MANAGEMENTLETTER

Veiligheidsregio Kennemerland

BDO

Aanbiedingsbrief

Veiligheidsregio Kennemerland
t.a.v. het bestuur
Postbus 5514
2000 GM HAARLEM

Amstelveen, 18 januari 2021
Kenmerk: BvV/JvS/NS/JvdP/HV/AA21-0044

Geacht bestuur,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2020 van de Veiligheidsregio Kennemerland (hierna “VRK”) brengen wij u met deze managementletter 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 managementletter is daarom van nature kritisch van aard. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelf controlerend vermogen van uw organisatie, maar dit betekent niet dat de VRK momenteel niet in control is.

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

Wij willen de organisatie bedanken voor de prettige samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,

BDO Audit & Assurance B.V.
namens deze,

A.P. (Bas) van Veen RA

Inhoudsopgave

1. Dashboard

1 Dashboard

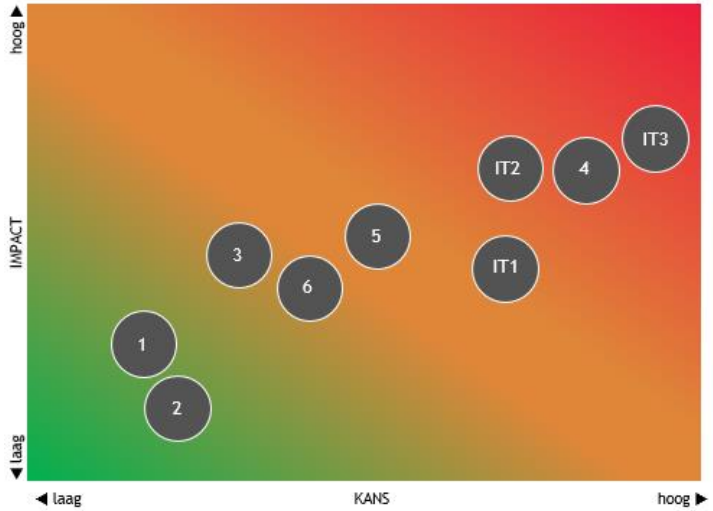
UW INTERNE BEHEERSING

- In het kader van onze controle hebben wij de effectiviteit van de voor onze controle relevante processen beoordeeld.
- Voor een organisatie met de omvang van Veiligheidsregio Kennemerland zou de norm volgens ons moeten zijn dat de processen in opzet, bestaan en werking (inclusief IT) geen belangrijke leemtes kennen. De Veiligheidsregio voldoet aan deze norm. Wij kunnen daarbij nog niet altijd steunen op de interne beheersing in de processen; onze controle is daarmee hoofdzakelijk gegevensgericht en achteraf.
- Wij constateren dat een aantal aandachtspunten van voorgaand jaar zijn opgevolgd. Tegelijk zien wij dat de personele bezetting op interne controle minder robuust is dan voorgaande jaren. Daarbij merken we op dat de coronamaatregelen niet tot noemenswaardige veranderingen in (beheersing van) de processen heeft geleid.

BEHEERSING IT

- Tijdens onze interim-controle 2020 hebben wij beperkte verbeteringen in de inrichting en uitvoering van de IT General Controls geconstateerd.
- Op de meeste onderdelen (met name beheerrechten) resteren voor 2020 dezelfde bevindingen en aanbevelingen, waardoor voor onze controle niet gesteund kan worden op de beheersmaatregelen in de applicaties en processen.
- Dit jaar rapporteren wij aanvullend rondom ADP en Clavis.
- De belangrijkste bevindingen zijn:
  - De toekenning en review van gebruikersrechten is niet robuust genoeg en voor een aantal applicaties onvoldoende (IT1).
  - Er zijn gebruikers met beheerrechten actief in de lijn die betrokken zijn bij het relevante proces (IT2).

HITTE KAART



ONTWIKKELINGEN

- In 2021 of 2022 zal de rechtmatigheidsverantwoording worden ingevoerd. Momenteel zijn nog niet altijd beheersingsmaatregelen (zichtbare) in processen aanwezig. Hierdoor is het noodzakelijk de juistheid en rechtmatigheid van balansstanden en processen vast te stellen door controles achteraf. Het risico bestaat dat onrechtmatigheden niet tijdig worden gesignaleerd en niet kunnen worden gerepareerd.
- De notitie vastlegging en onderbouwing prestatielevering bij inkopen door decentrale overheidsorganisaties vraagt om beleid ten aanzien van controle en vastlegging (2.1).

VERBIJZONDERDE INTERNE CONTROLE

- Gedurende 2020 is er een interim-controller aangenomen om de werkzaamheden van de VIC uit te voeren en voor de toekomst vorm te geven.
- In de samenwerking met de financieel adviseurs werken we naar verdere verbetering van de tijdige afstemming van werkzaamheden en aanlevering van documentatie voor onze controle. In het bijzonder hebben we de sterkere controleaanpak en spendanalyse ten aanzien van de Europese aanbestedingen gezamenlijk afgestemd.
- Met het oog op de invoering van de rechtmatigheidsverklaring in 2021 kan de meerwaarde van de VIC voor de organisatie & onze controle verder worden vergroot. Naast de controle van de Europese aanbestedingen is de beheersing van de prestatielevering een ontwikkelstap.

DETAILBEVINDINGEN

1	Planning & Control - Vastlegging van controles en aansluitingen in de verder sterke planning & control cyclus kunnen nog meer de volledigheid van de processtappen borgen.
2	Planning & Control - Controles op de memoriaalboekingen niet altijd geheel zichtbaar.
3	Planning & Control - Inrichting interne controle voor rechtmatigheidsverantwoording, onder andere doorbreking ingerichte functiescheiding eerste halfjaar VeiligThuis en investeringsfacturen.
4	Aanbestedingen - Kennis van verscherpingen aanbestedingswetgeving onvoldoende geborgd in het proces.
5	Aanbestedingen - Ontbreken tijdige signalering van overschrijdingen.
6	Aanbestedingen - Controle contractinvoer in contractenmodule ontbreekt. Niet alle contracten zijn geregistreerd.
IT1	Procedure autorisatiebeheer niet robuust genoeg en voor aantal applicaties onvoldoende.
IT2	Administrator- en superuser-accounts toegekend aan eindgebruikers.
IT3	Beheersing voor de niet financiële applicaties is onvoldoende, waarbij ADP het gewenste inzicht niet biedt.

2. Ontwikkelingen en aandachtspunten

2.1 Gevolgen coronacrisis voor de jaarrekening 2020

Veiligheidsregio Kennemerland communiceert voldoende over effecten Corona

BDO corona-scan verstrekt

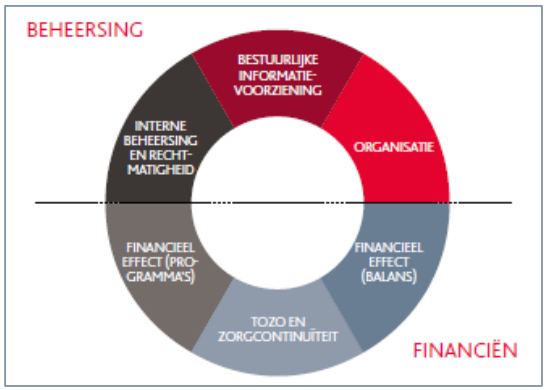
Toets naast financieel impact ook effect op interne beheersing en jaarrekening

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

Impactanalyse

De lange termijn impact van het coronacrisis op de maatschappij en economie zijn nog steeds hoogst onzeker. In de jaarrekening 2019 had de VRK, in lijn met de verslaggevingsrichtlijnen hieromtrent, een eerste toelichting opgenomen omtrent de coronacrisis. Daarnaast heeft de Veiligheidsregio ook in haar voortgangsverslag een analyse gemaakt van de mogelijke (financiële) gevolgen van de coronacrisis.

Om een goede inschatting te maken voor de mogelijke gevolgen van de coronacrisis voor de jaarrekening 2020 hebben wij een uitgebreide corona-scan lokale overheid opgesteld en gedeeld met de organisatie. Daarbij hebben wij onderscheid gemaakt naar de impact op enerzijds de beheersing en anderzijds op de financiën van de Veiligheidsregio.



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.

De VRK heeft de corona-scan ingevuld. Hieruit kwamen geen niet eerder door de VRK zelf geïdentificeerde risico's.

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 Veiligheidsregio na te gaan wat het effect van Corona is op de interne beheersing; zowel inzake de uitgaven als inkomsten (mogelijke extra verantwoordingseisen ten aanzien van bijdragen van het rijk).
- Wij adviseren de Veiligheidsregio niet alleen de programma's en taken te analyseren, maar ook mogelijke effecten van Corona op belangrijke balanspositie zoals vorderingen op derden. Daarbij ligt het voor de hand tevens aandacht te schenken aan mogelijke corona-effecten op het weerstandsvermogen van de Veiligheidsregio.

Op dit moment kijkt de commissie BBV naar mogelijke effecten van coronamaatregelen op de intern en externe controle van de rechtmatigheid. De onzekerheden en mogelijk aanvullende eisen die kunnen worden gesteld aan extra middelen kunnen tot gevolg hebben dat de controle een langere (doorloop-) tijd gaat vragen. Ook risico's in de naleving van bijvoorbeeld declaratievoorwaarden, waarderingen van balansposten, aanbestedingsrisico's door gewijzigde inkoop volumes etc. kunnen dit effect hebben (zie verder ook onze scan).

Bij de VRK zijn reeds stappen zijn gezet op het gebied van de identificatie en beheersing. Graag gaan/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.

2.2 Rechtmatigheidsverantwoording

Invoering rechtmatigheids-verantwoording 2021

Invoering naar onze mening een kans

Invoering rechtmatigheidsverantwoording met ingang van 2021 of 2022

In ons accountantsverslag van 2019 hebben wij aangegeven dat op termijn de rechtmatigheidsverantwoording ingevoerd wordt voor overheidsorganisaties. Op dit moment is de formele status nog steeds dat de rechtmatigheidsverantwoording wordt ingevoerd met ingang van 2021, echter kan dit met een jaar vertraagd worden. Of 1 januari 2021 daadwerkelijk de invoeringsdatum wordt hangt sterk af van het wetgevingstraject dat eind dit jaar wordt verwacht.

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 Veiligheidsregio Kennemerland immers zelf verantwoordelijk voor de rechtmatigheidsverantwoording en moet het bestuur 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.

De wijziging in de verantwoordelijkheden ten aanzien van rechtmatigheid betekent niet dat er minder rechtmatigheidscontroles moeten worden uitgevoerd, maar dat het dagelijks bestuur 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 dagelijks bestuur een getrouw beeld geeft.

Vanuit onze gesprekken begrijpen we dat de Veiligheidsregio haar opties en mogelijkheden momenteel nog aan het overwegen is. De komende periode zal zij dit vertalen in concrete plannen, om vervolgens de verantwoordelijkheden, controles en processen in te richten en uit te voeren. Wij gaan graag in gesprek over uw visie en plannen richting de prestatieverantwoording.

2.3 Actualiteiten BBV en SDO

Notitie prestatielevering bij inkopen door decentrale overheidsorganisatie

BBV Actualiteiten

De wijzigingen in het Besluit Begroting en Verantwoording van gemeenten en provincies (BBV) lijken dit jaar beperkt. Wij lichten ter voorbereiding op het jaarrekeningtraject 2020 hieronder alleen een van de SDO notities kort toe.

Notitie vastlegging en onderbouwing prestatielevering bij inkopen door decentrale overheidsorganisaties

De controle van de prestatielevering op inkopen heeft in de afgelopen jaren voor veel onduidelijkheid en discussie gezorgd bij meerdere overheidsorganisaties. Als reactie is door het BADO een notitie geschreven waarin handvatten geboden worden aan overheidsorganisaties en accountants. De notitie stelt onder andere dat:

a) De overheidsorganisatie is verantwoordelijk voor het bepalen van de norm en het inrichten van organisatie en processen om het risico op onrechtmatige betalingen te verkleinen. Afstemming met de accountant van de normen is sterk aanbevolen.
b) Bij de norm kan de overheidsorganisatie grenzen hanteren die aangeven, wanneer zwaardere dan wel lichtere eisen aan de onderbouwing van de prestatielevering gelden. Die grenzen zullen in de procesbeschrijving moeten zijn opgenomen. Het onderscheid wordt ingegeven door het risicoprofiel van de verschillende soorten inkopen.
c) De overheidsorganisatie moet aangeven hoe invulling gegeven wordt aan de beheersmaatregel, die de prestatielevering vaststelt alvorens een factuur betaalbaar te stellen.
d) De documentatie van de prestatielevering moet altijd voldoende en geschikt zijn.
e) Als een geselecteerde waarneming niet adequaat onderbouwd kan worden met voldoende en geschikte controle-informatie, dan heeft dit effect op het oordeel van de accountant en kan dit – afhankelijk van de aard en omvang van de fouten en onzekerheden - leiden tot een verdere uitbreiding van de deelwaarneming en extra werk.

Wij zien dat de Veiligheidsregio hier momenteel op acteert. Er kunnen hier nog verdere verbeteringen worden doorgevoerd door het opslaan van pakbonnen of andere leveringsbewijzen.

Wij benadrukken dat het inbedden van de norm in de processen essentieel is. Relevant in dit kader is dat functiescheiding nodig is tussen de initiatie van de inkoop, het plaatsen van de inkoop en het vaststellen van de levering. Deze functiescheiding en de onderbouwingen dienen goed gedocumenteerd zijn zodat de Veiligheidsregio intern haar rechtmatigheidsverantwoording kan afleggen (vanaf 2021) en wij ons oordeel kunnen vormen.

3. Bevindingen significante processen

3.1 Onze controle transparant (1/2)

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

Onze inschatting van de significante risico's

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 uw Veiligheidsregio:

- 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 significant risico benoemd. Als accountant moeten wij in onze werkzaamheden hier specifiek aandacht aan besteden. Wij zijn van mening dat binnen de Veiligheidsregio 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
  - Onterecht niet Europees aanbesteden.
  - Meer besteden dan geraamd als gevolg van een wezenlijke wijziging in het contract.

Onze inschatting van de risico's en belangrijkste processen

In onze aanpak is de insteek, daar waar mogelijk te steunen op de interne beheersing in de significante processen van de Veiligheidsregio. Vanuit onze rol als accountant maken wij een risico-inschatting op basis van de (voorgeschreven) materialiteit en zijn de volgende materiële processen onderkend:

Wij beoordelen de volgende processen

- De interne Planning & Control-cyclus
- Het inkoopproces
- Het aanbestedingsproces
- Het personeelsproces
- Het betalingsproces.

Natuurlijk zijn er meerdere processen te onderkennen, ook met financiële gevolgen. 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, verbands-controles, etc. Bij de voorbereiding van de jaarrekeningcontrole maken wij, evenals voorgaande jaren, afspraken over de resterende werkzaamheden, aanpak en de hiervoor benodigde informatie.

3.1 Onze controle transparant (2/2)

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

De beheersorganisatie is in opzet voldoende tot goed.

Wij kunnen nog niet altijd steunen op de interne beheersing; onze aanpak is daarmee hoofdzakelijk gegevens-gericht

Uitwerking controlestrategie per proces

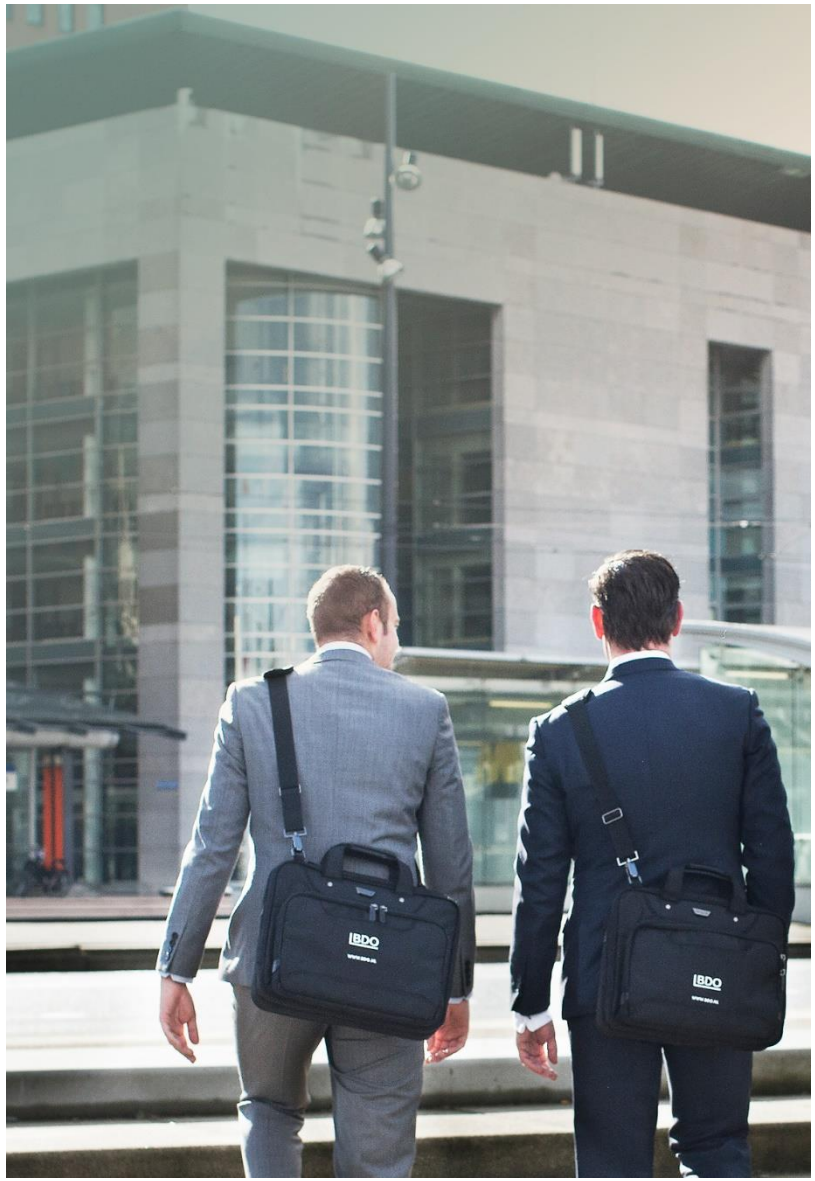
Voor elk proces beoordelen wij de volgende onderdelen:
- **AO/IB:** Is sprake van een actueel en toereikend procesbeschrijving met voldoende beheersmaatregelen?
- **IT-maatregelen:** Zijn in en rondom het systeem voldoende waarborgen getroffen t.a.v. de betrouwbaarheid van de gegevensverwerking?
- **VIC:** 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. Voor de Veiligheidsregio verrichten wij op alle processen aanvullende gegevensgerichte werkzaamheden.

Samenvatting effectiviteit van de processen

In de overzichten op de volgende pagina's geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook hoofdstuk 4 t.a.v. IT-omgeving) en welke belangrijkste detailbevindingen wij per proces hebben geconstateerd.

Op basis van onze uitgevoerde werkzaamheden komen wij op dit moment tot de conclusie dat de beheersorganisatie van de Veiligheidsregio (voor zover relevant voor de controle van de jaarrekening) in opzet voldoende scoort. De belangrijkste bevindingen zien toe op de aanbestedingen.



3.2 Effectiviteit processen

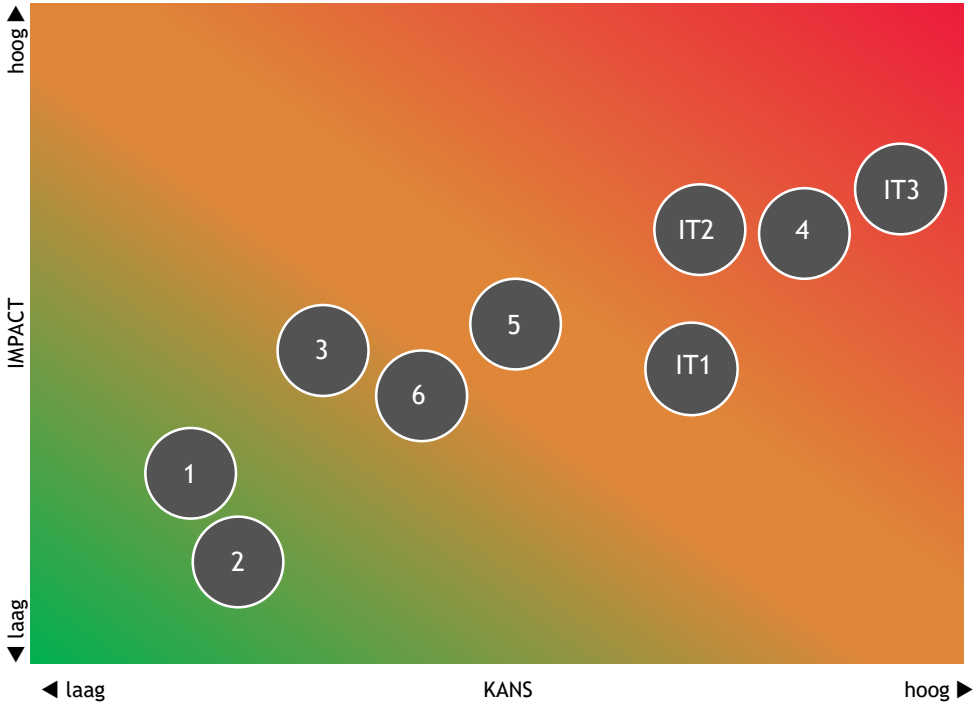
PROCES	OPZET AO/IB 2019	OPZET AO/IB 2020	WER-KING AO/IB	ITGC'S	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Planning & Controle				n.v.t	n.v.t	Het opstellen van de maandrapportages is ten opzichte van vorig jaar verbeterd, er zijn momenteel zichtbare controles op de maandrapportages en de verantwoordelijkheden worden verdeeld. In het structureren van de vastleggingen van controles binnen het begrotingsproces (inclusief BERAPs) zien wij nog verbeterpunten. Door structureler versiebeheer en een volledigheidschecklist kan de volgende stap gezet worden.
Inkopen					n.v.t	Wij hebben geconstateerd dat in de inrichting, weloverwogen, sprake is van ontbreken zichtbare functiescheiding op investeringen. Daarnaast constateren we dat ingerichte functiescheiding gedurende het eerste halfjaar voor facturen van VeiligThuis niet aanwezig was, maar dit achteraf is hersteld. Vanwege beide bovenstaande bevindingen hebben wij een aanvullende data-analyse en steekproef gepland.
Aanbestedingen				Niet getoetst	n.v.t	Er is geconstateerd dat het vereiste kennisniveau omtrent de aanbestedingswetging nog niet voldoende geborgd is binnen het aanbestedingsproces. De VRK is momenteel bezig om de contractadministratie op orde te brengen en met het aantreden van een interim-controller worden de controles uitgevoerd en vooral beleid en processen uitgezet naar de toekomst toe. Hierbij kunnen er verbeteringen worden aangebracht bij contractinvoer en signalering van overschrijdingen.
Personeel					n.v.t	De bevoegdheden en autorisaties zijn in ADP niet te achterhalen. De beheersing rond het systeem vraagt aandacht en maakt een systeemgerichte controle niet mogelijk.
ICT/ automatisering				n.v.t.	n.v.t.	Ten aanzien van ICT zijn door ons net zoals voorgaande boekjaren belangrijke aandachtspunten gesignaleerd (zie hoofdstuk 4).

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

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

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

3.3 Detailbevindingen



KORTE OMSCHRIJVING DETAILBEVINDINGEN	
1	Planning & Control - Vastlegging van controles en aansluitingen in de verder sterke planning & control cyclus kunnen nog meer de volledigheid van de processtappen borgen.
2	Planning & Control – Controles op de memoriaalboekingen niet altijd geheel zichtbaar.
3	Planning & Control - Inrichting interne controle voor rechtmatigheidsverantwoording, onder andere doorbreking ingerichte functiescheiding eerste halfjaar VeiligThuis en investeringsfacturen.
4	Aanbestedingen – Kennis van verscherpingen aanbestedingswetgeving onvoldoende geborgd in het proces.
5	Aanbestedingen - Ontbreken tijdige signalering van overschrijdingen.
6	Aanbestedingen – Controle contractinvoer in contractenmodule ontbreekt. Niet alle contracten zijn geregistreerd.
IT1	Procedure autorisatiebeheer niet robuust genoeg en voor aantal applicaties onvoldoende.
IT2	Administrator- en superuser-accounts toegekend aan eindgebruikers.
IT3	Beheersing voor de niet financiële applicaties is onvoldoende, waarbij ADP het gewenste inzicht niet biedt.

4. IT-beheersing

4.1 IT-beheersing

Wij beoordelen de betrouwbaarheid en continuïteit IT voor zover relevant voor de controle van de jaarrekening of door de veiligheidsregio gevraagd

Beoordeelde systemen:
- Unit 4 Business World
- Veiligheidspaspoort
- InPlanning
- ADP
- Clavis

Detailbevindingen IT gedeeld met de organisatie

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 managementletter zijn gericht geweest op het beoordelen van de opzet en het vaststellen van het bestaan van algemene IT-beheersmaatregelen. Wij hebben in samenwerking met onze IT-auditors een aantal van deze maatregelen beoordeeld voor Unit 4 Business World, VeiligheidsPaspoort, InPlanning, ADP en Clavis. Dit om de (potentiele) risico's van onbeheerste wijzigingen, ongeautoriseerde handelingen en verstoringen te kunnen vaststellen voor die systemen die gekoppeld zijn aan de voor ons relevantie processen en posten (zie hoofdstuk 3).

In dit hoofdstuk geven wij allereerst een samenvatting van onze bevindingen voor de genoemde applicaties. De detailbevindingen rondom deze systemen zijn met de organisatie afgestemd.

In de bijlagen gaan wij, vanuit onze natuurlijke adviesfunctie, in op een aantal actuele ontwikkelingen ten aanzien van de trend naar de cloud.

Logische toegangs-beveiliging Unit 4 Business World (criteria 1-5) nog deels ontoereikend

Change management (criteria 6-7) grotendeels toereikend.

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar de met de organisatie gedeelde detailbevindingen.

PROCES	2019	2020
1. Procedure autorisatiebeheer		
2. Periodieke controle op juistheid ingerichte autorisaties		
3. Identificatie van gebruikers voor toegang tot systemen en data		
4. Wachtwoordbeleid (authenticatie)		
5. Administrators en superusers		Vanaf juli
6. Wijzigingenbeheer updates		
7. Gescheiden omgevingen (ontwikkel-test-productie)		

onvoldoende verbeterpunten voldoende

KORTE OMSCHRIJVING RESULTATEN	
1	Een normpositie van de rechten per rol en de toegestane rollen per organisatorische functie is aanwezig (voldoet). T.a.v. uit dienst en tijdig intrekken van gebruikersaccounts hebben wij begrepen dat dit niet structureel tijdig wordt uitgevoerd/doorgegeven aan de applicatiebeheerder.
2	Vastgesteld dat een review van autorisaties naar de gebruikers en toegekende rollen in 2020 heeft plaatsgevonden (voldoet). Een periodieke review naar de juistheid onderliggende rechten per rol (a.d.h.v. de normpositie als basis) is in 2020 nog niet uitgevoerd.
3	Geen opmerkingen.
4	Geen opmerkingen.
5	Superuser accounts zijn per juni 2020 beperkt toegekend aan een strikt noodzakelijke groep gebruikers buiten de operationele organisatie (voldoet). Vóór juni 2020 beschikte een medewerker uit de operationele organisatie nog over deze rechten, wat in basis in het kader van functiescheiding onwenselijk is. Ten tijde van de controle is dit opgelost en wordt dit vanaf juni 2020 toereikend geacht.
6	Sinds 2019 is de regie meer naar Unit 4 geschoven. De leverancier beschikt wel over een SOC-assuranceverklaring met controls rondom change management. VRK acht daardoor testen minder noodzakelijk en heeft dit voor de 2 reguliere updates in 2020 niet zichtbaar uitgevoerd. Het SOC assurancerapport wordt nog niet zelf door de VRK beoordeeld.
7	Geen opmerkingen.

4.3 Bevindingen IT-beheersing | overige applicaties

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

Change management (criteria 6-7) nog ontoereikend.

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar de met de organisatie gedeelde detailbevindingen.

PROCES	InPlanning (registratie diensten)		Veiligheids-Paspoort (registratie toeslagen)		ADP (personeel)		Clavis (Veiligthuis)		CONCLUSIE T.A.V. DE CONTROLEAANPAK
	'19	'20	'19	'20	'19	'20	'19	'20	
1. Procedure autorisatiebeheer					n.v.t.		n.v.t.		De procedure autorisatiebeheer is niet sluitend en er is geen of beperkte vastlegging van een periodieke review van autorisaties.
2. Periodieke controle op juistheid ingerichte autorisaties					n.v.t.		n.v.t.		Periodieke reviews van gebruikers zijn niet uitgevoerd in 2020.
3. Identificatie van gebruikers voor toegang tot systemen en data					n.v.t.		n.v.t.		Clavis geen opmerkingen bij de overige applicaties gebruikers die niet herleidbaar zijn tot een persoon en/ of accounts waarvan die niet noodzakelijk zijn volgens de applicatiebeheerder(s).
4. Wachtwoordbeleid (authenticatie)					n.v.t.		n.v.t.		Er bestaan uitzonderingen op het ingerichte wachtwoordbeleid. Eisen ten aanzien van periodiek wijzigen, wachtwoordhistorie en een lock-out policy zijn niet aanwezig bij InPlanning en VP.
5. Administrators en superusers					n.v.t.		n.v.t.		Gebruikers met superuser rechten gevonden uit de operationele organisatie die wij in basis onwenselijk achten in het kader van functiescheiding. Bij Clavis is niet eenduidig zichtbaar wie ruime rechten bezit.
6. Wijzigingenbeheer updates					n.v.t.		n.v.t.		Wijzigingenbeheer updates en toezicht op kritieke IT-leveranciers is niet volledig ingericht.
7. Gescheiden omgevingen (ontwikkel-test-productie)					n.v.t.		n.v.t.		Geen opmerkingen.

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

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

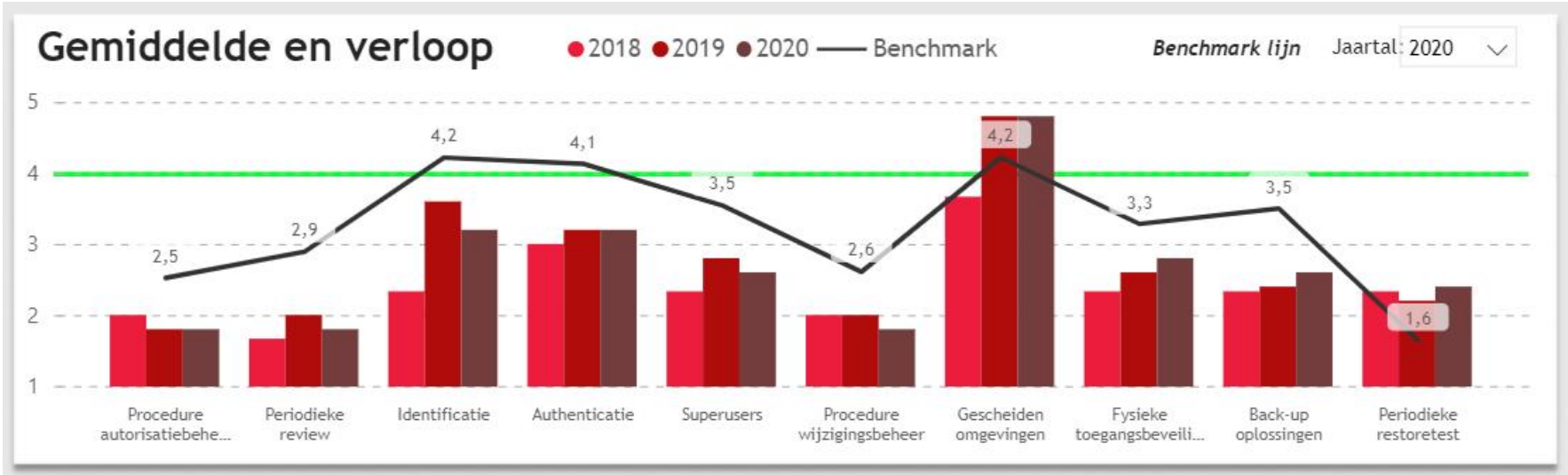
Proces is adequaat, enkel aanbevelingen ter verdere optimalisatie. Kans x impact is laag.

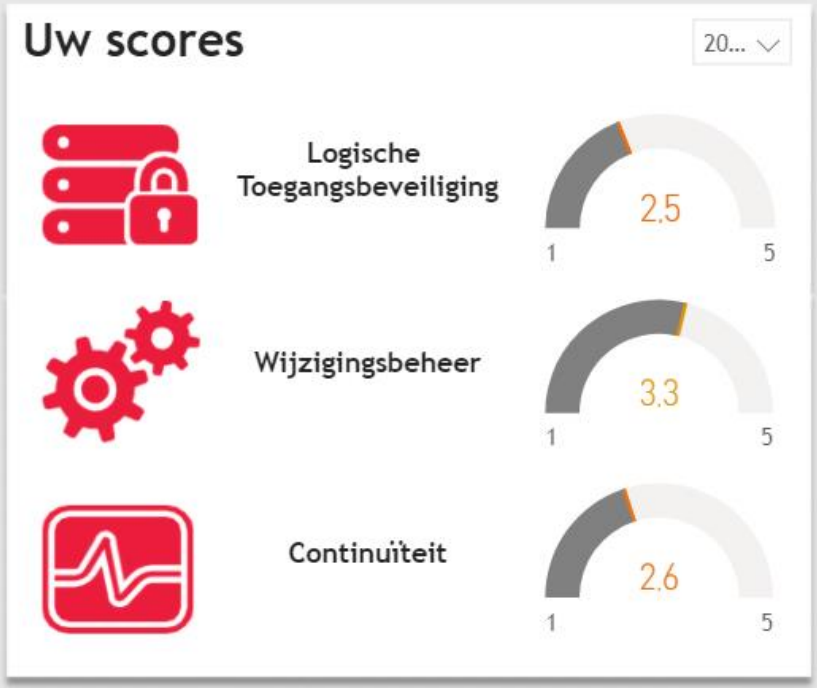
4.4 IT Audit | Benchmark Overheid

VRK scoort over alle applicaties samen onder zowel de benchmark als de norm. Voor Unit4BW scoort VRK vergelijkbaar met de benchmark op de financiële systemen (niet in deze weergave terug te zien)

Wij hebben een benchmark ontwikkeld welke uw scores afzet tegen het gemiddelde van onze klanten binnen de Overheidssector, voornamelijk gemeenten (70-100mio lasten). Een impressie van deze benchmark is hier weergegeven.

Graag presenteren wij u de aanvullende inzichten en gaan wij met u in gesprek over het vervolg.





Uitleg Benchmark

BDO

Op basis van onze kennis en inzichten die wij hebben opgedaan bij de uitvoering van IT audits hebben wij een benchmark ontwikkeld.
Deze benchmark geeft inzicht in de IT audit resultaten van uw organisatie afgezet tegen het gemiddelde van vijftig van onze klanten binnen de Overheidssector.
Bovendien laat deze benchmark zien hoe uw organisatie zich heeft ontwikkeld op het gebied van IT-beheersing over de afgelopen jaren.
Hierin is een score van 1 tot en met 5 per norm weergegeven waarbij BDO een score van minimaal 4 toereikend acht.

Deze pagina geeft een korte impressie van onze interactieve benchmark. Graag presenteren wij u de aanvullende inzichten en gaan wij met u in gesprek over het vervolg.

5. Interne controle

5.1 Interne controle

Eisen aan accountantscontrole en onze rapportages

Wij gaan graag het gesprek aan over uw ambities en de normen die gesteld kunnen worden aan uw interne beheersing in het licht van de rechtmatigheidsverantwoording door het dagelijks bestuur.

Afspraken gemaakt over versterking van de interne controle op de aanbestedingen

Inleiding en ambities

Ten behoeve van het realiseren van de doelstellingen en het sturend vermogen van de overheidsorganisatie is het van groot belang dat de processen in de basis op orde zijn, vanuit een goed werkend instrumentarium 'plan-do-check-act'. Het controlebewustzijn van medewerkers en een systeem van interne controles, gebaseerd op een gedegen risico-inschatting moet zijn gewaarborgd. Wij constateren dat Veiligheidsregio Kennemerland stappen heeft gezet in de beheersing, maar net als veel andere overheidsorganisaties op korte termijn (nog) niet in staat is gebleken de interne beheersing op het gevraagde niveau te krijgen. Dit betekent niet dat uw organisatie niet in control is, maar wel dat er ruimte is voor verbeteringen. In deze managementletter geven wij praktische handvatten om de interne beheersing nog verder te optimaliseren, rekening houdend met de omvang van uw organisatie.

Wij gaan graag met u in gesprek over uw ambities. Wij willen graag voorkomen dat de lat in onze controle-aanpak te hoog ligt/niet haalbaar lijkt en wij desondanks elk jaar hierover blijven rapporteren. De afweging ten aanzien van uw ambitie ligt primair bij de veilgheidsregio, in de organisatie, dagelijks- en algemeen bestuur, ieder in haar eigen rol.

Daarnaast gaan wij graag met u in gesprek over uw ambities ten aanzien van de interne beheersing en interne controle binnen uw organisatie. Met de rechtmatigheidsverantwoording door het dagelijks bestuur (zie 2.2) zien wij uitdagingen in onderstaande bevinding:

1. Het naleven van interne en Europese aanbestedingsregelgeving is het belangrijkste aandachtspunt. Gezien het karakter van onrechtmatigheden, ze zijn achteraf niet te herstellen, is het belangrijk voor de beheersing om preventieve maatregelen te treffen. Dit kan door voor het aangaan van verplichtingen beheersmaatregelen in te regelen, of door periodieke analyses op voortgang en verwachtingen ten aanzien van opdrachten en contracten in te richten. Bij dreigende, geprojecteerde overschrijdingen kan tijdig geanticipeerd worden.
2. De prestatielevering ten aanzien van de kosten is een belangrijk onderdeel van de rechtmatigheidsverantwoording. Binnen de huidige, weloverwogen, inrichting van het financiële systeem is op bepaalde lasten geen zichtbare controle op de prestatielevering. De organisatie zal daardoor achteraf op deze lasten voldoende zekerheid verkrijgen dat de prestatie geleverd is. Zoals gesteld in de notitie van het SDO (2.3) is beleid en zichtbare vastlegging een belangrijk te zetten stap. Onze bevinding ten aanzien van doorbreking van de ingerichte functiescheiding voor VeiligThuis vergroot de omvang en afhankelijkheid van de controle achteraf.

Ten aanzien van de aanbestedingen hebben wij in onze interim-controle geconstateerd dat het kennisniveau omtrent de aanbestedingswetgeving onvoldoende is gewaarborgd binnen het proces (met name inhuur derden en raming versus realisatie). Daarmee is er sprake van een verhoogd risico dat hier onrechtmatigheden uit naar voren komen. Beheersmaatregelen in systemen, bijvoorbeeld signalering in het contractenmodule dat bestedingen binnen een contract bijna uitgeput zijn, zijn niet ingericht. Ons advies is om de kennis bij de medewerkers te versterken en na te gaan hoe signalering ten aanzien van uitputting van contracten en benadering van de aanbestedingsdrempel binnen de processen geborgd kan worden. Wij zullen de aanbestedingen tijdens de balanscontrole, achteraf, gegevensgericht controleren. Om het inzicht van de organisatie te versterken, tijdiger te signaleren en om de controle soepeler te laten verlopen zijn met de financieel adviseurs en interim-controller afspraken gemaakt omtrent de controle door de organisatie. De vastlegging van de audittrail, structurele aanpak van de controle en specifiek de controle van de aandachtspunten inhuur en wezenlijke wijziging zijn afgestemd. Het afstemmen van tussentijdse vragen zou moeten voorkomen dat wij in de eindejaarscontrole meer aanvullende werkzaamheden moeten verrichten dan deze ondersteuning.

5.2 Verbijzonderde interne controle

VIC-functie wordt geheroriënteerd

Meerwaarde door tussentijdse metingen en versteking van de signalering aan de voorkant.

Versterking van de VIC positie ondersteund de verantwoording door het dagelijks bestuur

Ons beeld

Afgelopen jaren zien wij dat de personele bezetting op de verbijzonderde interne controle met het vertrek van de controller niet opnieuw is ingevuld. Daarnaast is het hoofd Financiën vertrokken en wordt dit momenteel waargenomen.

In oktober 2020 heeft de VRK een interim-controller ingehuurd met de opdracht de rechtmatigheid verder te borgen in de organisatie. Wij hebben begrepen dat het uitvoeren van de VIC taak geen onderdeel is van de opdracht aan de interim-controller. Wij achten het voor de toekomst wel van belang deze taak uit te voeren. De omvang en selectie van de te controleren items wordt bepaald in overleg met het BDO controleteam en met de tools van BDO.
In gesprekken heeft u aangegeven dat u zich op de VIC-functie heroriënteert. Wij benadrukken het belang van een onafhankelijke VIC-functie en treden hier dan ook graag met u over in gesprek.

Aanbevelingen

Wij constateren dat er momenteel geen VIC-functionaris is die proactief controles uitvoert en beleidsvoorstellen doet voor de toekomstige inrichting. Ons advies is om naar de toekomst een vaste VIC-functionaris aan te stellen die onafhankelijk van de Finance-afdeling opereert. Hierbij is het van belang dat de VIC deskundig genoeg is om controlewerkzaamheden uit te voeren, vooral op het vlak van (aanbestedings)rechtmatigheid. De controle op de rechtmatigheid, die de grondslag is voor de verantwoording door het dagelijks bestuur vanaf 2021, kan zo voldoende zekerheid bieden. Het dagelijks bestuur krijgt daarmee tevens mogelijkheden om tussentijds bij te sturen.

6. Bijlagen

Fiscale ontwikkelingen

Belangrijkste fiscale aandachtspunten 2020

Fiscale actualiteiten

De fiscale wijzigingen met impact op de financiële verantwoording van de Veiligheidsregio zijn in 2020 beperkt. Wij lichten ter voorbereiding op het jaarrekeningtraject 2020 hieronder enkele fiscale ontwikkelingen toe. Bij deze toelichting maken wij onderscheid tussen vennootschapsbelasting, loonbelasting en omzetbelasting.

Vennootschaps-belasting

Vennootschapsbelasting

Diverse overheidsbedrijven zijn per 1 januari 2016 belastingplichtig voor de vennootschapsbelasting. Voor veiligheidsregio's geldt dat zij belastingplichtig zijn indien en voor zover er sprake is van een onderneming in fiscale zin, hiervan is sprake indien aan de volgende eisen wordt voldaan:

- Duurzame organisatie van arbeid en kapitaal.
- Deelname aan het economisch verkeer.
- Winst wordt beoogd en is redelijkerwijs te verwachten ('winststreven').

Wij adviseren u jaarlijks een inventarisatie te doen van de overheidsactiviteiten welke onderhevig zijn aan vennootschapsbelasting en de impact op de belastingaangifte te bepalen. De voornaamste overheidsactiviteit welke onderhevig (kan) zijn aan vennootschapsbelasting is:

- Detachering: Met betrekking tot detachering kan sprake zijn van een onderneming voor de vennootschapsbelasting indien sprake is van positieve resultaten. In de meeste gevallen worden slechts de bruto loonkosten doorbelast (al dan niet inclusief werkgeverslasten). In dergelijk gevallen is geen sprake van een winststreven. Indien in de detacheringsovereenkomst echter vaste uurtarieven zijn overeengekomen dient te worden beoordeeld hoe deze zich verhouden tot de werkelijke loonkosten.

Loonbelasting

Loonbelasting

Voor de loonbelasting willen wij u attent maken op de registratie van de personeelsdossiers:

- In een personeelsdossier dienen de vereiste persoonsgegevens, geldig kopie legitimatiebewijs (op moment van indiensttreding) en opgaaf loonheffingen/loonbelastingverklaring te worden opgenomen. Het is van belang dat alle (dus ook de oudere) personeelsdossiers compleet zijn. In de praktijk zien we dit vaak fout gaan, met name in het geval van een fusie of splitsing in het verleden of bij digitalisering van de dossiers. Indien de personeelsdossiers niet op orde zijn kan dat leiden tot toepassing van het anoniementarief. Dit betekent dat loonheffing moet worden ingehouden en afgedragen tegen het hoogste tarief in de loonbelasting. Tijdens onze interim-controle hebben wij hier geen bevindingen geconstateerd.

Omzetbelasting

Omzetbelasting

De jurisprudentie en regelgeving omtrent de omzetbelasting is ook steeds in beweging. In 2020 heeft dit de nodige wijzigingen tot gevolg:

- In dezelfde uitspraak heeft de Hoge Raad geoordeeld dat het enkel uitvoeren van een wettelijke taak door een overheidslichaam onvoldoende is om tot overheidshandelen voor de btw te komen. Het overheidslichaam moet daarnaast bij de uitvoering van de activiteit ook gebruik maken van bijzondere overheidsbevoegdheden, waarover private partijen niet beschikken. Wanneer deze bevoegdheden ontbreken dan is geen sprake van overheidshandelen. Dit leidt ertoe dat Veiligheidsregio's hun activiteiten "labeling" op dit punt moeten beoordelen op mogelijk meer ondernemers- niet-economische activiteiten. Wij adviseren om deze beoordeling van overheidshandelen tijdig uit te voeren.

Ontwikkelingen en risico’s van cloudoplossingen (1/2)

“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.

Ontwikkelingen en risico’s van cloudoplossingen (2/2)

Zeven algemene aandachtsgebieden om grip te houden op uw cloud-oplossingen

De 7 aandachtsgebieden van cloud computing

Wij hebben zeven algemene 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.