

xx januari 2021

MANAGEMENT LETTER 2020

Gemeente Geertruidenberg

CONCEPT D.D. 22 JANUARI 2021

BDO

Aanbiedingsbrief

Gemeente Geertruidenberg
T.a.v. het college van B&W
Postbus 10001
4941 GA RAAMSDONKSVEER

Tilburg, xx januari 2021

Kenmerk: StH/NvE/DMe/…/1049939/…

Geacht college,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2020 van de gemeente Geertruidenberg 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. Onze management letter is daarom van nature kritisch van aard. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelfcontrolerend vermogen van uw organisatie.

Als gevolg van de aanhoudende coronacrisis zijn wij helaas niet in staat geweest om bij u op locatie te komen waardoor wij veel digitaal hebben moeten afstemmen. Ondanks de minder persoonlijke en directe contacten is de interim-controle en samenwerking goed verlopen.

Wij vertrouwen erop u met deze management letter naar aanleiding van onze interim-controle 2020 van dienst te zijn geweest.

Wij willen de medewerkers in uw 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

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

VORIGE PAGINA VOLGENDE PAGINA
DASHBOARD AANBIEDINGSBRIEF

Inhoudsopgave



1. DASHBOARD



2. ONTWIKKELINGEN & AANDACHTSPUNTEN



3. BEVINDINGEN INTERNE CONTROLE



4. BEVINDINGEN SIGNIFICANTE PROCESSEN



5. IT-BEHEERSING

1. Dashboard

1.1 Dashboard

1.1 Dashboard

ACTUALITEITEN - WET- EN REGELGEVING

- Behandeling van de rechtmatigheidsverantwoording in de Tweede Kamer stond in december 2020 gepland. Er moeten nog meerdere stappen worden doorlopen voordat invoering een feit is, waardoor er onzekerheid is of de invoering in 2021 zal ingaan.
- De BBV-wijzigingen zijn in 2020 beperkt ten opzichte van vorig jaar.
- Uitgebrachte notities door het SDO en de commissie BADO bieden handvatten voor de gemeente.
- De notitie Meerjarig financieel inzicht geeft gebruikers van de jaarrekening inzicht in de financiële positie van de gemeente op de korte en langere termijn en legt uit hoe diverse onderdelen in de jaarrekening en begroting in samenhang kunnen worden gezien.

ACTUALITEITEN - CORONA

- De gemeenteraad wordt onder andere middels bestuurs-rapportages geïnformeerd over de gevolgen van corona en de financiële impact hiervan.
- BDO heeft in het najaar een corona zelfscan ontwikkeld, welke is gedeeld met de organisatie en deze is momenteel onderhanden bij de organisatie. Deze scan geeft inzicht over mogelijke gevolgen van de coronacrisis voor de financiën, organisatie en informatievoorziening en geldt als startpunt voor de jaarrekeningcontrole 2020.
- Belangrijke thema's zijn zorgcontinuïteit en TOZO:
  - Wij adviseren tijdig te starten met een analyse van de impact van de zorgcontinuïteit op de jaarrekening.
  - De TOZO-regeling is een SiSa-regeling. Bevindingen in de regeling hebben directe gevolgen op balansposities.
- Wij adviseren u, naast de financiële gevolgen, ook de gevolgen voor de interne beheersing te betrekken, maatregelen te prioriteren en het verloop van onzekerheden monitoren.

ONS BEELD VAN DE INTERNE BEHEERSING

- In het kader van onze controle hebben wij de effectiviteit van de voor onze controle relevante processen beoordeeld. Onder 'bevindingen significante processen' geven wij een samenvatting van onze bevindingen.
- Voor een organisatie met de omvang van de gemeente Geertruidenberg zou de norm kunnen zijn dat de processen in opzet, bestaan en werking (inclusief IT) goed werken en getoetst worden door de VIC (SOLL).
- Wij kwalificeren de interne beheersing over het algemeen in opzet voldoende en binnen de primaire processen is sprake van minimaal noodzakelijke primaire functiescheiding. Binnen de processen is er ruimte om verbeteringen door te voeren. Gezien de omvang van de organisatie en de effectiviteit van de processen achten wij dit niet noodzakelijk.

BEVINDINGEN SIGNIFICANTE PROCESSEN

- Bij de gemeente Geertruidenberg constateren wij (IST):
  - Niet voor alle materiële processen hebben wij een geactualiseerde procesbeschrijving inclusief documentatie ter onderbouwing van het proces ontvangen.
  - Het vastleggen van prestatielevering en het vastleggen van een inkoopverplichting blijven de belangrijkste bevindingen binnen het inkoopproces; hier hebben in 2020 nog geen verbeteringen plaatsgevonden ten opzichte van vorig jaar.
  - Binnen de primaire processen is sprake van beheersmaatregelen. Voor onze jaarrekeningcontrole zijn deze echter niet toereikend vastgelegd en toetsbaar, waardoor achteraf niet direct herleidbaar is of controlemaatregelen zijn uitgevoerd en hoe deze zijn uitgevoerd.
- Als gevolg van deze bevindingen is de controle gegevensgericht van aard.

BEHEERSING IT

- Wij hebben uw financiële applicatie Key2Financiën gecontroleerd in het kader van de jaarrekeningcontrole. Aanvullend hebben wij het wachtwoordbeleid en de superusers binnen GISVG en ADP beoordeeld.
- Er is nog geen concrete opvolging gegeven aan de bevindingen uit onze management letter 2019.
- De belangrijkste bevindingen zijn:
  - Binnen de applicatie en ADP hebben medewerkers met bevoegdheden binnen de primaire processen (salarisadministrateurs) superuser-rechten. Binnen de applicatie Key2Financiën beschikt een niet persoonsgebonden account over superuser rechten.
  - Er hebben geen wijzigingen plaatsgevonden ten opzichte van vorig jaar binnen het proces omtrent change management.
  - Vanwege deze bevindingen kunnen wij (nog) niet steunen op de IT-beheersmaatregelen.

VERBIJZONDERDE INTERNE CONTROLE

- De interne controles zijn uitgevoerd conform het intern controleplan.
- Wij kwalificeren de VIC in overeenstemming met de BADO-notitie bij gemeente Geertruidenberg als variant 3; VIC als interne beheersmaatregel voor de processensubsidies, inkopen en sociaal domein (BUIG & WMO). Voor de overige processen kwalificeren wij de VIC als instrument voor de aanlevering van stukken aan de accountant.
- De VIC kan meer toegevoegde waarde leveren door:
  - De deelwaarnemingen zelf te selecteren.
  - Het aantal waarnemingen per proces te baseren op basis van de omvang, het aantal transacties en de risico-inschatting.
  - Een uniform format hanteren voor de IC-rapportages.
  - De welwillendheid voor de interne controles bij de afdelingen creëren zodat de VIC efficiënter kan werken.

2. Ontwikkelingen & Aandachtspunten

2.1 Gevolgen coronacrisis voor de jaarrekening 2020
2.2 Rechtmatigheidsverantwoording
2.3 Actualiteiten BBV

2.1 Gevolgen coronacrisis voor de jaarrekening 2020 (1/2)

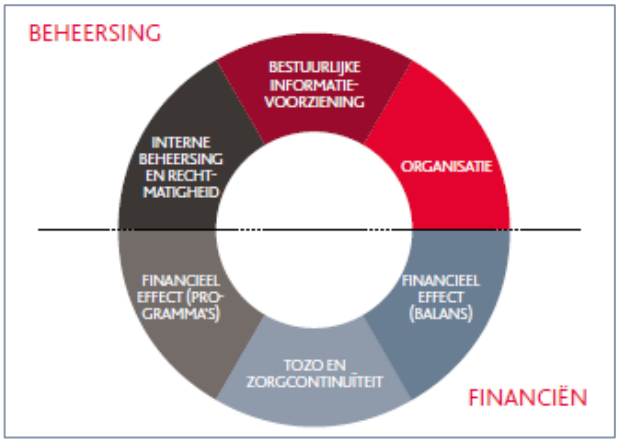
Gemeente Geertruidenberg communiceert voldoende over effecten corona

BDO corona-zelfscan verstrekt

Centrale thema's:
- Zorgcontinuïteit
- TOZO-regeling

Impactanalyse

De lange termijn impact van de coronacrisis op de maatschappij en economie zijn nog steeds hoogst onzeker. In de jaarrekening 2019 had de gemeente Geertruidenberg, in lijn met de verslaggevingsrichtlijnen hieromtrent, een eerste analyse opgenomen van de belangrijkste risico's en onzekerheden. Daarnaast blijkt uit de derde tussenrapportage, welke in de raadsvergadering van 17 december 2020 wordt behandeld, welke begrotingsafwijkingen per programma het gevolg zijn van corona voor zover de gemeente ten behoeve van deze bestuursrapportage heeft kunnen voorzien. In deze bestuursrapportage is eveneens de compensatie vanuit het Rijk toegelicht.



Om een goede inschatting te maken van de mogelijke gevolgen van de coronacrisis voor de jaarrekening 2020 hebben wij een uitgebreide corona-zelfscan opgesteld en gedeeld met de organisatie. Daarbij hebben wij onderscheid gemaakt naar de impact op enerzijds de beheersing en anderzijds op de financiën van uw gemeente. De corona-zelfscan is momenteel onderhanden bij de gemeente.

De vragen over de beheersing gaan over de invulling van de bestuurlijke informatievoorziening en de gevolgen voor de organisatie en de interne beheersing (VIC en rechtmatigheid). De vragen over de financiën gaan zowel over de balans, programma's als specifieke onderwerpen (waaronder TOZO).

Belangrijkste thema's

Voor gemeenten zijn twee thema's als gevolg van corona van belang. Dit betreffen de betalingen van zorgcontinuïteit en de TOZO-regelingen. Beiden hebben mogelijk een grote impact op gemeenten.

Zorgcontinuïteit

Als gevolg van corona hebben vanuit gemeenten of de regio betalingen plaatsgevonden aan zorginstellingen (Jeugd en Wmo) om de continuïteit van de zorg door te betalen. Tevens is door corona de prestatielevering van de zorg lastig vast te stellen. De betaling van de zorgcontinuïteit kent hierbij geen koppeling met de prestatielevering, waarbij de oproep is om de continuïteitsbijdrage te beperken tot een specifieke periode gevolgd door een verantwoording / verrekening achteraf over deze specifieke periode (afrekenen variant over een bepaalde periode). Afspraken tussen de gemeente en zorginstellingen zijn leidend voor de getrouwheid en rechtmatigheid van het voorschot en door I-sociaal domein zijn formats opgesteld die als hulpmiddel kunnen dienen om de bijdrage te berekenen. De controle op de continuïteitsbijdrage wordt uitgevoerd door de zorgaccountants en is in het ISD-protocol 2020 opgenomen. Over dit onderwerp volgt nog een SDO/BADO-notitie. Wel adviseren wij tijdig te starten met een analyse van de impact van de zorgcontinuïteit op de jaarrekening.

TOZO-regeling

Deze regeling is voor zelfstandig ondernemers, waaronder zzp'ers, en voorziet in een aanvullende uitkering voor levensonderhoud en in een lening voor bedrijfskapitaal om liquiditeitsproblemen op te vangen. TOZO 1 en 2 zijn een SiSa-regeling (G4) bij de jaarrekening 2020 van gemeenten. Deze regeling kent 3 soorten rechtmatigheidseisen, te weten fundamentele, belangrijke en formele. Bevindingen bij de SiSa-controle leiden direct tot een terugvordering bij gemeenten door het Rijk en hebben daarmee directe gevolgen voor de balansposities in de jaarrekening.

2.1 Gevolgen coronacrisis voor de jaarrekening 2020 (2/2)

Toets naast financieel impact ook effect op interne beheersing en jaarrekening

Advies voor de kortere termijn; toets naast financieel impact ook effect op interne beheersing

Juist omdat de onzekerheden aanzienlijk zijn, is het naar onze mening cruciaal niet alleen de financiële impact te beoordelen, maar ook de gevolgen van voor de interne beheersing. Wij adviseren hiervoor een aantal maatregelen te treffen: *(niet-limitatief)*

- Wij adviseren de gemeente na te gaan wat het effect van corona is op de interne beheersing en de VIC; zowel inzake de uitgaven (met name subsidies, andere continuïteitsbijdragen en TOZO) als inkomsten (mogelijke extra verantwoordingseisen ten aanzien van bijdragen van het rijk);
- Wij adviseren de gemeente niet alleen de programma's en taken te analyseren, maar ook mogelijke effecten van corona op belangrijke balansposities zoals leningen derden en de waardering van gronden en verbonden partijen. Daarbij ligt het voor de hand tevens aandacht te schenken aan mogelijke corona-effecten op het weerstandsvermogen van de gemeente.
- Wij adviseren de gemeente na te gaan wat het effect van corona is op onder andere soft controls binnen de interne beheersing en de VIC.

De onzekerheden en mogelijk aanvullende eisen die kunnen worden gesteld aan de extra middelen kunnen tot gevolg hebben dat de controle meer (doorloop-) tijd gaat vragen (bv. TOZO). Ook risico's in de naleving van bijvoorbeeld subsidievoorwaarden, financiële tekorten van verbonden partijen, waarderingen van balansposten, etc. kunnen dit effect hebben (zie verder ook onze checklist).

Voor de lange termijn een scenario analyse opstellen om aan de juiste knoppen te draaien

Advies voor de langere termijn: Scenario analyse

Naast de analyse van de (financiële) impact en de bedrijfsvoering is voor de langere termijn het denken in scenario's een volgende stap, ook als uitwerking van risicomanagement en weerstandsvermogen.

Daarbij kunnen de navolgende stappen worden doorlopen:

- Definieer organisatie (programma) specifieke toekomstscenario's op basis onzekerheden
- Bepaal per toekomstscenario mogelijke strategie en maatregelen
- Prioriteren van maatregelen
- Monitor onzekerheden en verloop van scenario's en pas eventueel maatregelen aan

De op te stellen scenario's kunnen zowel betrekking hebben op het beleid als op potentiële gevolgen van corona op de processen en de bedrijfsvoering.

Graag blijven wij in gesprek over effecten op controle van de jaarrekening 2020

Graag blijven wij de komende periode tussen de interim- en jaarrekeningcontrole met u in gesprek over deze ontwikkelingen en de gevolgen van eventuele aanvullende werkzaamheden voor de jaarrekening 2020. Ook denken wij graag met u mee in hoeverre een scenario analyse de gemeente Geertruidenberg kan helpen in de beheersing van de coronaonzekerheden.

2.2 Rechtmatigheidsverantwoording

Invoering rechtmatigheids-verantwoording 2021

Tolerantiegrenzen te bepalen (0% - 3%)

Invoering naar onze mening een kans

Invoering rechtmatigheidsverantwoording met ingang van 2021

In onze eerdere rapportages zijn wij uitgebreid ingegaan op de ontwikkeling van de rechtmatigheidscontrole door de externe accountant naar rechtmatigheidsverantwoording door het college. Op dit moment is de formele status nog steeds dat de rechtmatigheidsverantwoording wordt ingevoerd met ingang van 2021. Of dit daadwerkelijk de invoeringsdatum wordt hangt sterk af van het wetgevingstraject dat eind dit jaar wordt verwacht.

Om deze verplichting te kunnen invoeren zullen het Besluit Accountantscontrole Decentrale Overheden (BADO), de Kadernota rechtmatigheid, etc. nog worden aangepast.

De invoering van de rechtmatigheidsverantwoording 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 naar onze mening ook een kans voor uw organisatie en interne beheersing. Met ingang van verslagjaar 2021 wordt de gemeente Geertruidenberg immers 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.

Uit de notitie van de commissie BBV hierover blijkt dat er een standaard model voor de verklaring komt, rechtmatigheid wordt beperkt tot drie rechtmatigheidsaspecten, de raad kan de tolerantiegrenzen bepalen (tot 3%) en bevindingen moeten worden opgenomen in de paragraaf bedrijfsvoering. De commissie BADO komt naar verwachting ook nog met een nadere uitwerking en toelichting.

BDO ziet de invoering van de rechtmatigheidsverantwoording als een kans om de controlerende rol van de raad te versterken en te investeren in een verdere ontwikkeling van de bedrijfsvoering. Het gaat daarbij om fundamentele vragen als:

- Op welke onderwerpen en met welke diepgang wilt u kaders stellen en controleren?
- In hoeverre werkt het college rechtmatig en/of bent u in control?
- In hoeverre is uw bedrijfsvoering, interne controle en IT beheer op orde en wat is ervoor nodig om daar te komen?
- En misschien wel de moeilijkste vraag van allemaal: wat zijn uw ambities en is uw huidige organisatie in staat om aan die doelen en verwachtingen te voldoen?

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.

Een en ander betekent ook dat wij als accountant de rechtmatigheidscontrole nog tenminste over het boekjaar 2020 zullen uitvoeren.

2.3 Actualiteiten Wet- en regelgeving

BBV Actualiteiten

De wijzigingen in het Besluit Begroting en Verantwoording van gemeenten en provincies (BBV) lijken dit jaar beperkt. Wel zijn er in 2020 een aantal notities uitgebracht. Wij lichten ter voorbereiding op het jaarrekeningtraject 2020 hieronder enkele actualiteiten kort toe.

BADO - Vastlegging en onderbouwing prestatielevering bij inkopen door decentrale overheidsorganisaties

In deze notitie wordt aangegeven waar de aandacht naar uit dient te gaan bij de vastlegging en onderbouwing van de prestatielevering bij inkopen door decentrale overheidsorganisaties. Uitgangspunt hierbij is dat de gemeente zelf verantwoordelijk is voor het inrichten van de AO/IB en een norm bepaalt wanneer de prestatielevering voldoende is vastgesteld. Deze documentatie moet altijd voldoende en geschikt zijn in relatie tot het risico. In de bijlage bij de notitie zijn concrete voorbeelden opgenomen die u als gemeente op weg helpen.

Wij adviseren u kennis te nemen van deze notitie en het beleid vooraf met ons te delen, waarbij wij het risico op onrechtmatige betalingen evalueren.

SDO-Notitie Controle recht op zorg jeugd en Wmo

Per 1 januari 2015 zijn gemeenten in Nederland verantwoordelijk geworden voor de taken in het sociaal domein, waarbij met name de activiteiten met betrekking tot de jeugdzorg en Wmo hebben geleid tot een problematiek van diverse aard. De afgelopen jaren is het recht op zorg en toetsing van de prestatielevering van de zorg door zorgaccountants steeds meer onder de aandacht gekomen. De SDO-notitie is opgesteld vanuit de probleemstelling dat er altijd vanuit wordt gegaan dat er een geldige toewijzing en/of verwijzing van een indicerend orgaan of medisch specialist aanwezig moet zijn ter onderbouwing van het recht op zorg. De verwijzing van het indicerend orgaan of de medisch specialist is niet beschikbaar bij gemeenten, waar dit in gemeentelijke verordening vaak een harde eis is.
Momenteel wordt de controle op recht op zorg onvoldoende afgedekt door het landelijk protocol, maar is wel onderhanden. Deze SDO-notitie geeft de oplossingsrichtingen voor gemeenten in deze situatie aan.

Lastneming subsidies

In februari 2019 heeft de commissie BBV vragen en antwoorden betreffende het omgaan met subsidies gepubliceerd. Daarna zijn vooral bij provincies vragen gerezen hoe om te gaan met de lastneming van het verstrekken van subsidies in verschillende situaties en in het bijzonder betreffende (meerjarige) projecten. De provincies hebben een memo opgesteld en voorgelegd aan de commissie BBV, wat heeft geleid tot het definiëren van een drietal vragen waarop de commissie BBV in haar laatste vergadering de antwoorden heeft vastgesteld. Dit memo ziet toe op projectsubsidies die het boekjaar overschrijden en speelt met name bij provincies, maar is ook voor gemeenten toepasbaar. De strekking van het memo is dat de subsidielast wordt toegerekend aan de periode waarin de prestatie wordt geleverd. Hierbij stelt de gemeenteraad het grensbedrag voor deze subsidies vast. Deze wijziging ziet toe op uitgaande projectsubsidies en is voor gemeente Geertruidenberg niet van toepassing.

Meerjarig financieel inzicht

In september 2020 heeft de commissie BBV de notitie *Meerjarig financieel inzicht voor de raad* vastgesteld. Deze notitie gaat specifiek in op enkele onderdelen die in het BBV zijn voorgeschreven en er op zijn gericht om de gebruiker van de jaarrekening (met name de raadsleden) (meer) inzicht te geven in de financiële positie van de gemeente op de korte en langere termijn. Hierbij wordt uitgelegd hoe de diverse onderdelen uit de begroting en jaarrekening in samenhang gezien kunnen worden om een oordeel te vormen over de financiële positie van de gemeente en/of de gevolgen te overzien van bepaalde beleidskeuzes voor de ontwikkeling van die financiële positie.

3. Bevindingen interne controle

3.1 Verbijzonderde interne controle

3.1 Verbijzonderde interne controle (1/2)

Ons beeld van de VIC

Ons beeld van de VIC

In onze management letter 2019 hebben wij u geïnformeerd over de positionering en de werkzaamheden van de VIC en hebben wij gerapporteerd over ons beeld van de VIC. Het primaire doel van de VIC is vast te stellen of de administratieve organisatie en de daarin vervatte maatregelen van interne controle voldoende waarborgen dat de financiële informatievoorziening juist en volledig is en niet leidt tot een materiële afwijking of onrechtmatigheden.

Binnen de Gemeente Geertruidenberg wordt de VIC-functie vervuld door uw medewerker Interne Controle. De medewerker Interne Controle is verantwoordelijk voor de Interne Controles op de primaire processen, behalve het sociaal domein. Voor de invulling van de VIC-functie voor het sociaal domein, zijnde de interne controles op BUIG en Wmo, huurt de gemeente Geertruidenberg de expertise in van een interne controle functionaris van een buurgemeente. Met ingang van het eerste half jaar van 2020 worden deze controles door een functionaris van een andere buurgemeente uitgevoerd.

Uw medewerker Interne Controle is gepositioneerd als de staffunctie control onder de gemeentesecretaris. Het controleplan 2019 is geactualiseerd in 2020 en aangevuld met een themaonderzoek met betrekking tot corona. In het controleplan staat onder andere aangegeven op welke wijze de interne controles worden uitgevoerd en met welke frequentie interne controles worden uitgevoerd. Per proces zijn uitgebreide werkprogramma's opgesteld die de basis zijn voor de uitvoering van de interne controles. In geval van geconstateerde fouten of tekortkomingen doet de medewerker voorstellen om deze te herstellen of te corrigeren. Eveneens worden door de medewerker Interne Controle aanbevelingen gedaan ten aanzien van het verbeteren van de administratieve organisatie, de informatievoorziening en risicobeperkende maatregelen.

Naar aanleiding van de uitgevoerde interne controles worden rapportages opgesteld met bevindingen, conclusies en aanbevelingen die worden gedeeld met de clustermanagers. De rapportages en de bevindingen uit de interne controles alsmede de status van de interne controles zijn besproken in het MT-overleg en het DT-overleg. In 2020 is in het MT-overleg concrete actie ondernomen naar aanleiding van de bevindingen inzake de vastlegging van prestatielevering uit de interne controle op het inkoopproces.

Variant 3: VIC als interne beheersmaatregel

Wij concluderen dat het op dit moment niet realistisch om te voldoen aan de eisen van de COS 610 (Nederlandse controlestandaard met betrekking tot de interne audit dienst) c.q. dit op korte termijn ook niet het streven is / moet zijn. Wij hebben de VIC beoordeeld in het kader van de BADO-notitie. Voor de interne controles op Wmo en BUIG worden uitgebreide rapportages opgesteld en voor het proces inkoop & aanbesteding wordt na elke interne controle een memo opgesteld met bevindingen en aanbevelingen. Intern is er een controleplan. Dit plan is niet formeel vastgesteld. Ten behoeve van de jaarrekeningcontrole kwalificeren wij de VIC op de processen BUIG, Wmo en inkopen als variant 3. Voor de processen subsidies en belastingen is een gegevensgerichte controle efficiënter en voor de overige processen steunen wij niet op de interne controle en kwalificeren wij de VIC als variant 1.

3.1 Verbijzonderde interne controle (2/2)

Aanbevelingen:
- De deelwaarnemingen zelf selecteren
- Het aantal waarnemingen baseren op de omvang en risico-inschatting per proces
- Uniform format hanteren voor de rapportages
- Welwillendheid voor de interne controles bij de afdelingen creëren

Aanbevelingen

Wij constateren dat de VIC organisatiegericht is ingestoken, waarbij de interne controles achteraf plaatsvinden om de risico's op onrechtmatigheden in processen te beheersen. De frequentie van de interne controles verschilt per proces. Voor een aantal processen worden de te controleren deelwaarnemingen met de externe accountant afgestemd, zodat voor de accountantscontrole voldoende interne controles worden uitgevoerd. Een aanbeveling is om het aantal te controleren items voor alle processen zelf te selecteren en hierbij een duidelijke audittrail van de selectie op te nemen in de rapportages. Tevens adviseren wij in het controleplan per proces een risico-inschatting op te nemen waarbij het aantal deelwaarnemingen per jaarrekeningpost/proces wordt bepaald op basis van de omvang en het aantal transacties en de risico-inschatting van de gemeente per proces.

Wij hebben geconstateerd dat er geen uniform format is voor de opgestelde rapportages per proces. Wij adviseren om een uniform format te hanteren voor alle processen waarin de noodzakelijk onderwerpen zijn opgenomen, zoals de (opvolging van de) bevindingen uit de interne controle van het vorige verslagjaar/de vorige periode, de werkzaamheden, de conclusie, de bevindingen en aanbevelingen alsmede de reactie van de clustermanager. Tot slot is gebleken dat de benodigde documentatie voor de interne controles niet altijd volledig en tijdig wordt aangeleverd vanuit de organisatie. Dit is echter wel van belang voor een goed werkende interne controle en een tijdige afronding, zodat vanuit de interne controles ook tijdig aanbevelingen kunnen worden opgesteld voor de organisatie. Met deze wijzigingen neemt de meerwaarde van de interne controles toe en geeft u tevens invulling aan de rol van de VIC bij de uitvoering van de rechtmatigheidsverantwoording.

Graag gaan wij met u de dialoog aan om deze adviespunten nader toe te lichten.

4. Bevindingen significante processen

4.1 Onze controle nog transparanter
4.2 Effectiviteit processen

4.1 Onze controle nog transparanter (1/2)

Eisen aan accountantscontrole en onze rapportages

Onderkende potentiële risico's:
- Management override
- EU-aanbestedingen
- ICT

Wij beoordelen de volgende processen

Inleiding

De afgelopen jaren is er veel discussie (geweest) over de eisen die worden gesteld aan de accountantscontrole, wat direct en indirect ook gevolgen heeft voor de verwachtingen die wij als accountants hebben van onze klanten. Wij vinden het van groot belang dat wij inzicht geven in de normen en verwachtingen ten aanzien van onze controle en de vertaling hiervan specifiek voor uw gemeente. Een goede interne beheersing maakt immers ook dat de risico's voor de organisatie geringer zijn en de externe controle effectiever en efficiënter kan plaatsvinden. In deze management letter hebben wij daarom 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 2020 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 Geertruidenberg:

- 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. Om het resterende risico te beperken beoordelen wij schattingsprocessen en bijzondere journaalposten in detail;
- Het niet naleven van de Europese aanbestedingsregels;
- De gevolgen van ongeautoriseerde handelingen in Key2Financiën wegens een omvangrijk aantal superusers. Hiervoor verwijzen wij naar hoofdstuk 5 in de management letter.

In onze aanpak steunen wij, daar waar mogelijk, op de interne beheersing in de significante processen van de gemeente. Daarbij maken wij, indien mogelijk, gebruik van uw eigen verbijzonderde interne controle (VIC).
In het kader van onze controle hebben wij de volgende processen beoordeeld:

- De interne Planning & Control-cyclus;
- Het subsidieproces;
- Het inkoopproces (incl. aanbestedingen);
- Het proces rondom grondexploitaties (schattingsproces en grond aan- en verkopen);
- De beheersing van verbonden partijen;
- Het proces omtrent IT/automatisering.

Voor onder andere de processen treasury, personeel en omgevingsvergunningen zijn de procesbeschrijvingen nog niet geactualiseerd en hebben wij ons in ons oordeel gebaseerd op de procesbeschrijvingen van vorig jaar.

Natuurlijk zijn er meerdere processen te onderkennen die zowel door de gemeente worden uitgevoerd als zijn uitbesteed, ook met financiële gevolgen. Voorbeelden zijn het proces t.a.v. lokale heffingen, verhuur en diverse kleinere (schattings-)processen. Op basis van onze ervaring, de kwaliteit en omvang van deze processen en om efficiency redenen hebben wij deze echter niet procesmatig / systeemgericht getoetst, maar zullen wij (achteraf) gegevensgerichte werkzaamheden uitvoeren in de vorm van steekproeven / deelwaarnemingen, cijferanalyses, verbandscontroles etc. Bij de voorbereiding van de jaarrekeningcontrole maken wij afspraken over de resterende werkzaamheden, aanpak en de hiervoor benodigde informatie.

4.1 Onze controle nog transparanter (2/2)

Onderscheid systeem- en gegevensgerichte controleaanpak

Onze aanpak afhankelijk van uw interne beheersing

Doordat wij nog niet op interne controles en de IT General Controls kunnen steunen, is onze controle-aanpak gegevensgericht van aard. Ten behoeve van de jaarrekeningcontrole 2020 hebben wij de interne beheersmaatregelen en wijzigingen ten opzichte van vorig jaar beoordeeld om de controle-aanpak voor de jaarrekening 2020 te kunnen bepalen.

Om een systeemgerichte controle-aanpak te kunnen hanteren, worden hoge eisen gesteld aan de interne controles in de processen en dienen wij eveneens op de IT General Controls te kunnen steunen. Zo lang wij niet kunnen steunen op de interne beheersingsmaatregelen in de organisatie, zijn wij genoodzaakt (omvangrijkere) deelwaarnemingen te verrichten en verrichten wij minimale werkzaamheden aan de interne beheersing.

Criteria:
- Voldoende functiescheiding
- Voldoende beheersmaatregelen
- IT-beheersing op orde
- Toetsing door verbijzonderde interne controle

Uitwerking controlestrategie per proces

Voor elk proces beoordelen wij de volgende onderdelen:
- **Controle technische functiescheiding (CTFS):** Is er binnen de primaire processen sprake van voldoende functiescheiding?
- **AO/IB:** Is sprake van een actueel 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?

Indien al deze vragen positief kunnen worden beantwoord, is de organisatie optimaal in control en kunnen ook wij gebruik maken van uw eigen interne beheersing. De vaak tijdrovende en gedetailleerde gegevensgerichte werkzaamheden (die ook nog eens achteraf plaatsvinden), kunnen dan beperkt blijven tot een minimum.

Samenvatting effectiviteit van de processen

In het overzicht op de volgende pagina geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook hoofdstuk 5 t.a.v. IT-omgeving) en welke detailbevindingen wij per proces hebben geconstateerd.

De beheersorganisatie is in opzet voldoende

Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat binnen de processen sprake is van minimaal noodzakelijke primaire functiescheiding. Tevens is binnen de processen sprake van interne beheersmaatregelen. Deze maatregelen worden echter niet toereikend genoeg vastgelegd, waardoor achteraf niet direct herleidbaar 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 wat betreft onze controle nog niet op de processen steunen en bestaat onze controleaanpak overwegend uit gegevensgerichte werkzaamheden. Voor de processen Wmo, BUIG en inkopen steunen wij op de werkzaamheden van de verbijzonderde interne controle en voor de processen subsidies en belastingen is een gegevensgerichte controle-aanpak efficiënter.

Aandachtspunt blijft de vastlegging van prestatielevering

Voorgaand jaar hebben wij gerapporteerd over het voornemen van de gemeente Geertruidenberg ten aanzien van de vastlegging prestatielevering bij inkopen. De voorwaarde die de gemeente hierbij stelde, is dat de prestatielevering eerst consequent goed moet worden vastgelegd bij factuurcontrole. Deze bevinding was reeds voorgaand jaar geconstateerd door uw medewerker interne controle. Uit de interne controles die in 2020 zijn uitgevoerd blijkt dat hierin vooralsnog geen verbeteringen hebben plaatsgevonden. Mogelijk biedt de BADO-notitie ‘Vastlegging en onderbouwing prestatielevering bij inkopen door decentrale overheidsorganisaties’ handvatten voor de gemeente bij de verdere invulling binnen de organisatie. Hierover hebben wij ten tijde van de interim-controle reeds gesproken met de ambtelijke organisatie.

4.2 Effectiviteit processen

PROCES	CTFS	AO/IB	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Planning & Controle			n.v.t.	Er is sprake van een adequaat functionerende planning & control cyclus; memoriaalboekingen en begrotingswijzigingen worden door financieel medewerkers opgesteld en transitorische posten worden door uw controller gecontroleerd. Niet alle memoriaalboekingen worden (zichtbaar) gecontroleerd/vastgelegd, waardoor wij de memoriaalboekingen middels data-analyse controleren.
Subsidies				Er is sprake van een minimaal noodzakelijke (primaire) functiescheiding. Binnen het subsidieproces zijn echter geen controlemaatregelen waar wij op kunnen steunen. Van belang is dat de controlemaatregelen zichtbaar worden vastgelegd, zoals de toets of de subsidiebeschikking aan de subsidievordering voldoet en de toets of er geen sprake is van een overheidsopdracht die aanbesteed had moeten worden.
Inkopen & betalingen				In opzet is sprake van een toereikende beheersmaatregel. Ten tijde van de interimcontrole waren de verbijzonderde interne controles voor de eerste twee kwartalen van 2020 afgerond. Uit deze interne controle is gebleken dat, ondanks de in 2019 genomen acties naar aanleiding van de bevindingen uit de interne controles, verplichtingen nog niet (structureel) worden aangemaakt en dat prestatieonderbouwing nog altijd onvoldoende wordt vastgelegd. Wij concluderen dat nog geen opvolging heeft plaatsgevonden van de vorig jaar geconstateerde bevindingen binnen het inkoopproces.
Aanbestedingen				Er is sprake van een mandaatregeling en budgethoudersregeling binnen de gemeente welke dateren uit 2017. Binnen het aanbestedingsproces is geen sprake van beheersmaatregelen en lijnmanagers kunnen zelf aanbestedingen doen. Het aanbestedingsproces, inclusief het aanmaken van verplichtingen, maakt onderdeel uit van de VIC inkopen. Er vindt een interne controle plaats op nieuwe, in het boekjaar, aangegane verplichtingen. Deze interne controle is nog niet als zodanig concreet verwoord en opgenomen in het IC-plan. Wel wordt door uw controller achteraf een spendanalyse uitgevoerd om onrechtmatige aanbestedingen, die niet zijn gemeld bij het inkoopbureau en in de interne controle zijn opgenomen, te constateren. Wij constateren dat het proces ongewijzigd is ten opzichte van vorig jaar.
Personeel				Van het personeelsproces is nog geen geactualiseerde procesbeschrijving aanwezig. Onze bevindingen uit de controle 2019 blijven daarmee onverminderd van kracht; er is sprake van minimaal noodzakelijke functiescheiding, maar beheersmaatregelen zijn onvoldoende toetsbaar. De verbijzonderde interne controles zijn ten tijde van de interim-controle nog niet afgerond.
Grondexploitaties incl. verkopen en aankopen			*	Binnen het proces is sprake van minimaal noodzakelijke functiescheiding. Beheersmaatregelen rondom de actualisatie van grondexploitaties zijn echter niet zichtbaar. De nota grondbeleid (eind 2019) en de exploitatieoverzichten en uitgangspunten (eind 2020) zijn geactualiseerd. De VIC op grondexploitaties, aan- en verkopen is in lijn met het interne controleplan ten tijde van de interimcontrole nog niet uitgevoerd.
Sociaal Domein (Jeugd, Wmo, BUIG)				Er is sprake van een minimaal noodzakelijke (primaire) functiescheiding. Dit proces is onveranderd ten opzichte van voorgaand boekjaar. De in het proces opgenomen controlemaatregelen worden door de consulenten zelf uitgevoerd en zijn onvoldoende om voor de controle op te kunnen steunen. Voor de VIC op BUIG en Wmo wordt gebruik gemaakt van de kennis en expertise van een interne controlemedewerker van een buurgemeente.
Belastingen			n.v.t.	Er is sprake van een minimaal noodzakelijke (primaire) functiescheiding. Dit proces is onveranderd ten opzichte van voorgaand boekjaar. Voor onze controle is een totaalaansluiting efficiënter, waardoor wij de VIC voor dit proces niet hebben beoordeeld.
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. Wel is in 2019 door de gemeenteraad de financiële richtlijnen begroting 2021 verbonden partijen alsmede de beleidskaders verbonden partijen vastgesteld. In 2020 zijn geen nieuwe gemeenschappelijke regelingen opgericht.
ICT/automatisering	n.v.t.			Voor een overzicht van de bevindingen verwijzen wij naar hoofdstuk 5.

Proces is ontoereikend, meerdere bevindingen en aanbevelingen. Risico x impact is hoog.

Proces is toereikend, één of enkele aanbevelingen resteren. Risico x impact is middel.

Proces is adequaat, enkel aanbevelingen ter verdere optimalisatie. Risico x impact is laag.

5. IT-beheersing

5.1 Externe ontwikkelingen

5.2 IT-beheersing

5.3 Bevindingen IT-beheersing | Key2Financiën

5.4 Actuele IT-ontwikkelingen vanuit onze natuurlijke adviesrol

5.5 Ontwikkelingen en risico's van cloudoplossingen

5.1 Externe ontwikkelingen

Toenemende dreiging bij verdergaande digitalisering

Cybersecurity

Organisaties en consumenten krijgen door de toenemende digitalisering, 'Big Tech' en globalisering steeds meer te maken met dreigingen in het cyberdomein. Cybercriminaliteit, activisme, terreur en statelijk handelen kunnen leiden tot incidenten met een negatief effect op de beschikbaarheid, integriteit en/of vertrouwelijkheid van de digitale gegevensverwerking en daarmee uitmonden in reputatieschade, betrouwbaarheid van gebruikte gegevens en zelfs financiële of fysieke schade. Daarbij stelt wet- en regelgeving (en richtlijnen) in toenemende mate eisen aan beveiliging van informatie en geautomatiseerde gegevensverwerking, bijvoorbeeld als onderdeel van privacywetgeving of wetgeving aangaande computercriminaliteit.

Het is daarom van belang voor organisaties om zicht te hebben op de (belangrijkste) cyberrisico's en passende maatregelen te treffen tegen deze risico's. Hierbij dient de organisatie onder meer aandacht te besteden aan:

- Het adequaat beleggen van taken en verantwoordelijkheden aangaande cybersecurity;
- Het kunnen identificeren van dreigingen, kroonjuwelen, kwetsbaarheden en het hieruit volgende cyberrisico voor de organisatie;
- Het inrichten van beveiligingsmaatregelen en beveiligingsbewustzijn om cyberincidenten te voorkomen en/of impact hiervan te beperken;
- Het inrichten van detectiemogelijkheden om pogingen tot of de gevolgen van ongeautoriseerde handelingen te detecteren;
- Het opstellen van een reactieplan en inrichten van activiteiten om adequaat te reageren op (de gevolgen van) een cyberincident en de nadelige effecten hiervan te beperken;
- Het opstellen van een herstelplan en inrichten van activiteiten om in geval van een cyberincident de continuïteit van de organisatie te waarborgen of herstellen en de nadelige effecten te corrigeren.

Aandacht voor informatiebeveiliging en cybersecurity

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

5.1 Externe ontwikkelingen

‘Veilig’ thuiswerken tijdens COVID-19

Veilig thuiswerken tijdens COVID-19

Door de uitbraak van de COVID-19 was het advies voor werkend Nederland: werk zo veel als mogelijk thuis. Deze overheidsmaatregel lijkt relatief eenvoudig, maar heeft meer impact op uw organisatie dan op het eerste oog lijkt. Veel organisaties boden reeds mogelijkheden om te werken op afstand, echter door COVID-19 is de omvang en behoefte in zeer korte tijd enorm toegenomen. Hierdoor is het voor veel organisaties niet mogelijk geweest om alle risico’s die hiermee gepaard gaan goed (onderbouwd) te overwegen. Nu de situatie zich op het vlak van thuiswerken redelijk stabiliseert is het goed om zicht te hebben of te krijgen op deze risico’s en passende maatregelen te treffen en effectiviteit van deze maatregelen te monitoren.

Hierbij dient u concreet extra aandacht te besteden aan de volgende thuiswerk risico’s:

- Bewustzijn; De grenzen tussen privé en werk vervagen. De aandacht van uw medewerkers moet worden verdeeld over de thuissituatie, het huishouden en werk. Kwaadwillenden spelen in op de toename in momenten van onoplettendheid en voor u het weet heeft een medewerker toch op die malafide link geklikt of gereageerd op die telefonische oplichting.
- Beveiliging van externe toegang; De noodzaak om IT systemen via het internet te ontsluiten is explosief toegenomen. Dat betekent ook dat de ‘voordeur’ van deze systemen door meer mensen en ook kwaadwillende te benaderen zijn. Het is belangrijk om voldoende maatregelen te treffen om deze ‘buiten de deur’ te kunnen houden.
- IT support; Niet alleen uw medewerkers hebben te maken met de thuiswerksituatie, uw IT medewerkers en dienstverleners ook. In korte tijd hebben zij thuiswerken moeten inrichten en faciliteren. Dit gaat ten koste van regulier beheer. Daarnaast kunnen zij uw medewerkers niet de normale ondersteuning bieden bij problemen en lopen zij tegen thuiswerkproblemen die ook voor hun nieuw zijn of door gebruik van thuisapparatuur niet direct oplosbaar. Duidelijke afspraken die toezien op de gewijzigde vorm en omvang van ondersteuning helpen problemen voorkomen.
- Samenwerken op afstand; Samenwerken op afstand vraagt om inzet van samenwerking technologieën, zoals videobellen, online documenten delen en andere hulpmiddelen. Deze technologieën en het gebruik van thuisapparatuur bieden veel mogelijkheden en creëren tegelijkertijd nieuwe risico’s voor privacy en beveiliging. De risico’s van deze hulpmiddelen ten aanzien van beveiliging en privacy dienen (voor gebruik) geëvalueerd en afgewogen geworden tegen de mogelijkheden en voordelen.

Al deze risico’s zijn niet nieuw, zeker niet wanneer u al mogelijkheden tot thuiswerken aan uw medewerkers aanbood. Echter de omvang en snelheid waarmee het gebruik zich ontwikkelt nemen door de situatie een vogelvlucht en vragen uw risicobeheersing daarin mee te bewegen! Deze snelheid heeft gezorgd voor een periode waarin tijdelijke oplossingen onder hoge druk zijn ingericht. Omdat frequenter thuiswerken nu wordt gevraagd en door ervaren voordelen naar verwachting ook zal blijven zult u structurele maatregelen moeten treffen en zo bouwen aan een veilig fundament.

5.2 IT-beheersing

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

Beoordeelde systemen:
▶ Key2Financiën

Detailbevindingen IT

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. 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 4).

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 aanvullende (gegevensgerichte) werkzaamheden noodzakelijk om aan te tonen dat er zich geen risico's of fouten hebben voorgedaan.

Toelichting status IT General Controls

Het schema op de volgende pagina bevat een weergave van de status van de opzet en het bestaan van de IT General Controls in het huidige jaar binnen het door ons in het kader van de jaarrekeningcontrole onderzochte systeem, zijnde Key2Financiën. In dit schema zijn onze bevindingen tekstueel toegelicht per item, verdeeld naar: Logische toegangsbeveiliging, Change management en Continuïteit. Een toelichting van de relevante detailbevindingen met betrekking tot de IT General Controls en overige IT-gerelateerde bevindingen treft u hierna aan.

Vanuit onze natuurlijke adviesfunctie sluiten wij het hoofdstuk van IT-beheersing af met de mogelijkheden van data-analyse en processmining en de ontwikkelingen en risico's van cloudoplossingen. Cloudoplossingen zijn een hot topic in de sector.

5.3 Bevindingen IT-beheersing | IT General Controls

Detailbevindingen: ten opzichte van vorig jaar is de

PROCES	2020
Logische toegangsbeveiliging	
1. Procedure autorisatiebeheer	
2. Periodieke controle op juistheid ingerichte autorisaties	
3. Identificatie van gebruikers voor toegang tot systemen en data	
4. Wachtwoordbeleid (authenticatie)	*
5. Administrator- en Superuser-accounts	*
Change management	
1. Wijzigingsbeheer	
2. Gescheiden omgevingen	
Continuïteit	
1. Fysieke omgeving	
2. Back-up	
3. Restoretest	

KORTE OMSCHRIJVING BEVINDINGEN	
Logische toegangsbeveiliging	
1	Er is sprake van een structurele procedure met betrekking tot in- en uit dienst treding van medewerkers. Een normpositie om rechten toe te kennen aan nieuwe gebruikers ontbreekt echter. Binnen dit proces hebben geen wijzigingen plaatsgevonden t.o.v. vorig jaar.
2	Er is geen sprake van een normpositie die gehanteerd wordt bij de periodieke review op de juistheid van ingerichte autorisaties. Het risico bestaat dat dat een functionaris over meer bevoegdheden beschikt dan uit hoofde van de functie noodzakelijk is.
3	Geen significante bevindingen.
4	Het wachtwoordbeleid van Key2Financiën voldoet aan de BDO Best Practice norm alsmede aan de BIO norm.
5	Gebruikers met de autorisatie FFISAU20 beschikken over superuser-rechten. Vanwege het aanstellen van een nieuwe applicatiebeheerder is er sprake van vier accounts (2019: drie) met superuser-rechten, waarvan één niet persoonsgebonden account. Wij hebben begrepen dat in 2021 dit aantal wordt verminderd.
Change management	
1	Er hebben geen wijzigingen plaatsgevonden ten opzichte van vorig jaar. De aanbevelingen uit onze managementletter 2019 blijven onverminderd van kracht.
2	Er hebben geen wijzigingen plaatsgevonden ten opzichte van vorig jaar. De aanbevelingen uit onze managementletter 2019 blijven onverminderd van kracht.
Continuïteit	
1	Geen significante bevindingen.
2	Geen significante bevindingen.
3	Er hebben geen wijzigingen plaatsgevonden in het proces rondom het terugzetten van back-ups. We adviseren een inhoudelijke controle uit te voeren op de data integriteit van de uitkomsten van de restoretest.

onvoldoende verbeterpunten voldoende

* Aanvullend hebben wij in het kader van de jaarrekeningcontrole het wachtwoordbeleid en de superusers GISVG en ADP beoordeeld. Het wachtwoordbeleid van beide applicaties wordt als toereikend aangemerkt. Wij adviseren bij GISVG echter wel een maximum aantal inlogpogingen te hanteren.
Binnen GISVG betreffen de superusers allen medewerkers die gerelateerd zijn aan de ICT-afdeling. Binnen ADP beschikken beide salarisadministrateurs echter over superuser-rechten en classificeren wij deze als ontoereikend.

5.4 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol

Data-analyse en process mining als mogelijke innovaties in de interne en externe controle

Voordelen en randvoorwaarden

Laagdrempelige en visuele data-analyses bieden nieuwe perspectieven op het proces

Data-analyse en process mining

In de praktijk zien wij dat steeds vaker dat de interne en/of externe controle gebruik maakt (of wil gaan maken) van geautomatiseerde controles. Data-analyse en process mining zijn voorbeelden van geautomatiseerde en gegevensgerichte controles die grote hoeveelheden data uit de geautomatiseerde systemen kunnen analyseren en controleren. Bij data-analyse ligt de nadruk op de kenmerken en afwijkingen in de gegevens, terwijl bij process mining het accent ligt op het proces die de data heeft doorlopen.

Daarnaast zijn er (verschillende soorten) nieuw ontwikkelde technieken op basis van het zogenaamde machine learning, waarbij zonder manuele tussenkomst gegevens volledig worden geïnterpreteerd, geanalyseerd en gecontroleerd. De intern of externe controle kan zich dan richten op de gerapporteerde uitzonderingen en mogelijke risico's in de data.

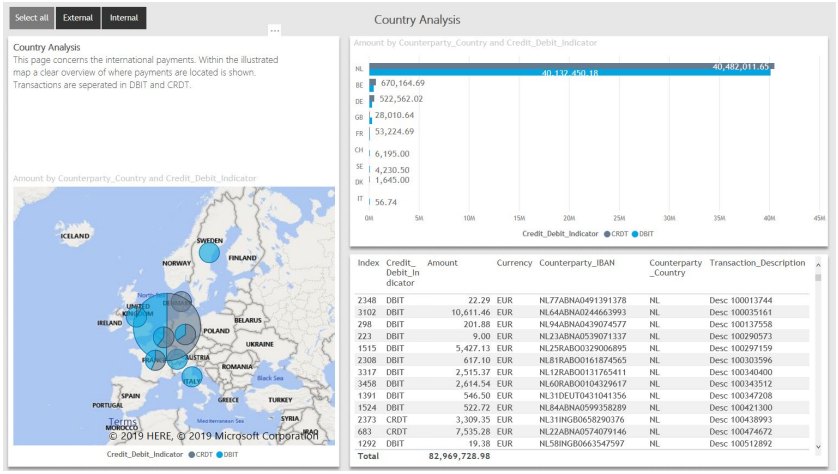
Het grote voordeel van data-analyse is dat de interne / externe controle niet plaatsvindt door middel van statistische steekproeven / deelwaarnemingen, maar dat alle data integraal kan worden geanalyseerd en gecontroleerd.

Afhankelijk van de in te zetten data-analyses zijn een aantal randvoorwaarden vereist om de betrouwbaarheid en juistheid van de data te waarborgen. In de basis dienen minimaal de IT General Controls rondom administrators en superusers, identificatie en wachtwoordinstellingen adequaat te zijn ingericht.

Wij hebben diverse data-analyses ontwikkeld op de veel voorkomende systemen bij gemeenten, zoals Key2Financien, BNG en we werken aan een data-analyse op Suite4Sociaal Domein.

Daarnaast werken wij aan innovaties waarbij grote handmatige steekproeven deels of volledig kunnen worden geautomatiseerd.

Het plaatje hiernaast geeft een voorbeeld van een visueel weergegeven data-analyse van betalingsgegevens, waaronder bijvoorbeeld het inzicht in buitenlandse betalingen.



Index	Credit_Debit_Indicator	Amount	Currency	Counterparty_IBAN	Counterparty_Country	Transaction_Description
2348	DBIT	22.29	EUR	NL77ABNA0491391378	NL	Desc 100013744
3102	DBIT	10,611.46	EUR	NL64ABNA0244663993	NL	Desc 100035161
298	DBIT	201.88	EUR	NL94ABNA0439074577	NL	Desc 100137558
223	DBIT	9.00	EUR	NL23ABNA0539071337	NL	Desc 100290573
1515	DBIT	5,427.13	EUR	NL25RABO0329006895	NL	Desc 100297159
2308	DBIT	617.10	EUR	NL81RABO0161874565	NL	Desc 100303596
3317	DBIT	2,515.37	EUR	NL12RABO0131765411	NL	Desc 100340400
3458	DBIT	2,614.54	EUR	NL60RABO0104329617	NL	Desc 100343512
1391	DBIT	546.50	EUR	NL31DEUT0431041356	NL	Desc 100347208
1524	DBIT	522.72	EUR	NL84ABNA0599358289	NL	Desc 100421300
2373	CRDT	3,309.35	EUR	NL31INGB0658290376	NL	Desc 100438993
683	CRDT	7,535.28	EUR	NL22ABNA0574079146	NL	Desc 100474672
1292	DBIT	19.38	EUR	NL58INGB0663547597	NL	Desc 100512892
Total		82,969,728.98				

5.5 Ontwikkelingen en risico's van cloudoplossingen

"The cloud is just someone else's computer"

Digitale overheid

Cloud computing is inmiddels stevig ingeburgerd bij overheidsinstanties en wordt steeds innovatiever toegepast, denk aan Smart Cities. Steeds meer overheidsinstanties gaan over tot het opstellen van grondige cloud strategieën.

Inmiddels gebruikt ruim driekwart van de organisaties een hybrid-cloud- of multi-cloud-model. Deze modellen bieden de voordelen van cloud computing, maar streven tegelijkertijd na de hieruit voortkomende risico's te mitigeren. Te denken valt hierbij aan risico's op het gebied van cybersecurity en dataprivacy, maar ook aan overmatige afhankelijkheid van leveranciers.

De voortgaande digitalisering gaat geen enkel organisatieproces voorbij. Ook de inrichting en het beheer van de IT-infrastructuur niet; in toenemende mate wordt de infrastructuur software-defined. Beschikbaarheid van IT blijft derhalve kostbaarder worden. Dit onderstreept te meer de noodzaak van het in staat zijn om data binnen korte tijd volledig te kunnen herstellen. Public cloud-leveranciers bieden hiertoe kwalitatief goede mogelijkheden.

Cloud computing is niet zonder risico's

Transitie naar cloud
Een veel voorkomende valkuil is het onderschatten van de data-migratie en het realiseren van de aansluiting van de cloud op bestaande oplossingen. Dit resulteert in hogere kosten dan begroot. Daarnaast vergt de 'nieuwe' regie-rol op ICT wezenlijk andere competenties dan het traditioneel functionerend houden van de IT-omgeving.

Leverancier 'lock-in'
Ook neemt de afhankelijkheid van leverancier ten opzichte van on-premise software toe. Dit kan zich in geval van gebrekkige governance uiten in onverwacht hoge kosten en hogere drempels om van leverancier te wisselen.

Informatiebeveiliging en privacy
Een ander groot risico is dat de data onvoldoende beveiligd is. Als gegevens onvoldoende beveiligd zijn kunnen ze gehackt worden of in handen komen van derden met enorme imagoschade en boetes als gevolg. Ook is vaak onbekend waar de data wordt opgeslagen. Het kan dus zo zijn dat uw data wordt opgeslagen in een land waar ze het niet zo nauw nemen met de privacy-wetgeving.



5.5 Ontwikkelingen en risico’s van cloudoplossingen

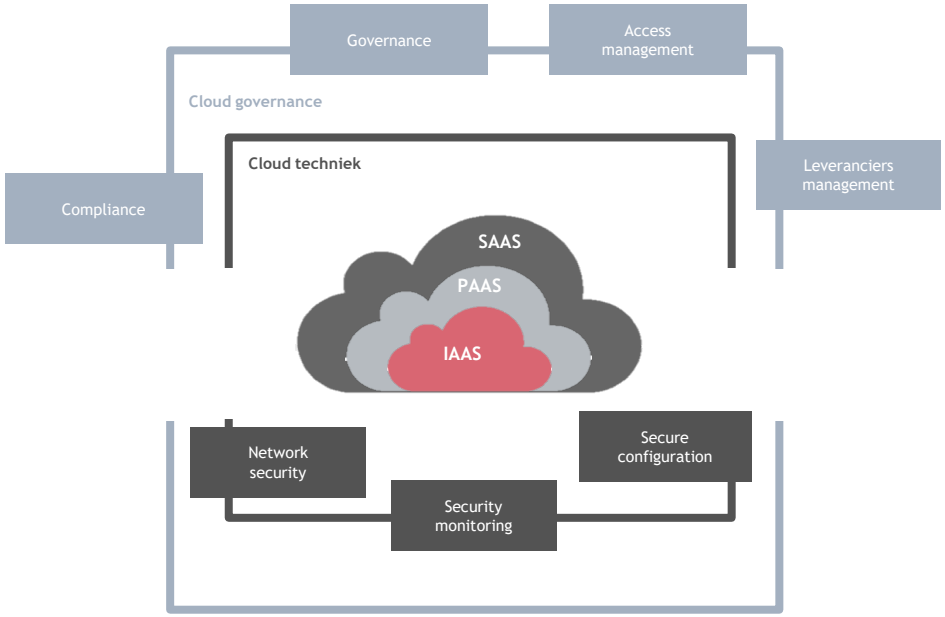
“The cloud is just someone else’s computer”

De 7 aandachtsgebieden van cloud

Wij hebben zeven aandachtsgebieden geformuleerd om grip te houden op cloud risico’s:

1. **Cloud Governance**: Duidelijke afstemming en vastlegging van verantwoordelijkheden tussen uw organisatie en de cloudleverancier zijn belangrijk om efficiënte bedrijfsvoering en informatiebeveiliging te borgen in de processen. Heldere afspraken omtrent performance, processen en escalaties met de cloudleverancier en een exit procedure zijn key;
2. **Access Management:** Toegang tot de cloudoplossing heeft u meestal zelf in beheer. Een helder proces zorgt ervoor dat medewerkers alleen toegang hebben tot de data die zij nodig hebben voor hun functie en dat ongeautoriseerde personen er niet bij kunnen;
3. **Compliance:** Het gebruik van cloudoplossingen is steeds meer aan regels gebonden, ook in internationale context. Een overzicht van welke cloudoplossingen u gebruikt en in welke landen de data wordt opgeslagen en verwerkt helpt u om te bepalen welke wet- en regelgeving op uw organisatie van toepassing is;
4. **Leveranciersmanagement:** Als regieorganisatie dient u actief de dienstverlening, performance, beveiliging en kosten van uw belangrijkste cloudleveranciers te monitoren. Dat kan bijvoorbeeld door het opvragen, beoordelen en opvolgen van service level rapporten en assurancerapporten;
5. **Secure Configuration:** Voorkomen is beter dan genezen: het veilig configureren van cloudsystemen helpt u om uw bedrijfsvoering veilig te houden. De systemen in de cloud worden veilig geconfigureerd volgens geldende standaarden en periodiek geëvalueerd;
6. **Network Security:** Er moet een veilige verbinding zijn met de cloudoplossing zodat verkeer niet onderschept kan worden. Penetratietesten helpen u om zowel externe als interne kwetsbaarheden op te sporen;
7. **Security Monitoring:** Een SOC- of SIEM-oplossing monitort verdacht verkeer en rapporteert over verdachte events, zodat u op de hoogte bent wat in uw IT-omgeving plaatsvindt.

Graag gaan wij met u in gesprek over de status van cloud binnen uw organisatie en wat voor effect dit heeft en/of kan hebben op de interne beheersing en continuïteit van de dienstverlening.



bdo.nl