



Concept Management letter

Gemeente Overbetuwe
Boekjaar 2019

Vertrouwelijk

Het College van Burgemeester en Wethouders
van de gemeente Overbetuwe
Postbus 11
6660 AA ELST

Zwolle, 14 november 2019

Geachte leden van het College,

Als onderdeel van de controle van de jaarrekening 2019 van Overbetuwe hebben wij de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing beoordeeld, teneinde onze controlewerkzaamheden in overeenstemming met Nederlands recht waaronder de controlestandaarden te kunnen bepalen.

De opzet, het bestaan en de werking van de interne beheersingsmaatregelen van de belangrijkste processen, inclusief de geautomatiseerde gegevensverwerking, in uw gemeente zijn beoordeeld en getoetst, zodat we een terugkoppeling kunnen geven over de betrouwbaarheid van de interne informatievoorziening en de jaarrekening.

Onze bevindingen zijn gebaseerd op de normale werkzaamheden in het kader van de jaarrekeningcontrole. Deze brief bevat daardoor niet alle onvolkomenheden in uw gemeente, die bij een eventueel uitgebreid en hierop specifiek gericht onderzoek naar voren zouden kunnen komen.

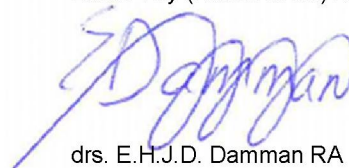
Zoals u zult begrijpen, is de management letter van nature kritisch. Wij rapporteren over de eventuele leemtes of mogelijkheden ter verbetering van de financiële en administratieve processen, de administratieve organisatie daarvan en de daarin opgenomen maatregelen van interne beheersing.

Op uw verzoek geven wij in deze management letter aan op welke wijze verbeteringen van de administratieve organisatie en de daarin opgenomen maatregelen van interne beheersing kunnen worden gerealiseerd. De aanbevelingen en oplossingsrichtingen zoals beschreven in deze management letter bieden u handvatten voor deze uitwerking.

Deze management letter is door ons opgesteld voor uw informatie en mag niet zonder onze uitdrukkelijke toestemming geheel of gedeeltelijk aan derden ter beschikking worden gesteld.

Wij danken u en uw medewerkers voor de samenwerking en zijn graag bereid tot het verstrekken van nadere toelichting.

Hoogachtend,
Baker Tilly (Netherlands) N.V.



drs. E.H.J.D. Damman RA

Inhouds- opgave

1. Management samenvatting	4
2. Bevindingen	10
3. Bevindingen IT beheersing	13
4. Attentiepunten jaareinde controle en overige aandachtspunten	19
5. Overige onderwerpen	24

Management samenvatting

1. Management samenvatting

1.1 Inleiding

Deze management letter bevat onze bevindingen die zijn gebaseerd op de onze werkzaamheden in het kader van de jaarrekening-controle voor het jaar eindigend op 31 december 2019. Deze werkzaamheden zijn dan ook niet gericht op het geven van een oordeel over de interne beheersing van uw gemeente als geheel.

Onze werkzaamheden bij de interimcontrole zijn een belangrijk onderdeel van onze risicoanalyse in het kader van de jaarrekeningcontrolecyclus 2019. Binnen uw gemeente zijn op diverse niveaus in de organisatie doelstellingen bepaald welke bijdragen aan de specifieke doelstellingen van de gemeente Overbetuwe als geheel. Om als gemeente te kunnen sturen op het behalen van deze doelstelling is een goede interne beheersing van groot belang. Deze draagt namelijk niet alleen bij aan het realiseren van de gestelde doelstellingen maar ook aan het op betrouwbare wijze verantwoording afleggen daarover. Kort gezegd: hoe meer effectieve waarborgen de interne beheersing bevat, hoe meer zekerheid er bestaat dat de door uw gemeente opgeleverde informatie (waaronder ook de jaarrekening) betrouwbaar is. Onze controlewerkzaamheden worden afgestemd op onze bevindingen alsmede onze inschatting van de risico's dat de jaarrekening een afwijking van materieel belang bevat als gevolg van fraude of fouten.

Voorgaand jaar hebben wij in onze rapportages diverse aanbevelingen benoemd ter verbetering van de bestaande administratieve organisatie. Wij zien dat uw organisatie inmiddels actief aan de slag is gegaan met het opvolgen van een aantal van deze bevindingen. Hierin zijn bewuste keuzes gemaakt. In deze management letter geven wij u een schriftelijke update van onze bevindingen omtrent de interne beheersing.

Voor de jaarrekeningcontrole onderkennen wij een aantal risicogebieden, die een verhoogd risico met zich meebrengen op een materiële fout in uw jaarrekening. Deze risicogebieden zijn hieronder weergegeven. Opname van het risicogebied in deze opsomming betekent overigens niet dat dit risico ook manifest wordt bij uw gemeente. Het is slechts bedoeld om aan te geven dat wij hier tijdens onze controle extra aandacht aan zullen besteden.

- Rechtmatigheid aanbestedingen;
- Betalingsverkeer (beheersing uitgaande geldstromen);
- Waardering en beheersing voorraden (grondexploitaties);
- Management override of controls - het risico op het doorbreken van interne beheersingsmaatregelen die anderszins effectief lijken te werken – door het management, de directie of het college (met name bij memoriaalboekingen en de oneigenlijke beïnvloeding van schattingsposten, i.c. voorzieningen).

Naast bovenstaande onderwerpen zullen wij in het kader van onze jaarrekeningcontrole 2019 tevens specifieke aandacht besteden aan:

- Prestatielevering inkopen en sociaal domein;
- Implicaties van de Notitie Grondbeleid in begroting en jaarstukken zoals gepubliceerd door de Commissie BBV in juli 2019.

1. Management samenvatting

1.2 Beeld interne beheersing

Uw gemeente beschikt over een kritische verbijzonderde interne controlefunctie die werkt vanuit een gestructureerd intern controleplan. De opvolging van eerder door ons genoemde verbeterpunten binnen de interne beheersing wordt intern gemonitord.

In onze voorgaande management letter hebben we gerapporteerd dat het intern controleplan steeds belangrijker zal worden als gevolg van het in de toekomst verplicht worden van een rechtmatigheidsverklaring door het college. Daarbij hebben wij aangegeven dat het intern controleplan, om als kader te kunnen dienen teneinde tijdig invulling te kunnen geven aan de rechtmatigheidsverklaring die vanaf 2021 verplicht wordt, nog wel doorontwikkeld moet worden. Belangrijke kwaliteitsimpulsen betreffen een opbouw waarbij gestart wordt met de financiële omvang van posten en stromen en het koppelen van deze posten en stromen aan relevante wet- en regelgeving. Het is van belang om per post en stroom de risico's concreet te maken, op basis van deze risicoanalyse ga je vervolgens bepalen wat de belangrijkste maatregelen (key-controls) zijn waar je gebruik van wilt gaan maken.

Daarnaast is het van belang om per post en stroom te bepalen of het mogelijk is om systeemgericht te controleren (werking van het proces) dan wel dat het noodzakelijk is gegevensgericht (output) te controleren.

1. Management samenvatting

1.3 Sociaal domein

Vanaf boekjaar 2015 is uw gemeente voor haar inwoners verantwoordelijk voor de Jeugdzorg, de Wet Maatschappelijke Ondersteuning (WMO) en de Participatiewet. De uitvoering van deze taken vindt plaats binnen de gemeente zelf. Daarnaast is de administratieve verwerking van de PGB's (verplicht) onder gebracht bij de SVB.

Prestatielevering

Voor het vaststellen van de levering heeft de gemeente zich sinds de introductie van het sociaal domein gebaseerd op het landelijk accountantsprotocol, de verwachting is dat ook de gemeente Overbetuwe voor 2019 nog in grote mate afhankelijk zal zijn van deze wijze van vaststellen van de prestatielevering. Wel zien wij hierin een belangrijke ontwikkeling binnen uw organisatie, de contouren van het interne controleplan staan inmiddels. Een belangrijke vervolgstap voor dit plan is het verder concretiseren van de risico's om vervolgens ook te kunnen bepalen welke werkzaamheden zullen worden uitgevoerd.

Als gevolg hiervan wordt de afhankelijkheid van de leveringsverklaringen voor de gemeente Overbetuwe steeds kleiner. Afgelopen jaar heeft de gemeente ad-hoc na afloop van het boekjaar nog aanvullende werkzaamheden uitgevoerd voor deelstromen binnen het sociaal domein, teneinde de onzekerheden als gevolg van ontbrekende leveringsverklaringen terug te brengen.

Het is van belang in de toekomst de processen op een dusdanige manier in te richten dat er niet meer ad-hoc achteraf maar gedurende het boekjaar reeds wordt vastgesteld dat de in rekening gebrachte zorg ook daadwerkelijk geleverd is. Hierbij is het van belang dat de gehanteerde controlemiddelen toetsbaar worden vastgelegd. Voorbeelden hiervan zijn de vastlegging van 'keukentafelgesprekken' en het inrichten van een adequate klachtenregistratie.

Voor sommige zorgvormen in de jeugdzorg (o.a. als gevolg van privacywetgeving) zal de gemeente echter niet in staat zijn om de levering met voldoende zekerheid vast te stellen, hierbij kan zij terugvallen op de leveringsverklaring vanuit het landelijk accountantsprotocol. Bij deze zorgvormen is het van belang zorgleveranciers vroegtijdig te benaderen en hen te verzoeken bij eventuele complicaties in het verantwoordingsproces naar de gemeente vroegtijdig te informeren.

Voor boekjaar 2018 heeft u gebruik gemaakt van de Toetspraktijk, indien u dit voor boekjaar 2019 weer gaat doen willen wij u erop wijzen dat het van belang is om op basis van de door de Toetspraktijk aangeleverde conclusies zelf een analyse te maken van de impact op de rechtmatigheid van de daarmee samenhangende lasten

Indicatieproces

Het goed beschreven en ingericht hebben van het indicatieproces leidt ertoe dat de gemeente zelf een goede administratie heeft van burgers in zorg. Voor zorg aan cliënten die via de gemeente toegang tot hulp ontvangen wordt dit ingericht met indicatiestellingen die in functiescheiding tot stand komen. Deze functiescheiding is binnen uw gemeente niet aanwezig, binnen de gemeente Overbetuwe is ervoor gekozen dat consulent zelfstandig bevoegd zijn voor het afgeven van een beschikking. Als gevolg hiervan zullen wij een aanvullende steekproef uitvoeren op het recht, de hoogte en de duur van de verstrekking vast te stellen.



1. Managementsamenvatting

1.4 Fraude en corruptie



Als onderdeel van onze controle hebben wij u verzocht inzicht te geven in uw inschattingsproces rondom de risico's dat de jaarrekening een materiële afwijking zou kunnen bevatten als gevolg van fraude. Hierbij gaat het om de aard, omvang en frequentie van deze inschattingen, het proces dat de directie daarbij hanteert en ook de communicatie daarover met het personeel en met het toezichthoudend orgaan.

Uit de gesprekken die wij met u hebben gevoerd en de vastleggingen die zijn gedaan blijkt het belang dat u hecht aan het vermijden en ontdekken van fraude. Wij hebben daarbij vastgesteld dat het periodiek opstellen en actualiseren van (fraude)risicoanalyses plaatsvindt en structureel onderdeel vormt van de interne beheersingsomgeving. Wij adviseren u deze lijn door te zetten en de huidige frauderisicoanalyse aan te vullen met de binnen de gemeente eventueel aanwezige corruptierisico's.

Van de accountant wordt op grond van de regels van de beroepsorganisatie NBA een professioneel-kritische houding verwacht ten aanzien van afwijkingen van materieel belang als gevolg van fraude. Ter invulling van deze houding zal de accountant een inschatting moeten maken van de frauderisico's, zich een beeld moeten vormen van de maatregelen van interne beheersing die de organisatie heeft getroffen om mogelijke fraudes van materieel belang te voorkomen en moeten bezien of deze maatregelen effectief zijn.

Wanneer sprake is van een aanwijzing voor fraude, zal de accountant dit moeten communiceren met, afhankelijk van de aard van de fraude, de direct leidinggevende, het college en, in sommige gevallen (fraude in de top van de organisatie) en wanneer onvoldoende herstelwerkzaamheden worden ondernomen, de raad.

Om invulling te geven aan de eerdergenoemde verplichting hebben wij een fraudediscussie gevoerd binnen het controleteam. Bij gesprekken met vertegenwoordigers van uw gemeente is het onderwerp fraude betrokken, waarbij wij de nadruk hebben gelegd op de eventuele mogelijkheden van materiële onjuistheden als gevolg van fraude in relatie tot de jaarstukken en op preventieve maatregelen daarbij. Van deze vertegenwoordigers hebben wij geen signalen ontvangen dat er onregelmatigheden zijn geconstateerd.

Daarnaast hebben wij conform onze beroepsregels zelfstandig werkzaamheden uitgevoerd die erop waren gericht om het risico van het 'omzeilen' van de interne beheersingsmaatregelen door het management te detecteren. Hoewel wij, zoals hiervoor beschreven, een kritische houding hebben ten opzichte van risico's van fraude, merken wij op dat onze controle niet specifiek gericht is op het ontdekken van fraude.

Tijdens de uitvoering van onze interimcontrole hebben wij geen aanwijzingen verkregen dat er sprake is geweest van fraude.

Management samenvatting

1.5 General IT

Uit onze IT-audit komt naar voren dat ook op de door ons geïdentificeerde aandachtsgebieden van automatisering wijzigingsbeheer en toegangsbeveiliging nog verbeteringen noodzakelijk zijn. Voor wijzigingsbeheer geldt dat veel handelingen op dat gebied niet geformaliseerd zijn in procedures en de uitkomsten van de handelingen ook achteraf vaak niet zichtbaar zijn anders dan dat wijzigingen zijn doorgevoerd. Wij adviseren u de procedures te beschrijven en daarbij specifiek aandacht te besteden aan de controleerbaarheid van de ingeregelde controlemomenten. Naast wijzigingsbeheer is toegangsbeveiliging relevant. We delen dit op in authenticatie en autorisatie. Uit de stoplichten valt op te maken in hoeverre we gebruik kunnen maken van de randvoorwaarden die binnen uw organisatie aanwezig zijn voor de controle. Voor onze detailbevindingen verwijzen wij naar hoofdstuk 3

	Netwerk	Civision Middelen
Authenticatie Door middel van authenticatie wordt geborgd dat de gebruiker zichzelf kan identificeren binnen een geautomatiseerde omgeving. Kort gezegd: de gebruiker toont aan dat hij/zij inlogt met een eigen persoonsgebonden account en daarmee is wie hij/zij claimt te zijn. Wij scharen onder dit onderwerp met name wachtwoordvereisten en herleidbaarheid van accounts.		
Autorisatie Op het gebied van autorisatie zijn verschillende vormen van diepgang te definiëren. Wat wij onderzoeken als het gaat om de randvoorwaarden rondom autorisatie, zijn de rechten die de mogelijkheid bieden om autorisatie-structuren te wijzigen en of deze rechten belegd zijn bij functionarissen met een onafhankelijke positie ten opzichte van de jaarrekening. Daarnaast is een effectieve procedure voor het wijzigen van rechten noodzakelijk.		
Wijzigingsbeheer Gedurende een (boek)jaar worden wijzigingen doorgevoerd in de IT-omgeving van uw organisatie. Wanneer deze wijzigingen een impact hebben op de functionaliteiten of rapportages die een rol spelen in de jaarrekening (en uw organisatie deze niet signaleert), heeft dit gevolgen voor de controlewerkzaamheden. Wij beoordelen dit onderdeel door te steunen op uw procedure of werkzaamheden uit te voeren op documentatie vanuit de leverancier.	N.V.T.	



Op dit moment voldoende



Vereist verbetering op korte termijn



Urgente verbetering vereist

2. Bevindingen

2. Bevindingen 2019

Bevinding	Risico	Aanbeveling	Gevolgen jaareindecontrole
Inkopen Binnen het proces inkopen geeft de Prestatie-akkoord-verklaarder akkoord voor de geleverde prestatie. Op dit moment is het onvoldoende herleidbaar op welke basis hij/zij de factuur autoriseert.	Hierdoor bestaat het risico dat er facturen betaald worden waarvoor geen prestatie geleverd is. Daarnaast is de controle van dit proces hierdoor onnodig tijdrovend.	Wij adviseren u om de vastlegging van de documentatie rondom het vaststellen van de prestatielevering te formaliseren en minimaal te laten vullen met de overweging van de akkoordverklaarder om de factuur te autoriseren	Als gevolg van het ontbreken van een adequate vastlegging rondom de prestatielevering dienen wij aanvullende gegevensgerichte werkzaamheden uit te voeren. Hierover zijn reeds afspraken gemaakt met de afdeling interne controle.
Sociaal domein Binnen uw gemeente zijn consultants gemandateerd om indicatiestellingen WMO en jeugd te verlenen. Als gevolg hiervan is er geen sprake van functiescheiding binnen het indicatieproces.	Hierdoor bestaat het risico op onrechtmatige lasten als gevolg van het onterecht verstrekken van een indicatie.	Wij adviseren u om functiescheiding aan te brengen in het indicatieproces.	Als gevolg hiervan zullen wij een aanvullende steekproef uitvoeren op het recht, de hoogte en de duur van de verstrekking vast te stellen.
Schattingsposten Omdat schattingen per definitie subjectief zijn, besteden wij in onze controle nadrukkelijk aandacht aan de onderbouwing en redelijkheid van de aannames. Op basis van specifieke kennis van de gemeente en haar omgeving worden effecten van de schattingen (voornamelijk voorzieningen en grondexploitatie) in de komende jaren ingeschat en wordt bepaald wat de omvang dan wel het verwachte resultaat zal c.q. moet zijn. De directie en college laten zich hierbij ondersteunen door specialisten. Op dit moment is onvoldoende zichtbaar wie welke controles uitvoert binnen dit proces.	Hierdoor ontstaat het risico op onjuiste waardering van schattingsposten in de jaarrekening.	Wij vragen uw aandacht voor het zichtbaar maken van interne beheersingsmaatregelen die uw gemeente heeft ingericht met betrekking tot het zorgvuldig tot stand komen van de schattingen. Voor de jaarrekeningcontrole is het belangrijk dat, een adequate onderbouwing beschikbaar is voor alle (mogelijk te vormen) voorzieningen voor verplichtingen, risico's, opbrengsten en kosten (middels een beschrijving van de schattingsmethoden, de uitgangspunten daarbij alsmede scenario-analyses en wie welke controles heeft uitgevoerd).	Wij hebben met de gemeente afspraken gemaakt om de belangrijkste schattingsposten en de daarbij behorende uitgangspunten voor aanvang van de feitelijke jaarrekeningcontrole te controleren. Op deze wijze wordt voorkomen dat het controleproces vertraging oploopt en wordt bereikt dat eventuele correcties tijdig verwerkt worden.

2. Bevindingen eerdere jaren en follow up

Bevinding	Risico	Aanbeveling	Status	Gevolgen jaareindecontrole
Personeel Jaarlijks worden de premiepercentages gewijzigd en ingevoerd in het salarispakket. In 2018 heeft de controle op juiste invoer van premiepercentages nog niet plaatsgevonden.	Het risico bestaat dat de premiepercentages onjuist zijn ingevoerd in het salarispakket. Dit heeft tot gevolg dat de mogelijkheid bestaat dat de afdracht loonheffing en sociale lasten niet juist zijn.	Voor 2018 de premiepercentages zoals die in de salarisadministratie zijn ingevoerd controleren op juistheid op basis van de door de belastingdienst uitgegeven premies en beschikkingen e.d. Daarnaast preventief controle op juistheid premiepercentages uitvoeren om risico op onjuiste afdracht loonheffing en sociale lasten te voorkomen.	● Afgerond Voor boekjaar 2018 is achteraf vastgesteld dat de juiste percentages gehanteerd zijn. Wij hebben vastgesteld voor boekjaar 2019 de premiepercentages zijn gecontroleerd in januari.	Geen impact op de jaarrekeningcontrole.
Treasury In het treasurystatuut is onder het hoofdstuk 'verantwoordelijkheden' opgenomen dat de externe accountant in het kader van haar reguliere controletaak de naleving van het treasurystatuut dient vast te stellen.	Het treasurystatuut maakt onderdeel uit van de normenkader. De gemeente is echter zelf primair verantwoordelijk voor het naleven van hetgeen opgenomen in het treasurystatuut. Het opnemen van de accountant als verantwoordelijke in interne beleidsdocumenten leidt af van deze verantwoordelijkheid en is derhalve niet wenselijk.	Wij adviseren u om bij de actualisatie van het treasurystatuut deze passage te laten vervallen	● Onderhanden Actualisatie treasurystatuut moet nog plaatsvinden. Planning was om dit voor 1 juli 2019 te realiseren. Huidig treasurystatuut is door de Raad vastgesteld. Insteek is om deze bevoegdheid bij het College B&W te beleggen. Wijziging van de financiële verordening staat ook op de planning. I.v.m. de samenhang hiermee is het vast stellen van een geactualiseerd Treasurystatuut vertraagd.	Geen impact op de jaarrekeningcontrole.
Treasury De liquiditeitsplanning van de gemeente wordt gemonitord door de medewerker treasury. Echter wordt de liquiditeitsplanning en de analyse hiervan niet gedocumenteerd. In het treasurystatuut staat echter wel vermeld dat er een liquiditeitsplanning aanwezig dient te zijn. Derhalve voldoet de gemeente niet aan de interne wet- en regelgeving.		Wij adviseren u de liquiditeitsplanning en de analyse hiervan te documenteren.	● Afgerond Er is zowel een jaarplanning van het lopende jaar, met onderverdeling in maanden, als een meerjarenplanning aanwezig. Van de analyse wordt geen rapportage gemaakt. Via P&C cyclus wordt via de paragraaf Financiering info aan de Gemeenteraad gemeld.	Geen impact op de jaarrekeningcontrole.

3. Bevindingen IT-beheersing

3. Bevindingen IT-beheersing

3.1 Algemeen

Veel handelingen die binnen organisaties plaatsvinden, worden geregistreerd door middel van automatisering. Daarbij zijn diverse interne beheersingsmaatregelen steeds vaker geautomatiseerd in softwarepakketten. Wij onderzoeken daarom de algemene onderwerpen rondom de beheersing van uw IT omgeving en rapporteren daarover in de navolgende pagina's.

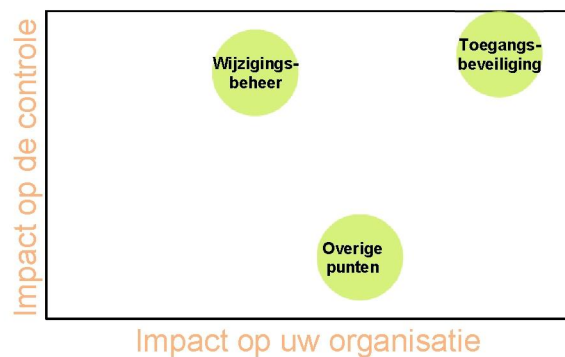
Werkzaamheden

Op basis van de door ons uitgevoerde werkzaamheden hebben wij onze inschatting van de kwaliteit van uw IT systeem (netwerk) en/of applicatie (Civision) opgenomen. Hierbij hebben wij de volgende onderverdeling gemaakt om de kwaliteit weer te geven:

-  Op dit moment voldoende
-  Benodigd verbetering op (korte) termijn
-  Urgente verbetering vereist

Let op: de onderwerpen die niet gerelateerd zijn aan toegangsbeveiliging en wijzigingsbeheer volgen uit interviews en hierop zijn door ons over het algemeen geen testwerkzaamheden uitgevoerd om vast te stellen dat de IT-omgeving is ingericht zoals ons voorgesteld is. Dit beperkt de zekerheid die u kunt ontleen aan de door ons beschreven aandachtspunten.

De mate van risico die u als organisatie loopt bij constatering verschilt per aandachtsgebied. Een grafische inschatting van de impact op de controle en op uw organisatie vindt u in onderstaande afbeelding.



Toegangsbeveiliging

Bij het toetsen van 'toegangsbeveiliging' wordt onderzocht of de inrichting van de IT-omgeving de authenticiteit van de gebruiker van een gebruikersaccount borgt. Vervolgens onderzoeken wij de mogelijkheden voor het 'steunen' op autorisaties en de processen rondom het verstrekken, muteren en ontnemen van autorisaties binnen de omgeving. Wanneer de randvoorwaarden hiervoor voldoende aanwezig zijn, kunnen wij in de controle gebruik maken van ingerichte functiescheiding in het systeem.

Wijzigingsbeheer (Change management)

Bij het toetsen van 'wijzigingsbeheer' wordt vastgesteld dat wijzigingen aan Civision middelen op gestructureerde en gecontroleerde wijze worden doorgevoerd. Voor uw organisatie heeft wijzigingsbeheer ten doel om te voorkomen dat applicaties zich niet gedragen zoals u verwacht na een wijziging in de software, resulterend in, wellicht niet opgemerkte, (financiële) gevolgen.

Adviespunten zonder directe impact

Het is voor ons van belang om inzicht te krijgen in de verantwoordelijkheden die binnen de organisatie zijn ingericht – of met andere organisaties overeen zijn gekomen (uitbesteding) – ten aanzien van de beheersing van de IT omgeving. Hierbij kijken wij naar beleidsstukken ten aanzien van IT strategie, beveiliging en functiescheiding. Ook de interne beheersingsmaatregelen die al dan niet zijn ingericht binnen de IT omgevingen zijn onderdeel van onze scope. Indien maatregelen periodiek worden uitgevoerd kunnen wij hier gebruik van maken in de jaarrekeningcontrole. Deze adviespunten hebben niet een directe impact op onze controlewerkzaamheden, maar zijn wel wenselijk.

3.2 Toegangsbeveiliging

Wij onderscheiden vijf bouwstenen ten aanzien van toegangsbeveiliging, waarbij bouwstenen gestapeld, naast een sterke IT beheersing, ook de meeste controlezekerheid oplevert. Beperkingen in de onderliggende steen, zorgt voor een verzwakking van de bovenliggende stenen. De kleur groen betekend 'Voldoende' en grijs betekend 'Vereist verbetering'. Een toelichting:

Onze verwachting

Uw Organisatie



3.3 Wijzigingsbeheer

Bij het doorvoeren van wijzigingen in software-omgevingen ontstaan risico's voor de bedrijfsvoering van uw organisatie. Wij verwachten daarom dat het proces voor wijzigingen een proces doorloopt, waarmee de risico's die gelopen worden, zijn ingeschat, worden geadresseerd en dat hierop maatregelen genomen worden. Wij hebben onderstaand aangegeven wat wij verwachten per fase en wat wij hebben geconstateerd tijdens onze controle (deels op basis van interview) en of dit overeen komt met de verwachting.

1. Risico-inschatting:

Voor iedere software wijziging is het relevant om te beoordelen wat de risico's zijn die de wijziging met zich mee brengt voor de hoofdprocessen én welke geïdentificeerde technische en organisatorische wijzigingsrisico's worden geraakt bij het uitvoeren van de change, waaronder maatwerk. Per wijziging worden vastgesteld welke nieuwe of gewijzigde functionaliteit een risico vormt voor een goede werking van uw bedrijfsvoering.

Uw situatie:

Wij hebben geen concrete risicoanalyse bij uw organisatie geïdentificeerd. Hiermee is de kans groot dat bepaalde risico's in beperkte mate of geheel niet ondervangen zijn in het proces.

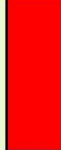


2. Opstellen testplan en -aanpak:

Vanuit de geïdentificeerde risico's kan een testplan worden gemaakt waarin de te testen elementen van de software benoemd zijn evenals de inhoudelijk uit te voeren testwerkzaamheden op deze elementen. Belangrijke elementen hierin zijn go/nogo momenten, het maken van een back up voor implementatie, wat te doen als een implementatie mislukt en de impact op de organisatie (opleiden van medewerkers)

Uw situatie:

U heeft aangegeven dat geen testplan wordt opgesteld vanuit de organisatie. U heeft aangegeven dat wijzigingen op gestructureerde wijze worden doorgevoerd, maar dat de kennis hierover niet is vastgelegd in een plan of procedure.



3. Testen en documenteren:

Softwarewijzigingen kunnen gestructureerd worden getest, na het correct uitvoeren van de voorgaande twee stappen. Een vastlegging van testwerkzaamheden is van belang voor de aantoonbaarheid en controleerbaarheid van de uitgevoerde stappen.

Uw situatie:

U heeft aangegeven dat geen vastlegging wordt gemaakt van de uitgevoerde testwerkzaamheden. Dit heeft tot gevolg dat wij werkzaamheden uitvoeren om de impact van wijzigingen te bepalen.



4. Gebruikersacceptatie:

Een wijziging is pas effectief als deze niet alleen is geaccepteerd vanuit een technisch oogpunt, maar ook vanuit de gebruikersorganisatie. Wij verwachten daarom een formele goedkeuring vanuit de gebruikersorganisatie, zowel voor implementatie als na de implementatie

Uw situatie:

U heeft aangegeven dat de 'Business' wordt betrokken bij het proces voor het doorvoeren van softwarewijzigingen, deze betrokkenheid is geformaliseerd in een akkoord vanuit de gebruikersorganisatie.



3.4 IT adviespunten zonder directe impact op de controle

Beleid en plannen

Beleid

Binnen uw organisatie is een uitgewerkt IT beleidsplan aanwezig, waarin de uitgangspunten voor IT beheer en ontwikkelingen zijn beschreven. Het beleid is vastgesteld in 2015 en u heeft aangegeven bezig te zijn met een vernieuwde versie van het beleid. Ons advies is om spoedig het nieuwe beleid vast te stellen en te communiceren.



Verantwoordelijkheden en functiescheiding

Wij verwachten dat binnen uw organisatie duidelijke afspraken zijn gemaakt ten aanzien van verantwoordelijkheden over uitvoering en strategie op het gebied van IT. U heeft aangegeven dat dit het geval is. Uw organisatie maakt gebruik van externe IT partijen, met deze partijen is een contract en Service Level Agreement overeen gekomen. Rapportages over de naleving van de SLA worden niet periodiek gemonitord.

Wij adviseren om op een actieve manier de dienstverlening van leveranciers te monitoren en te evalueren. Dit geldt zowel voor het netwerk als Civision middelen.

Uitvoering

Beheersing van incidenten

Om de performance van uw IT systemen en eventueel de performance van uw IT dienstverlener te monitoren, is registratie van de incidenten en problemen van belang. Hierdoor verkrijgt u inzicht in de performance van uw systemen, maar ook van uw IT organisatie en kunt u waar nodig uw beleidsplan corrigeren.

Wij adviseren u om de werkwijze voor de registratie en beheersing van incidenten in lijn te brengen met de procedure zoals in beleid beschreven.

Uitvoering beheersingsmaatregelen IT

Op verschillende vlakken worden (nog) geen toetsbare beheersingsmaatregelen uitgevoerd binnen uw organisatie. Denk aan:

- Procedure voor wijzigingsbeheer (zie ook punt 'Wijzigingsbeheer')
- Procedure rondom uitgifte en controle op unieke en individuele gebruikersnamen
- Periodieke controle op actieve gebruikers
- Periodieke controle op inrichting van wachtwoordbeleid
- Procedure voor het gestructureerd toekennen, wijzigen en ontnemen van rechten
- Periodieke controle op inrichting van rechten in het systeem conform beleid

Deze procedures en daaruit volgende controlemaatregelen zorgen ervoor dat uw organisatie grip houdt op de IT-omgeving en faciliteren dat de randvoorwaarden, die de effectiviteit van ingerichte beheersingsmaatregelen beïnvloeden, van voldoende niveau zijn. Dit geldt zowel voor het netwerk als Civision middelen.

Wij adviseren u om via een verbeterplan te monitoren dat de uitvoering van bovenstaande beheersingsmaatregelen ingebed wordt in uw organisatie.

3.4 IT adviespunten zonder directe impact op de controle

Continuïteitsmaatregelen



Recovery Point objective (RPO): De RPO is het punt in de tijd tot waar men minimaal de gegevens moet kunnen herstellen. Het is dus de acceptabele hoeveelheid aan dataverlies uitgedrukt in tijd.

Back-ups: U heeft aangegeven dat back-ups periodiek en incrementeel worden gemaakt en extern worden opgeslagen. Wij adviseren u om periodiek de back-ups te testen en van de testen verslagen vast te leggen.



Recovery Time Objective (RTO): Een RTO is de tijd waarna een proces/middel na een onderbreking moet teruggebracht zijn op een aanvaardbaar niveau, om een onacceptabele impact op de organisatie te vermijden

Recovery: Recent heeft geen volledige recovery test plaatsgevonden. Hierdoor beschouwen wij het risico op dataverlies en downtime voor uw IT organisatie als verhoogd. Wij adviseren om periodiek minimaal een recovery test uit te voeren voor de applicatie Civision, over de resultaten te rapporteren en bij te sturen indien noodzakelijk.

Uitwijk: U heeft aangegeven dat een uitwijkmogelijkheid is ingericht. Wij adviseren om periodiek een uitwijk test uit te voeren, over de resultaten te rapporteren en bij te sturen indien noodzakelijk.

Beveiliging



Beveiliging

De beveiliging van de IT-omgeving delen wij op in verschillende aspecten, welke wij hieronder hebben weergegeven.

Fysieke beveiliging: De serverruimte is voorzien van diverse beveiligingsmaatregelen ten aanzien van temperatuur, klimaat en brandrisico's.

Remote access: Voor het extern inloggen wordt gebruik gemaakt van extra beveiligingsmaatregelen zoals two-factor authenticatie.

Preventie: Een firewall en virusscanner zijn aanwezig en worden actief beheerd.

Monitoring: Afgelopen boekjaar heeft geen attack- en penetration test plaats gevonden. U laat wel periodiek vulnerability scans uitvoeren. Hierdoor is de beveiliging niet volledig getoetst. Wij adviseren om periodiek de te monitoren of de getroffen beveiligingsmaatregelen adequaat zijn ingericht.

4. Attentiepunten jaareinde controle en overige aandachtspunten

4. Attentiepunten jaareinde controle en overige aandachtspunten

Planning jaareinde controle

In het voorjaar van 2020 zal de jaareinde controle van de jaarrekening van Overbetuwe plaatsvinden. Belangrijk voor een goed controleproces is een tijdige en volledige oplevering van zowel de (concept) jaarrekening als het digitale balansdossier.

Wij verzoeken u het controledossier aan te leveren in Huddle zoals deze in de op te leveren stukkenlijst (PBC lijst) is opgenomen.

Aanbestedingsrechtmatigheid

Wij constateren dat de controle op de aanbestedingsrechtmatigheid in 2018 meer tijd van uw en onze organisatie heeft gekost. Belangrijke oorzaak hiervan is dat de gemeente geen centraal zicht heeft op de juiste naleving van de naleving van de (Europese) aanbestedingsregelgeving. Daarnaast heeft de Sectorgroep Decentrale Overheden (SDO) begin 2019 de notitie 'Uitvoering van de controle op aanbestedings-rechtmatigheid bij de jaarrekeningcontrole van decentrale overheden' gepubliceerd, waarin een aanscherping van de controle op de aanbestedingsrechtmatigheid is opgenomen. Wij adviseren u in het kader van de voorbereiding op de door u op te stellen spendanalyse over 2016-2019 kennis te nemen van deze notitie. Vanzelfsprekend adviseren wij u ook om de beheersing op de naleving van de aanbestedingsregelgeving aan te scherpen.

Ten behoeve van onze jaarrekeningcontrole is het noodzakelijk dat u een gedetailleerdere en onderbouwde spendanalyse oplevert. Wij vragen daarbij expliciet aandacht voor een toereikende analyse op alle uitgaven die gedurende de periode 2016-2019 hoger zijn dan € 221.000 en over 2019 hoger zijn dan € 55.000. Deze topdown analyse dient tenminste de volgende stappen te bevatten.

Ten aanzien van de uit de sluiten lasten, zoals subsidies, belastinglasten, pensioenbetalingen aflossingen en inkomensoverdrachten vragen we u specifiek de volgende zaken te evalueren:

- *Verstrekte subsidies*: gegroepeerd naar soort subsidie, alsmede een analyse van het mogelijke risico op overheidsopdrachten op subsidiesoort niveau en een nadere analyse van materiële risicovolle individuele subsidies.
- *Publiek publieke samenwerking*: onderscheid tussen verticale (quasi-inbesteden), horizontale (publiek publieke) samenwerking en/of alleenrecht, alsmede een nadere analyse in relatie tot de geldende voorwaarden.

Over de daadwerkelijke inkooplasten die mogelijk via een (Europese) aanbestedingsprocedure tot stand moeten komen vragen we in uw opdracht specifiek uw aandacht voor de volgende zaken:

- De spendanalyse dient op opdrachtniveau per crediteur opgesteld te worden. Daarbij dient de gemeente toereikend te onderbouwen dat er niet onrechtmatig opdrachten gesplitst worden.
- *ICT opdrachten*: uitgaven uit hoofde van ICT, een nadere analyse of sprake is van een zogenaamde 'vendor lock' en de maatregelen die zijn genomen om een 'vendor lock' te voorkomen.
- *Inhuur derden*: uitgaven uit hoofde van inhuur derden, een nadere analyse van de verschillende soorten contracten en de mogelijkheid dat alle opdrachten moeten worden beoordeeld als diverse individuele opdrachten.

We adviseren u bij het opstellen van de spendanalyse ook nadrukkelijk de kennis van uw inkoopadviseur te betrekken, zodat de naleving van de aanbestedingsregelgeving ook toereikend in verwijzing naar wetsartikelen aangetoond kan worden. In voorkomende gevallen waar het niet eenduidig is dat daadwerkelijk terecht wel of niet (Europees) is aanbesteed adviseren we om een advies van een inkoopjurist in te winnen. Ontoereikende oplevering en bevindingen leiden tot aanvullende werkzaamheden en meerkosten.

4. Attentiepunten jaareinde controle en overige aandachtspunten

Nieuwe Notitie Grondexploitaties 2019

Sinds de wijziging van het BBV in 2016 heeft de commissie BBV diverse uitingen gedaan en een veelheid aan vragen beantwoord over grondexploitatie en grondbeleid en daarmee samenhangende problematiek. Deze uitingen zijn samengevoegd in een nieuwe notitie Grondbeleid in begroting en jaarstukken, die met ingang van begrotingsjaar 2019 geldig is.

Enkele opvallende zaken uit de geactualiseerde notitie:

- *Nieuwe categorie Warme gronden woningbouw*: gronden (materiële vaste activa) waarvan op voorhand vaststaat dat deze als bouwgrond zullen fungeren, maar waarvoor geen operationele grondexploitatie is opgesteld. Om grote fluctuaties in de waardering van deze gronden tegen te gaan heeft de commissie BBV besloten dat onder cumulatieve voorwaarden bij de waardering uitgegaan mag worden van de grond tegen toekomstige bestemming in plaats van de huidige bestemming. Eerder toegepaste afwaarderingen mogen niet worden teruggedraaid. De cumulatieve voorwaarden zijn nader toegelicht in de notitie.
- *Versimpeling faciliterend grondbeleid*: de verantwoording over vorderingen inzake het faciliterend grondbeleid is in de geactualiseerde notitie eenvoudiger geworden. De verschillende vorderingen worden in plaats van onder een samenstel van balansposten (nog te verrekenen kosten) verzameld op de balanspost 'overige nog te ontvangen bedragen'. Binnen deze balanspost worden de verschillende vorderingen in de toelichting op de balans gespecificeerd als verhaalbare kosten, nog te verhalen kosten of nog te verrekenen kosten.
- *Verduidelijking tussentijdse winstneming*: in de geactualiseerde notitie is de berekening (poc-methode) van tussentijdse winstneming nader toegelicht aan de hand van voorbeelden. Daarnaast is toegevoegd dat teveel genomen winst in eerdere jaren verrekend moet worden met het huidige jaar of indien nodig zelfs (gedeeltelijk) teruggedraaid kan worden door een verliesneming in het huidige jaar.

Waardering grondexploitaties

Bij een deugdelijke en navolgbare onderbouwing van de grondexploitaties hoeft de interne en externe controle in het kader van de jaarrekening niet ingewikkeld te zijn. Wij vragen in dat kader specifieke aandacht voor de volgende punten:

- *Programma/planning*: actuele onderbouwingen van zowel het aanbod als de vraag, met bijbehorende realistische planningen.
- *Prijs*: deugdelijke en actuele onderbouwingen van (marktconforme) grondprijzen.
- *Parameters*: onderbouwen marktconforme kosten- en opbrengstenstijging voor korte en middellange termijn.
- *Planontwikkelingskosten*: inzichtelijke en projectspecifieke onderbouwingen van de planontwikkelingskosten (zowel plankosten als de kosten van Voorbereiding & Toezicht).
- *Civieltechnische werken*: geactualiseerde en degelijk onderbouwde civieltechnische ramingen, navolgbaar aansluitend op de laatste stand van de planvorming.
- *Risicoanalyse*: gefundeerde risicoanalyse mede ter onderbouwing van een eventuele projectspecifieke risicoafslag bij de tussentijdse winstneming.

Wij vragen u bij de dossiervorming kennis te nemen van de in september 2019 door de commissie Bedrijfsvoering, Auditing Decentrale Overheden (BADO) uitgebrachte notitie over grondexploitaties. Indien u voornemens bent taxaties uit te voeren vragen wij u om vooraf de te verstrekken opdracht af te stemmen met ons, hierdoor kan gegarandeerd worden dat de taxatie tevens bruikbaar is in onze controle.

Deze notitie beschrijft het gehele proces van woningbehoefte tot het sluiten van een grondexploitatie. Per processtap ligt in de notitie de focus op de documentatie die idealiter aanwezig is in het beheerdossier van een gemeente.

4. Attentiepunten jaareinde controle en overige aandachtspunten

Het RvS Stikstofbesluit (PAS regels)

De RvS heeft op 29 mei 2019 de bekende stikstofuitspraak gedaan. Gevolg is dat het Programma Aanpak Stikstof (PAS) niet langer gebruikt mag worden als basis om toestemming te verlenen voor activiteiten die leiden tot een stikstoftoename in de natura 2000-gebieden. Doordat de drempelwaarde en uitgestelde compensatie van PAS niet meer geldt, is het een stuk ingewikkelder geworden om ruimtelijke ontwikkelingen te realiseren. Bij elk project in Natura 2000-gebieden moet duidelijk gemaakt worden hoe de uitgestoten stikstof gecompenseerd gaat worden. Voor onlangs verleende, lopende of toekomstige aanvragen kan de uitspraak leiden tot extra vertraging, extra kosten en in het slechtste geval moet de haalbaarheid van de plannen opnieuw beoordeeld worden.

Wij adviseren u voor de gemeentelijke grondexploitaties te onderzoeken én navolgbaar te onderbouwen of de bovengenoemde uitspraak consequenties heeft voor de fasering van kosten en opbrengsten in de grondexploitaties:

- Onderzoek in hoeverre het RvS-besluit leidt tot vertraging in de grondexploitaties, onderbouw wel/geen vertraging, pas eventueel in de actualisatie per 1-1-2020 de afzetplanningen hierop aan;
- Onderzoek mogelijke risico's en verwerk die in de risicoanalyses;
- Onderzoek hoe, waar mogelijk met betrokken marktpartijen en maatschappelijk partners, knelpunten opgelost kunnen worden.

Voorziening groot onderhoud

Onderhoudskosten worden gemaakt om een object gedurende de levensduur op een bepaald kwaliteitsniveau te houden of weer te krijgen. Onderhoud kan worden onderscheiden in groot onderhoud en klein onderhoud. Wanneer een aanpassing leidt tot een significante kwaliteitsverbetering (object blijft niet in dezelfde staat), is geen sprake van groot onderhoud, maar van een investering (bijvoorbeeld een renovatie) die geactiveerd moet worden.

Lasten van groot onderhoud kunnen alleen dan ten laste van een gevormde voorziening worden gebracht, indien er een recent beheerplan van het kapitaalgoed aanwezig is. Onder recent wordt een beheerplan verstaan van maximaal vijf jaar oud. Deze vijf jaar dient te worden gehanteerd als richttermijn waar gemotiveerd van kan worden afgeweken. Een gemotiveerde afwijking houdt in dat deze motivatie is geautoriseerd door de Raad en verantwoord is in de paragraaf 'Onderhoud kapitaalgoederen'. Binnen deze vijf jaar bestaat wel de verplichting om het beheerplan tussentijds bij te stellen, indien het beheerplan in belangrijke mate niet meer aansluit bij de actuele situatie van staat van het onderhoud.

De hoogte van de periodieke toevoeging aan de voorziening wordt bepaald op basis van dit beheerplan, maar dient minimaal gebaseerd te zijn op de onderhoudslasten die in het beheerplan zijn opgenomen voor het begrotingsjaar plus de drie jaren van de meerjarenraming.

Het is niet toegestaan dat de voorziening een (verwachte) negatieve stand vertoont. Indien geplande onderhoudsuitgaven eerder uitgevoerd moeten worden dan oorspronkelijk gepland in het beheerplan, moet bezien worden of de voorziening geen negatieve stand bereikt.

In geval van achterstallig onderhoud, waarbij sprake is van kapitaalvernietiging en/of onveilige situaties, moet een voorziening worden gevormd. Wanneer de gemeente over onvoldoende middelen beschikt om een voorziening te vormen, moet het achterstallig onderhoud, daadwerkelijk en financieel, binnen een termijn van maximaal vier jaar worden ingelopen.

Wij vragen u om vast te stellen dat de gevormde voorziening voldoet aan de voorwaarden die zijn opgenomen in de notitie Materiële vaste activa van de Commissie BBV.

4. Attentiepunten jaareinde controle en overige aandachtspunten

WNT verantwoording

Wij verwachten dat u per jaareinde een analyse maakt van de WNT waarbij inzichtelijk wordt gemaakt, welke functionarissen voldoen aan de WNT. Voor deze functionarissen dient op basis van het controleprotocol adequaat te worden onderbouwd, welke salariscomponenten (en op welke wijze) verantwoord dienen te worden in de WNT-verantwoording. Wij vragen hierbij uw aandacht voor de nauwkeurigheid van de bedragen, maar ook voor de volledigheid (bijvoorbeeld inzake declaraties, welke niet via de salarisadministratie geboekt worden).

Structurele en incidentele baten en lasten

In de herziene notitie structurele en incidentele baten en lasten wordt het onderscheid tussen incidentele en structurele baten en lasten verduidelijkt, zodat de begrippen 'incidenteel' en 'structureel' meer eenduidig toegepast worden. Deze verduidelijking vindt in de notitie plaats door middel van een algemeen kader en diverse uitgewerkte (niet limitatieve) voorbeelden.

Wij vragen u bij het opstellen van de jaarrekening 2019 rekening te houden met de in de notitie opgenomen stellige uitspraken en aanbevelingen:

- Voor de in het overzicht van incidentele baten en lasten opgenomen posten is een nadere toelichting vereist;
- De Commissie BBV adviseert in de financiële verordening (artikel 212 Gemeentewet) een grensbedrag op te nemen vanaf welke omvang incidentele baten en lasten afzonderlijk gespecificeerd worden in het overzicht van incidentele baten en lasten;
- De Commissie BBV adviseert het structureel begrotingssaldo te presenteren conform het voorbeeld in hoofdstuk 4 van de notitie.

5. Overige onderwerpen

5. Overige onderwerpen

Rechtsmatigheidsverantwoording met ingang van boekjaar 2021

Met ingang van boekjaar 2021 dient het College van burgemeester en wethouders van de gemeente Overbetuwe zelf verantwoording af te leggen aan de Raad over het rechtmatig tot stand komen van de in de jaarrekening verantwoorde baten en lasten alsmede de balansmutaties, dat wil zeggen in overeenstemming met de begroting en met de relevante wet- en regelgeving, waaronder gemeentelijke verordeningen.

Deze verantwoording zal onderdeel gaan uitmaken van de jaarrekening van de gemeente en als zodanig object van onderzoek worden voor de accountant in zijn opdracht om een getrouwheidsoordeel bij de jaarrekening af te geven. De Raad zal de materialiteits- en rapporteringsgrens bepalen, mogelijk wel binnen een bepaalde wettelijke bandbreedte. Naar verwachting zal in het najaar van 2019 door het Ministerie van BZK en de Commissie BBV expliciet worden gecommuniceerd over de specifieke uitwerking. Ook de voorgestelde tekst van de rechtsmatigheidsverantwoording zal dan duidelijk worden. Daarin zal aandacht worden besteed aan de verantwoordelijkheid van het College, een overzicht van fouten en onzekerheden worden opgenomen (onderverdeeld naar de rechtsmatigheidscriteria: voorwaarden, begroting en misbruik & oneigenlijk gebruik) en optioneel het College een toelichting kunnen geven van eventueel te treffen beheersmaatregelen om geconstateerde fouten en onzekerheden naar de toekomst toe te beperken.

De aanstaande wetwijziging op dit punt is bedoeld om de kaderstellende en controlerende rol van de Raad te versterken. Tevens is de intentie dat hiermee de (politieke) verantwoordelijkheid ten aanzien van financiële rechtsmatigheid van het College wordt benadrukt en dat dit een kwaliteitsverhogend effect heeft op de financiële bedrijfsvoering van de gemeente. Juist vanuit deze achtergrond adviseren wij u om het gesprek tussen de Raad en het College te faciliteren en te voeren.

Wat is het gewenste en huidige niveau van de financiële bedrijfsvoering en welke ontwikkeling is daarbij nodig? Meer dan in de huidige situatie is voor de Raad inzichtelijk hoe het staat met de kwaliteit van de bedrijfsvoering.

Wij kunnen ons voorstellen dat het belangrijk is voor de Raad, het College, de griffie en de ambtelijke organisatie om duidelijkheid te krijgen over de invulling van ieders rol en verantwoordelijkheid en de eisen die worden gesteld aan de interne beheersing om tot een rechtsmatigheidsverantwoording te kunnen komen en met elkaar hierover het goede gesprek te hebben. Niet in de laatste plaats is het voor het College een nieuwe en expliciete verantwoordelijkheid. Daarbij is voor de wethouder Financiën mogelijk een coördinerende rol logisch, het is echter niet zijn zelfstandige verantwoordelijkheid, het voltallige College is verantwoordelijk. Op basis van onze visie als Baker Tilly én onze deelname aan landelijke overlegtafels inzake de rechtsmatigheidsverantwoording ondersteunen wij uw gemeente hier graag bij.

5. Overige onderwerpen

Eerste bevindingen visitatiecommissie sociaal domein

Naar aanleiding van zorgen van gemeenten over de financiële beheersbaarheid in het sociaal domein hebben de VNG en BZK een visitatiecommissie opgericht, met de opdracht gemeenten te helpen om grip te krijgen op de uitgaven in het sociaal domein. Hoewel pas een klein aantal gemeenten het volledige traject doorlopen hebben, is door de commissie al wel een aantal hoofdbevindingen gedeeld:

- *Nadruk op Jeugd:* zonder uitzondering gaat de meeste aandacht naar uitgaven onder de Jeugdwet, op afstand gevolgd door de Wmo-2015.
- *Data-gebruik:* gemeenten zijn in wisselende mate in staat om data te ontsluiten en te benutten voor de opbouw van een monitor en/of dashboard. Hierbij maken zij afzonderlijk van elkaar kosten voor de ontwikkeling van instrumentaria. Op dit moment bestaat nog geen model-monitor of ijkpunten waar gemeenten de monitor/dashboard op kunnen richten.
- *Regio:* er is een stevige positie van de gemeente nodig in de samenwerking met aanbieders, inwoners en omliggende gemeenten. Een zekere schaalgrootte is nodig om dit gesprek op het juiste niveau te kunnen voeren, zeker als het gaat om de rol van grote aanbieders. Tegelijkertijd levert regionale samenwerking ook nieuwe knelpunten op, bijvoorbeeld in besluitvorming of bij tegengestelde uitgangspunten.
- *Bezuinigingsmaatregelen:* een vroegtijdige start met de transformatie blijkt geen harde garantie voor grip op uitgaven en een afname van tekorten. Veel gemeenten hebben interventies ingezet om de uitgaven te temperen maar zien de uitgaven nog onvoldoende dalen.
- *Instream:* werkdruk bij de gemeentelijke toegang en de autonome positie van wettelijk verwijzers (Jeugd, met name huisartsen) geeft beperkte grip op de toegang. Zicht op veelvoorkomende (hulp-)vragen en een solide samenwerking met huisartsen biedt ruimte om schaarse middelen gericht in te zetten ('matched care' in plaats van 'stepped care').
- *Doorstroom:* afhankelijk van het inkoopmodel valt op dat trajecten vaak langer duren dan oorspronkelijk voorzien en dat de intensiteit opgeschaald wordt gedurende de looptijd. Dit terwijl het aantal trajecten dat verkort is kleiner is. Gemeenten die zicht hebben op de duur van trajecten kijken naar oorzaken van verlengingen en stellen zich zakelijker op naar aanbieders.
- *Uitstroom:* voorzieningen in de lokale basisinfrastructuur (zoals welzijnswerk) staan in sommige gemeenten onder druk vanwege oplopende tekorten. De commissie ziet een risico van verschraling, waardoor mogelijk de druk op professionele ondersteuning toeneemt.

5. Overige onderwerpen

Geprognosticeerde balans en EMU-saldo

De nieuwe notitie geprognosticeerde balans en EMU-saldo bevat handreikingen voor het opstellen van de geprognosticeerde (meerjaren)balans en voor de wijze van berekenen van het EMU-saldo. In de notitie wordt onder meer duiding gegeven aan de betekenis voor raadsleden en andere bestuurders: de bedoeling om meer naar toekomstige ontwikkelingen te kijken en eerder signalen af te geven om daardoor zo nodig bij te sturen. Zo geven de verschillende posten van de geprognosticeerde balans en de kengetallen de raad meer inzicht in de verwachte ontwikkeling van de financiële positie, het risicoprofiel van de financiële positie (risico's van investeringen, bouwgronden in exploitatie en schuldportefeuille) en de mate van flexibiliteit van de exploitatie(begroting). Meer investeringen en schulden betekenen immers ook structureel hogere vaste afschrijvings- en rentelasten en meer risico's die samenhangen met de investeringen en schuldportefeuille.

Het EMU-saldo kan gezien worden als een extra financieel kengetal, naast de andere vijf verplichte financiële kengetallen zoals de solvabiliteit en de (netto) schuldquote. Het EMU-saldo geeft namelijk in één oogopslag aan of de gemeente via reële transacties netto geld uitgeeft, of dat er netto geld binnenkomt. Het EMU-saldo van één jaar zegt relatief weinig. Een structureel negatief EMU-saldo is echter reden tot zorg: dit geeft aan dat de gemeente jaar-op-jaar meer geld uitgeeft dan de gemeente ontvangt. Andersom kan het ook onwenselijk zijn dat het EMU-saldo enkele jaren op rij een flink positief saldo vertoont. Dit geeft immers aan dat de gemeente mogelijk onnodig geld oppot, terwijl het geld besteed kan worden aan voorzieningen in de gemeente. Het is aan de Raad om het College om een toelichting te vragen en het gesprek aan te gaan.

Baseline Informatiebeveiliging Overheid (BIO)

Per 1 januari 2020 wordt de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO betreft een aanscherping van de "oude" normen van de BIR, BIWA en IBI die het rijk, waterschappen en provincies hanteren. Daarnaast brengt de BIO een vermindering van de administratieve last met zich mee. De IBD heeft een stappenplan gepubliceerd aan de hand waarvan een goede BIO-implementatie kan worden opgestart. Op deze pagina geven wij daar een nadere toelichting op.

Meer aandacht voor risicomanagement

In tegenstelling tot de "oude" normen is er bij de BIO meer aandacht voor risicomanagement en verschuiving van verantwoordelijkheden naar proceseigenaren. Als organisatie dient u aantoonbaar grip te houden op de processen ten aanzien van informatiebeveiliging.

Werk volgens een gefaseerde aanpak

Wij raden u aan om de implementatie van BIO binnen uw organisatie gefaseerd aan te pakken. Hiermee onderneemt u op een gestructureerde wijze actie en zet u de beschikbare middelen efficiënt in om tijdig aan de BIO te kunnen voldoen.

Stap 1: Zet BIO op de bestuurlijke agenda

Vraag op bestuurlijk niveau aandacht om het onderwerp informatiebeveiliging op de kaart te zetten.

Stap 2: Verkrijg inzicht in de huidige stand van zaken middels een nulmeting

Middels het uitvoeren van een BIO-nulmeting op de belangrijkste processen van uw organisatie krijgt u inzicht in de huidige stand van zaken ten aanzien van de BIO. Daarnaast identificeert u middels een nulmeting de aspecten die nog aandacht nodig hebben en kan gericht een plan van aanpak voor het oplossen van deze 'gaps' worden opgesteld.

Stap 3: Voer actief risicomanagement

Voer risicoanalyses uit die als input dienen voor het BIO-verbeterplan. Het BIO-verbeterplan kunt u gebruiken als instrument om informatiebeveiliging binnen uw organisatie te verbeteren, de voortgang van verbeteracties te bewaken en hierover te rapporteren.

5. Overige onderwerpen

Stap 4: Beleg de uitvoering van de BIO-maatregelen in de lijn

Vanuit de BIO-systematiek is de uitvoering van en verantwoording over beheersingsmaatregelen de verantwoordelijkheid van de lijn. Betrek deze functionarissen tijdig bij het proces.

Stap 5: Monitor en verbeter

Informatiebeveiliging is een continu proces. Periodieke monitoring op uitvoeringskwaliteit van beheersmaatregelen is daarom essentieel.

Baker Tilly helpt

De IT-auditors en adviseurs van Baker Tilly hebben ruime ervaring met informatiebeveiliging bij overheidsinstanties. Zij zijn bekend met het nieuwe normenkader en kunnen u begeleiden bij de implementatie van BIO. Van aandacht vragen voor informatieveiligheid tot en met het verschaffen van inzicht in de huidige stand van zaken ten aanzien van de BIO. Daarnaast adviseren wij over de te zetten stappen en bieden praktische ondersteuning tijdens de implementatie. Doordat onze IT-auditors en adviseurs ervaring inbrengen uit andere sectoren, waar het gedachtegoed van de Baseline Informatiebeveiliging Overheid al geruime tijd wordt gehanteerd, kunnen zij u ondersteunen vanuit de theorie en de praktijk.

Wij kunnen u middels een quick scan een snel eerste inzicht geven waarmee u vervolgens de BIO-implementatie goed kunt opstarten. Bij deze quick-scan besteden wij een beperkte, vaste hoeveelheid tijd om (met u) binnen uw organisatie het net op te halen en een eerste beeld te schetsen. Daarbij tonen we gelijk ook de kracht van het gebruik van ISMS-software om uw risicomanagement proces te ondersteunen, conform aanbeveling van IBD.

Privacywetgeving

De Algemene Verordening Gegevensbescherming (AVG) is vanaf 25 mei 2018 van toepassing. Omdat de AVG diverse nieuwe en striktere eisen stelt aan organisaties die persoonsgegevens verwerken, is het belangrijk om maatregelen te hebben getroffen om aan deze wet te kunnen voldoen. Het is raadzaam inzicht te hebben en houden over de mate waarin de nieuwe eisen relevant zijn en moeten worden geadresseerd.

Documentatieplicht

Als uw organisatie persoonsgegevens verwerkt, dan hoeft u daar geen melding van te doen bij de Autoriteit Persoonsgegevens. De AVG verandert de (passieve) registratieplicht in een documentatieplicht. U moet zelf de verwerkingen in een verwerkingsregister documenteren, waarmee u actief kunt aantonen dat uw organisatie de privacyregels naleeft.

Meer rechten betrokkenen

De personen wiens gegevens worden verwerkt en beschermd krijgen meer rechten, namelijk:

- Correctie van persoonsgegevens;
- Inzage in persoonsgegevens;
- Verwijderen van persoonsgegevens.

Mensen hebben het recht om u te vragen, persoonsgegevens die u van hen verwerkt, te laten verwijderen.

Impact assessment

Indien de verwerkingen van persoonsgegevens in een organisatie een hoog privacy-risico opleveren dan moet een Data Protection Impact Assessment (DPIA) uitgevoerd worden. Deze assessments geven meer zicht op de aard en omvang van deze gegevensverwerkingen en geven uitsluitsel of dat u aan uw verplichtingen voldoet.

Privacy aandachtspunt bij productontwikkeling

De Algemene Verordening Gegevensbescherming vereist dat al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht wordt besteed aan privacy verhogende (beveiligings)maatregelen.

5. Overige onderwerpen

Eigen Functionaris Gegevensbescherming

Organisaties kunnen verplicht zijn om een Functionaris Gegevensbescherming aan te stellen. Deze functionaris houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG. Binnen uw organisatie is naast een functionaris gegevensbescherming tevens een CISO en een Privacy Officer in dienst.

AVG: boetebeleidsregels aangescherpt in 2019

In Europa zijn de eerste boetes inmiddels uitgedeeld, het boetebeleid in Nederland is in maart 2019 nog aangepast.

Baker Tilly kan u helpen bij het in kaart brengen welke impact de verplichtingen van de AVG voor u hebben. Daarnaast kan met de quickscan AVG van Baker Tilly inzichtelijk worden gemaakt waar u staat en welke aspecten nog aandacht vragen. De quickscan AVG is gebaseerd op het Privacy Control Framework (PCF) uitgegeven door NOREA, de beroepsorganisatie van IT auditors.

Cybersecurity

Cyberaanvallen en internetcriminaliteit vormen een reëel gevaar voor elke organisatie. Cybercrime kan naast directe financiële schade ook flinke reputatieschade veroorzaken. Met cybersecurity kunt u uw organisatie beschermen tegen cybercriminaliteit. Helaas bestaan er geen wondermiddelen tegen cybercriminaliteit, maar cybersecurity is ook geen rocket science.

Stap 1: Identificeer uw kritische gegevens en processen

Maak voor uw organisatie inzichtelijk wat binnen uw organisatie echt de moeite waard is om actief te beveiligen. Denk daarbij aan belangrijke data, maar kijk ook naar kritische processen binnen uw organisatie. Welke data en processen zijn essentieel voor de continuïteit van uw bedrijfsvoering?

- Bepaal uw waardevolle assets;
- Bepaal wat gebeurt als bepaalde systemen en processen (voor langere tijd) niet operationeel zijn.

Stap 2: Ontwerp een veilige IT-omgeving

De inzichten uit de eerste stap zijn het vertrekpunt voor het inrichten van een veilige IT-omgeving. U weet welke gegevens en processen van belang zijn om de continuïteit van uw bedrijfsvoering te kunnen waarborgen. Uw IT-infrastructuur moet zo ingericht worden, dat die gegevens en processen veilig zijn.

- Beoordeel hoe uw technische landschap eruit ziet;
- Bepaal of cruciale data veilig is opgeslagen;
- Inventariseer hoe gebruikers bij de informatie komen en controleer dit regelmatig;
- Zorg voor veilige reservekopieën van uw kritische data;
- Richt procedures in voor systeembeveiliging en patching;
- Voer periodieke beveiligingstests uit op uw netwerk en op kritische applicaties.

Stap 3: Vergroot het bewustzijn bij uw medewerkers

De mens is vaak het grootste risico in de beveiliging van een omgeving. Het vergroten van het bewustzijn bij uw medewerkers en partijen waarmee u samenwerkt is dan ook essentieel om daadwerkelijk een veilige omgeving te creëren.

- Breng het belang van aandacht voor beveiliging continu onder de aandacht;
- Geef zelf het goede voorbeeld;
- Beloon goed gedrag en benoem ongewenst gedrag.

Stap 4: Richt noodscenario's in

Ondanks maatregelen om uw systemen, processen en informatie te beveiligen, kunt u alsnog schade oplopen als gevolg van cybercriminaliteit. U kunt zich gedeeltelijk op deze situaties voorbereiden.

- Bedenk hoe u kunt werken als kritische systemen en processen niet operationeel zijn;
- Bepaal hoe u eventuele schade kunt herstellen;
- Evaluer nut en noodzaak van een cyberverzekering.

Stap 5: Manage cybersecurity als een continu proces

Dreigingen in de buitenwereld kunnen veranderen. Effectieve beveiliging vergt een continue discipline van uw medewerkers én uw leveranciers. Uw actieve aandacht voor beveiliging is daarom essentieel om een veilige omgeving te behouden.

- Maak een manager binnen uw team verantwoordelijk voor cybersecurity en laat deze persoon regelmatig rapporteren over de stand van zaken;
- Benoem daarbij specifieke indicatoren waar u op stuurt.

Contactgegevens

Drs. Edwin Damman RA

Director

06 13 74 45 08

e.damman@bakertilly.nl

Wout Wentink

Manager RA

06 15 38 17 56

w.wentink@bakertilly.nl

Emmy Friesen

Junior manager RA

06 21 92 16 95

e.friesen@bakertilly.nl

Kantoorgegevens:

Baker Tilly (Netherlands) N.V.

Burgemeester Roelenweg 14-18, 8021 EV Zwolle

Postbus 508, 8000 AM Zwolle

038 425 86 00

