

30-11-2021

Bron: Geactualiseerde position papers van het management

Memo interne beheersing

In de managementletter worden een aantal bevindingen gerapporteerd, waarover de gemeente Meppel in het verleden al een standpunt heeft ingenomen.

Dit zijn (zie ML-2021, pag.38 e.v.):

1. Naleven aanbestedingsregels.
2. Prestatielevering inkoop.
3. Beheer crediteurenstamgegevens.
4. Controle verhuur.
5. Logische toegangsbeveiliging.
6. Wijzigingenbeheer updates.
7. IT continuïteit.

Daarnaast zijn we bezig een standpunt te ontwikkelen over (zie ML-2021, pag.13):

8. Afkoopsommen grafrechten.
9. Materiële vaste activa en asset management.

Het management
Ruben Zwart
Gerben Aukema

1. Naleven aanbestedingsregels

Aanleiding

Naar aanleiding van de managementletter van de accountant is deze position paper opgesteld. In de managementletter is de volgende opmerking opgenomen:

Vanuit het proces aanbestedingen is het van belang voor de gemeente Meppel om in het inkoopproces (prospectief) een controle uitte voeren voor het inkoopbeleid. Hierbij kan de Gemeente Meppel dan op basis van de inschatting van inkopen (op basis van een inkoopkalender / contractenregister) een gedegen afweging in het aanbestedingsproces maken welke vorm van aanbesteding gevolgd moet worden. Bij de uitvoering van de interim-controle van de Gemeente Meppel is geconstateerd dat de controle op al dan niet aanbesteden niet als een afzonderlijke processtap in het inkoopproces wordt afgedwongen en zichtbaar wordt vastgesteld en vastgelegd.

Wij verzoeken de gemeente Meppel een standpunt in te nemen over het in het proces opnemen van deze controlemaatregel. Indien de gemeente Meppel dit niet voornemens is en jaarlijks de spendanalyse uitvoert, zullen wij deze bevinding de komende jaren niet opnieuw rapporteren.

Standpunt Meppel

1. Vanuit Meppel zijn wij niet voornemens om het inkoopproces helemaal af te kaderen. Dit zou moeten betekenen dat alle inkoopfacturen middels een verplichtingen-administratie moet lopen. Dan zou in het werkproces bij iedere aangemaakte verplichting bij een bepaald grensbedrag een inkoper in de lijn moeten zitten. Dit is voor de omvang van de gemeente Meppel niet haalbaar.
2. Jaarlijks worden door het Cluster Inkooppresentaties en voorlichtingen gegeven aan alle teams over het verloop van de inkoopprocedures. Ook is er tussentijds periodiek overleg met teammanagers, budgethouders en projectleiders.

Werkwijze

1. Eind november van elk kalenderjaar wordt er een inkoopkalender opgesteld voor het daaropvolgende jaar.
2. Vanaf € 15.000 is het verplicht om voorafgaand aan de start van een aanbesteding een digitaal startformulier in te vullen. Op basis van dit startformulier wordt de aanbesteding door het Cluster Inkoop geregistreerd in het aanbestedingsregister.
3. In 2021 is de capaciteit van de cluster inkoop met de uitbreiding van twee inkoopadviseurs (2fte) en één contractmanager (1 fte) – allen vaste formatie - vergroot.
4. Begin 2022 wordt een nieuw contractmanagementsysteem inclusief een module spendmanagement geïmplementeerd zodat real-time bestedingen inzichtelijk zijn.

2. Prestatielevering inkoop

Aanleiding

Naar aanleiding van de managementletter van de accountant is deze position paper opgesteld. In de managementletter is de volgende opmerking opgenomen:

Binnen het proces inkopen is het van belang voor de Gemeente Meppel dat lasten zowel getrouw als rechtmatig zijn. Onderdeel van het toetsen van de getrouwheid en rechtmatigheid van inkopen is het vaststellen dat de prestaties, behorende bij de geautoriseerde en geboekte facturen, ook daadwerkelijk zijn geleverd. Ten tijde van de interim-controle van de gemeente Meppel is geconstateerd dat de toetsing van prestatielevering niet als een afzonderlijke processtap wordt afgedwongen en zichtbaar is vastgesteld en vastgelegd.

Advies BDO

Ten aanzien van de prestatielevering, voeren wij een detailcontrole uit, welke meeloopt in de detailcontrole op inkopen. Hierbij dient de prestatie door de gemeente aangetoond te worden, c.q. aannemelijk gemaakt te worden.

Wij verzoeken de gemeente Meppel een standpunt in te nemen over het in het proces opnemen van deze controlemaatregel

Standpunt Meppel

1. Meppel is momenteel zoekende in de diepgang van de vastlegging. Momenteel wordt er in de lijn reeds autorisatie uitgevoerd door een prestatieakkoordverklaarder (2e paar ogen). Echter wordt dit niet vastgelegd middels brondocumentatie. Het lastige is dat er veelal sprake is van voorschotfacturen en energienota's etc. waarbij het lastig is om de prestatie ook daadwerkelijk te onderbouwen met brondocumentatie. In de lijn zit voldoende functiescheiding ingebouwd. In de toekomst wordt nog gekeken of er bij een bepaald grensbedrag brondocumentatie wordt uitgevoerd.
2. Ieder jaar kunnen wij zonder al te veel moeite de prestatielevering op basis van de deelwaarneming opleveren. Dit geeft ons genoeg vertrouwen om erop te steunen dat de PAV'er voldoende onderbouwing heeft om het digitale akkoord te geven.

Argumenten

- Functiescheiding zit goed in het systeem verwerkt.
- Budgethouders zijn verantwoordelijk voor hun eigen budgetten. Wanneer er continu boekingen op de kostenplaatsen worden geboekt gaat dat opvallen.
- Ieder jaar wordt voor de accountantscontrole een selectie gedaan op de inkoopfacturen.
- Veel facturen is lastig om daar een juiste onderbouwing voor aan te leveren als het gaat om voorschotnota's, energienota's etc

3. Beheer crediteurenstamgegevens

Aanleiding

Naar aanleiding van de managementletter van de accountant is deze position paper opgesteld. In de managementletter is de volgende opmerking opgenomen:

Wij hebben geconstateerd dat er een gedeeltelijke opvolging heeft plaatsgevonden.

- 1. De gemeente voert vanaf dit jaar een controle uit op de mutaties in de crediteurenstamgegevens voordat betaling plaatsvindt. Wat ons betreft is dit het juiste moment voor uitvoering van deze controle en een verbetering ten opzichte van vorig jaar. Voor de controle van de gewijzigde crediteurenstamgegevens wordt de binnengekomen factuur gebruikt. Naar onze inschatting blijft hiermee nog een restrisico bestaan, omdat een onrechtmatig gewijzigde crediteurenstamgegeven naar alle waarschijnlijkheid gevolgd zal worden door een factuur met het onjuiste crediteurengegeven.*
- 2. Tevens constateren wij dat de medewerkers welke de eerste handtekening in het systeem kunnen zetten, de crediteurenstamgegevens kunnen muteren en nieuwe crediteuren kunnen aanmaken. Hierbij is geconstateerd dat zij mogelijkheid hebben om facturen om de standaard routing heen op het budget van een budgethouder te zetten en te verwerken tot en met de eerste handtekening in het betaalpakket (BNG).*

Standpunt Meppel

1. Wij erkennen het risico dat een medewerker van de administratie debiteuren/crediteuren een crediteur en bankrekening kan aanmaken, een factuur erop kan boeken en een eerste handtekening kan zetten. Een echte waarborg is er niet. De tweede handtekening bekijkt wel de factuur, echter gaat niet terug naar de bron. Vanuit de cluster inkoop gaan we in 2022 onderzoek doen naar de mogelijkheid om het proces van muteren op crediteurenstamgegevens zodanig in te richten dat dit niet meer mogelijk is.

4. Controle verhuur

Aanleiding

Naar aanleiding van de managementletter van de accountant is deze position paper opgesteld. In de managementletter is de volgende opmerking opgenomen:

Bevinding 2016

De gemiddelde opbrengsten voor pachten en huren bedraagt ruwweg € 2,5 miljoen. De gemeente Meppel heeft een controle ingeregeld om de juistheid van de huurprijzen te waarborgen.

Een dergelijke controle is voor de volledigheid van het aantal objecten niet ingeregeld.

Tevens vindt er door de gemeente geen controle plaats op eventuele leegstand, om vast te stellen dat de verhuuropbrengsten volledig zijn.

Standpunt Meppel

De gemeente Meppel is zich bewust van het feit dat het risico zich mogelijk voor doet dat er panden in eigendom zijn die verhuurd zouden kunnen worden. Echter het risico is zeer beperkt.

We kiezen er voor om geen jaarlijkse controle uit te voeren. Voor het jaar 2020 hebben wij een integrale controle gedaan op de volledigheid van de lijst in vergelijking met de BAG. Deze controle zal 1x in de 2 jaar uitgevoerd worden.

Opvolging

2019

De grootste panden van de gemeente zijn bekend binnen de gemeente. Echter of de lijst volledig is welke gehanteerd wordt is de vraag. Gezien het geringe risico hebben wij besloten om een risicoanalyse te maken. Hierbij kiezen wij ervoor om vanuit een lijst van de BAG de 10 grootste objecten (van de 58) te controleren of deze juist in het vastgoedboek staan. Hiermee hebben wij 41 mln. van de in totaal 55 mln. aan taxatiewaarde gecontroleerd.

Vanuit de BAG dient gewerkt te worden met een peildatum. De peildatum 2020 wordt bekeken met de stand per 2020 vanuit het vastgoedboek.

2020

Vanuit de BAG/WOZ medewerkers van de gemeente Meppel is een lijstwerk opgevraagd met de panden welke in eigendom zijn van de gemeente Meppel. Het betreffen in totaal 58 objecten. Deze objecten zijn in zijn geheel gecontroleerd door Anita Albers. Resultaat 1 woning aan Zetsel, geen eigendom gemeente, wel in lijst.

2021

Naar aanleiding van de GBK check (in 2020) gaan onderzoeken wat de status is van de panden die niet bekend zijn bij afdeling vastgoed. Resultaat van het onderzoek wordt dan vermeld in de eerst volgende IC rapport.

Dit onderzoek is niet uitgevoerd door team vastgoed (geen capaciteit).

Gepland voor 2022

1. In 2022 de 2-jaarlijkse controle uitvoeren van de lijst BAG met vastgoedboek en opdracht laten formuleren voor het instellen van een vervolgonderzoek.
2. In 2022 een risicoanalyse met werkwijze opstellen, samen met IC en adviseur vastgoed, voor nieuwe initiatieven die niet bekend zijn vastgoed, maar wel financiële verplichtingen kennen.
3. In het overzicht van de nota-opdracht huur bedrijfspanden en huur parkeerplaatsen ook de leegstand zichtbaar maken.

- 5. Logische toegangsbeveiliging
- 6. Wijzigingenbeheer updates
- 7. IT continuïteit

Inleiding

Informatisering binnen Meppel is sterk in ontwikkeling. Er is geconstateerd dat capaciteit ontbreekt en wij risico's lopen. Er is daarom een meerjarige aanpak opgesteld om Informatisering sterk te verbeteren. Dit heeft ook gevolgen voor de mogelijkheden om in de toekomst opvolging te geven aan de conclusies uit de IT audit.

Bij de interim controle van de accountant wordt de risico inschatting en controle aanpak geformuleerd. Op basis van de uitkomsten wordt er gekeken of bepaalde processen een verhoogd risico hebben. Ook wordt er gekeken naar de IT omgeving van de gemeente.

Wanneer processen perfect ingeregeld zijn in de digitale workflow kan de accountant ervoor kiezen om systeemgericht te controleren in plaats van gegevens gericht. Systeemgericht controleren wil zeggen dat de accountant enkel waarnemingen verricht om het systeem te testen. Om systeemgericht te controleren dient een IT omgeving aan veel eisen te voldoen. Ieder jaar rapporteert de accountant dezelfde opmerkingen en geeft de gemeente Meppel aan dat ze tevreden zijn met de inrichting in huidige situatie. Vanuit de accountant is het verzoek gekomen om een positie in te nemen in de ambitie van de gemeente Meppel. De accountant streeft naar een systeemgerichte controle, maar heeft ook geen probleem op een gegevensgerichte controle. Momenteel sluit een gegevensgerichte controle het beste aan, maar de ambitie hierin zou op termijn nog kunnen verschuiven naar systeemgericht.

Probleemstelling

De accountant rapporteert altijd naar de meest ideale situatie. De gemeente Meppel moet de lat gaan bepalen waarop de accountant rapporteert en wanneer het ambitieniveau bereikt is, moet dat kenbaar gemaakt worden. De accountant zal dit dan accepteren en hier niet meer over gaan rapporteren. Dit scheelt ieder jaar accountantskosten. In Nederland zijn er slechts enkele gemeenten waarbij de IT zo is ingericht dat een accountant een systeemgerichte controle kan uitvoeren.

Uitvoering

De bevindingen van de accountant zijn elk jaar geëvalueerd en daar waar nodig het beleid of maatregelen bijgesteld. De accountant richt zijn audit op twee systemen: Key2Financiën en Suite4Sociaal Domein, beide van Centric. Beide systemen zijn kwetsbaar omdat er grote hoeveelheden financiële stromen doorheen gaan.

Conclusie

Wij waarderen de rapportage en conclusies van de IT audit van de accountant. Het realiseren van verbeteringen is in de huidige schaal van Meppel met de grootte van het huidige team niet haalbaar. Met de meerjarenaanpak voor Informatisering (ICT) worden de komende jaren stappen gezet in onze processen en het beheer van onze systemen. Vanuit deze nieuwe ontwikkelingen achten wij het logisch dat de IT audit jaarlijks wordt uitgevoerd om een goed beeld te houden van onze risico's en de ontwikkeling in het mitigeren hiervan. Voorlopig zal een gegevensgerichte audit het meest passend blijven.

Bevindingen accountant

Hieronder staan de bevindingen van de accountant per applicatie. Alleen de bevindingen die de accountant als een risico heeft benoemd, zijn vermeld. Let op dit zijn 2 pakketten, Key2Financiën en Suite4sociaal domein. Hierdoor kan het lijken alsof de bevindingen dubbel zijn.

Autorisatie

De gemeente heeft een formeel proces ingericht voor het toekennen, wijzigen en verwijderen van gebruikers en toegewezen autorisaties in K2F en SSD. In het verlengde hiervan zijn autorisatiematrices opgesteld, welke niet formeel zijn goedgekeurd door het management. Eveneens is de autorisatiematrix van K2F niet opgesteld op basis van organisatorische functies.

Ten behoeve van het toekennen van autorisaties wordt gebruik gemaakt van een autorisatieformulier waarbij een voorbeeldgebruiker wordt aangehouden en dus geen autorisatiematrix wordt gebruikt om rechten toe te kennen.

Om adequate procedures rondom het aanmaken, wijzigen en verwijderen van gebruikers met bijbehorende rechten in applicaties te borgen, dient periodiek een review, op basis van een autorisatie-/functiescheidingsmatrix plaats te vinden waarbij eveneens gecontroleerd wordt op de actualiteit van gebruikers en bijbehorende rechten. Dergelijke reviews zijn voor beide applicaties uitgevoerd. Wij hebben enkel niet kunnen vaststellen dat de gebruikerslijsten juist en volledig zijn gecontroleerd. Voorts beschrijft hoofdstuk 3.8 in 'Autorisatiebeleid gemeente Meppel' een werkwijze waarbij een rol voor de controller en CISO in het proces van periodieke review is vastgelegd. Dit hebben wij niet als zodanig vast kunnen stellen.

De gemeente Meppel maakt gebruik van de applicatie WieisWie om de juiste wachtwoordeisen af te dwingen op Windows Active Directory. Voor een aantal eindgebruikers in K2F en SSD hebben wij vastgesteld dat zij hebben ingelogd met een wachtwoord dat ouder is dan 40 dagen (hetgeen wordt afgedwongen in de source code van WieisWie).

- Momenteel wordt gewerkt aan het finaliseren van de autorisatiematrices voor zowel Key2Financiën als SSD, deze zullen door het management geautoriseerd worden. Voor het duurzaam borgen van processen rondom toegang(sbeheersing), autorisatie, wachtwoordbeleid en het uitvoeren van controles geldt dat een meerjarenplan ICT opgesteld, waarin o.a. dit punt is opgenomen. De financiering hiervan is in de meerjarenbegroting opgenomen.

Wijzigingenbeheer

De gemeente beschikt over een generieke procedure waarin het wijzigingenbeheerproces voor de applicaties K2F en SSD is vastgelegd. Een formele goedkeuring op deze procedure is niet zichtbaar vastgelegd. Wijzigingen voor K2F en SSD worden ontwikkeld door de leverancier waarnaar vervolgens releasenotes worden verstuurd naar de applicatiebeheerders. De applicatiebeheerders beoordelen de releasenotes op impact, echter zijn de beoordelingen op de releasenotes niet zichtbaar vastgelegd waardoor achteraf niet mogelijk is om vast te stellen of wijzigingen terecht of tijdig zijn doorgevoerd. Bovendien worden de testresultaten van K2F niet structureel vastgelegd en worden key-users niet betrokken bij de testwerkzaamheden.

Voor een willekeurig gekozen wijziging van SSD hebben wij niet kunnen vaststellen dat de meldingen naar aanleiding van het testen zijn opgelost alvorens de wijziging is doorgevoerd op de productieomgeving. Aanvullend is vastgesteld dat deze meldingen niet belemmerend waren om de wijziging in productie door te voeren.

- Een meerjarenplan voor ICT is opgesteld, waarin o.a. dit punt is opgenomen. De financiering hiervan is in de meerjarenbegroting opgenomen.

Toegang serverruimte

Toegang tot de serverruimte is toebedeeld aan gebruikers die deze toegang uit hoofde van functie niet benodigd hebben. Hiertoe rekenen wij onder andere de wachtdienst, generieke servicepassen en enkele medewerkers van de 24/7-dienst. Wij hebben begrepen dat de gemeente aanvullende maatregelen heeft genomen (zoals camera's) om dit risico te mitigeren, deze maatregelen vallen buiten de scope van onze audit.

- De toegang is inmiddels al verder ingeperkt en er wordt onderzocht of de toegang verder verkleind kan worden.

Periodieke restoretest

Ten tijde van de audit is nog geen periodiek restore/disaster recovery test uitgevoerd waarbij is getest of in geval van calamiteit middels een back-up, dan wel uitwijk, een volledig werkende productieomgeving kan worden hersteld. Wij hebben vernomen dat een dergelijke test voor Q4 2021 op de planning staat.

Tevens beschikt de gemeente nog niet over een formeel continuïteitsplan om vast te kunnen stellen of de productie-omgeving binnen de eisen van de bedrijfsvoering is hersteld in termen van maximaal toelaatbaar gegevensverlies en maximaal toelaatbare uitvalsduur (hersteltijd). Wij hebben vernomen dat dit beleid ontwikkeld wordt als onderdeel van het jaarplan 2022.

- Zie hiervoor de door BDO al gegeven toelichting.

8. Afkoopsommen grafrechten

(V&A 2015.40 en 2017.150)

Aanleiding

Naar aanleiding van de managementletter van de accountant is deze position paper opgesteld. In de managementletter is de volgende opmerking opgenomen (pag.13):

Graag attenderen wij u op de wet-en regelgeving rondom de afkoopbedragen inzake grafrechten. De ontvangen (afkoop)bedragen voor het grafonderhoud worden als bijdragen van derden beschouwd voor een al dan niet kostendekkende jaarlijkse dienstverlening. De ontvangen afkoopbedragen worden opgenomen in een voorziening ex artikel 44-2 BBV. De ontvangen afkoopsommen vormen een verplichting aan degene die de afkoopsom heeft betaald en zal door de gemeente aan het onderhoud van de betreffende graven moeten worden besteed. Derhalve is het vormen van een voorziening verplicht (BBV art. 44 lid 2). Het gaat hier om van derden verkregen middelen met een specifieke bestedingsplicht.

Wij vragen u om voorafgaand aan het opstellen van de jaarrekening 2021 te inventariseren of deze situatie bij uw gemeente van toepassing is.

Standpunt Meppel

<in ontwikkeling>

Werkwijze

Er is bij betrokken medewerker een uitvraag gedaan naar een overzicht van deze afkoopsommen. Op basis daarvan gaat Financien een impact analyse doen, zodat we bij de jaarrekening een standpunt kunnen innemen.

9. Materiële vaste activa en asset management

Aanleiding

Naar aanleiding van de managementletter van de accountant is deze position paper opgesteld. In de managementletter is de volgende opmerking opgenomen (pag.13):

Mede naar aanleiding van de ontwikkelingen in de BBV (zie 2.1), hebben wij kennis genomen van de paragraaf onderhoud kapitaalgoederen in de jaarrekening 2020 en de gemeente gevraagd een analyse op hoofdlijnen op te stellen over het assetmanagement is geregeldten aanzien de hoofdcategorieën van de gemeentelijke bezittingen. Op basis van de jaarrekening 2020 betreft dit dan met namen woonruimten, bedrijfsgebouwen, grond-, weg-en waterbouwkundige werken, vervoermiddelen en machines/installaties.

Wij adviseren / verzoeken de gemeente Meppel een goede analyse (position paper) te maken ter onderbouwing.

Standpunt Meppel

<in ontwikkeling>

Werkwijze

Diverse vragen uitgezet, wachten op antwoord; daarna analyse door Financiën, zodat we bij de jaarrekening een standpunt kunnen innemen.