binnen de applicaties zoveel mogelijk in te perken. Tevens bevelen wij aan 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, loginstellingen, het installeren van updates) te centraliseren bij de ICT-afdeling.
Reactie management	

A.4 Wijzigingsbeheer

Bevinding	WIJZIGINGSBEHEER UPDATES K2F	RISICO: laag
Jaar van constatering	2022	IMPACT: gemiddeld

Onze bevinding	De wijzigingen worden geïnitieerd vanuit de leverancier en dienen vervolgens vanuit de gemeente Bernheze door eindgebruikers te worden getest. Wij hebben begrepen dat de wijzigingen voor K2F worden doorgezet in productie zonder een formeel akkoord vanuit de gebruikersorganisatie. Hierdoor zijn er noodzakelijke workarounds gevonden zodat de processen door kunnen gaan zoals dit zou moeten. Doordat er workarounds zijn opgesteld ziet de externe beheerder geen noodzaak om eventueel bugs op te lossen en moet Bernheze wachten tot de volgende standaard update.
Risico	Het risico bestaat dat changes worden doorgevoerd zonder dat deze uitvoerig getest zijn. Hierbij kunnen bugs ontstaan in de productieomgeving waarbij (mogelijk) functionaliteiten niet meer juist werken.
Onze aanbeveling	Het verdient aanbeveling om een procedure voor wijzigingsbeheer te beschrijven en te hanteren voor K2F. Hierbij dient ook aandacht te worden geschonken aan het testen en akkoord geven om een update/change in productie te nemen. Daarnaast zal er overleg moeten plaatsvinden over de procedure waarbij de externe beheerder eventuele updates/changes doorzet naar productie.
Reactie management	

A.5 Restore-test

Bevinding	Geen gedocumenteerde restore-test	RISICO: laag
Jaar van constatering	2022	IMPACT: hoog

Onze bevinding	Er is verklaard dat er een restore-test is uitgevoerd in het huidig boekjaar. Echter is hiervan gen documentatie beschikbaar waardoor wij geen oordeel kunnen geven over de juistheid van de uitgevoerde restore-test.
Risico	Doordat er geen documentatie beschikbaar is over het uitvoeren van een restore-test bestaat het risico dat de restore niet juist of volledig is uitgevoerd. In dat geval zou dit betekenen dat back-ups niet te restoren zijn.
Onze aanbeveling	Het is aan te bevelen om documentatie op te maken van wat en wanneer een volledig restore heeft plaatsgevonden en wat hiervan de bevindingen zijn geweest.
Reactie management	

bdo.nl