12 februari 2020

MANAGEMENTLETTER

Veiligheidsregio Kennemerland

BDO

Aanbiedingsbrief

Veiligheidsregio Kennemerland
T.a.v. de heer A. van de Velden
Postbus 5514
2000 GM HAARLEM

Amstelveen, 12 februari 2020
Kenmerk: RB/NS/DR/AA20-0193

Geacht bestuur,

In het kader van de aan ons verstrekte opdracht tot controle van de jaarrekening 2019 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 zelfcontrolerend vermogen van uw organisatie. Naast de verbeterpunten in de bedrijfsvoering worden de algemene ontwikkelingen kort behandeld.

Wij vertrouwen erop u met deze managementletter naar aanleiding van onze interim-controle 2019 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,

H.C.J. Bot RA

Inhoudsopgave

1. Dashboard

1.1 Dashboard

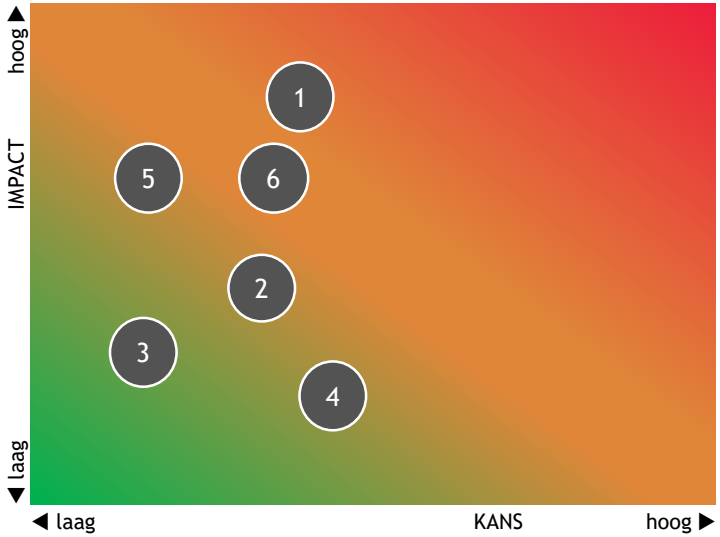
UW INTERNE BEHEERSING

- 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 de Veiligheidsregio Kennemerland zou de norm moeten zijn dat de processen in opzet, bestaan en werking (inclusief IT) geen belangrijke tekortkomingen kennen.
- Er is geconstateerd dat er een verbetering is omtrent het proces planning & control: er worden momenteel maandrapportages opgesteld. De belangrijkste verbeterpunten zien daarnaast toe op de aanbestedingen.
- Wij kunnen nog niet altijd steunen op de interne beheersing in de processen; onze controle is daarmee hoofdzakelijk gegevensgericht en achteraf.
- Voor de gedetailleerde procesbevindingen verwijzen wij naar Bijlage A van deze managementletter.

BEHEERSING IT: BEPERKT VERBETERD

- Tijdens onze interim-controle 2019 hebben wij verbeteringen in de inrichting en uitvoering van de IT General Controls geconstateerd ten opzichte van 2018.
- De belangrijkste bevindingen zijn:
  - Unit 4 Business World: opzet & bestaan van de IT General Controls over het algemeen voldoende met nog enkele verbeterpunten.
  - VP & InPlanning
    - Procedure autorisatiebeheer niet sluitend (B1).
    - Uitzonderingen op ingericht wachtwoordbeleid (B2).
    - Continuïteitsmaatregelen (B3).
    - Wijzigingenbeheer bij updates vereist aanvullende vastlegging (B4).
  - VP
    - Herleidbaarheid van gebruikers (identificatie) kan worden verbeterd en eindgebruikers met hoge rechten in de lijn (B5).

DETAILBEVINDINGEN



ONTWIKKELINGEN

Vanuit onze natuurlijke adviesfunctie onderkennen wij de volgende ontwikkelingen met betrekking tot de controle van de jaarrekening:

- Asset management: Een voorziening voor achterstallig onderhoud is vanaf dit lopende boekjaar 2019 verplicht.
- Wet Normering Topinkomens: Er is een verhoging van het bezoldigingsmaximum, uitbreiding van de term Topfunctionaris en aanscherping van de bezoldigingscomponenten.
- Aanscherping van de aanbestedingsrechtmatigheid.
- WNRA en beloning vrijwillige brandweer m.i.v. 2021.
- Ontwikkelingen ten aanzien van Meldkamer Noord-Holland.

VERBIJZONDERDE INTERNE CONTROLE

- Onze conclusies in relatie tot de vereisten vanuit de controle-standaard (COS) 610 zijn in 2019 ongewijzigd.
- Anders dan in voorgaande jaren is er momenteel geen sprake van een aparte VIC functie. Derhalve is het voor de jaarrekeningcontrole van belang nader af te stemmen hoe dit binnen de organisatie opgevangen gaat worden.

KORTE OMSCHRIJVING DETAILBEVINDINGEN

1	Contractenbeheer ondersteunt aanbestedingsproces niet voldoende
2	Controles en aansluitingen in de planning & control cyclus niet altijd zichtbaar
3	Niet alle processen en verantwoordelijkheden zijn in procesbeschrijvingen vastgelegd
4	Volledigheid verbonden partijen
5	Contracten debiteuren worden niet centraal geregistreerd
6	De inkomstenstromen worden niet volledig gemonitord

2. Bevindingen significante processen

2.1 Onze controle nog transparanter (1/3)

Eisen aan accountantscontrole en onze rapportages

Interne beheersing niet altijd voldoende / zichtbaar / aantoonbaar. Welke ambities heeft uw gemeenschappelijke regeling?

Wij gaan graag het gesprek aan over uw ambities en de normen die gesteld kunnen worden aan uw interne beheersing

Onze aanpak afhankelijk van uw ambitie en interne beheersing

De afgelopen jaren is 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. Om inzicht te geven in de eisen die gesteld kunnen worden aan de interne beheersing (en externe controle) hebben wij in onze managementletters van de afgelopen jaren hierover uitgebreid gerapporteerd. 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. Wij hebben vanuit onze natuurlijke adviesfunctie hiermee willen bijdragen aan de verbetering van uw bedrijfsvoering, onder andere door middel van procesanalyses, detailbevindingen/-aanbevelingen (voorzien van risico en impact), schema's over de kwaliteit van de IT-beheersmaatregelen, ons beeld van de VIC, etc.

Wij constateren echter dat uw gemeenschappelijke regeling, net als veel andere gemeenschappelijke regelingen, op korte termijn (nog) niet in staat is gebleken de interne beheersing op het gewenste niveau te krijgen. Dit betekent niet dat uw gemeenschappelijke regeling niet in control is, maar wel dat deze niet zichtbaar / aantoonbaar in de processen en systemen zit en dus de interne / externe controle hier niet op kan steunen. In onze visie zou de norm moeten zijn dat alle (significante) processen in opzet, bestaan en werking (inclusief IT) gedurende het gehele jaar goed werken en intern getoetst worden door uw VIC. Die norm kan er toe leiden dat gemeenschappelijke regelingen beter in control zijn en eventuele risico's eerder signaleren. Deze norm en dit niveau van interne beheersing vraagt echter wel de nodige inspanning en ambitie en de vraag is of en op welke termijn u deze wil/kan realiseren.

Wij gaan daarom graag met u in gesprek over deze ambities, zodat wij onze controleaanpak daarop aan kunnen passen. 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. Als bij voorbaat al duidelijk is dat uw organisatie (op korte termijn) niet kan of wil voldoen aan deze normen, kunnen wij ook onze controle achteraf en meer gegevensgericht aanpakken en daarmee efficiënter uitvoeren. Deze afweging ten aanzien van uw ambitie ligt echter primair bij de gemeenschappelijke regeling, zowel in de organisatie als het bestuur, ieder in haar eigen rol.

Belangrijke vragen bij uw ambities ten aanzien van de bedrijfsvoering zijn:

- Heeft u de ambitie om de interne beheersing (inclusief IT-maatregelen) naar bovengenoemd niveau te ontwikkelen (willen)?
- Bent u als organisatie / gemeenschappelijk regeling in staat dit gewenste niveau te bereiken, rekening houdend met uw omvang en specifieke situatie (kunnen)?
- Vindt u het risico acceptabel dat de interne en externe controle vooral gericht is op controles achteraf (risico's)?
- Bent u bereid te investeren in uw bedrijfsvoering (risico versus doelmatigheid)?
- Wat is uw visie op deze aspecten in relatie tot de wijziging van de verantwoordelijkheid voor de rechtmatigheidsverklaring?
- Wat verwacht u van onze dienstverlening en rapportages in relatie tot bovenstaande keuzes?

Wij stellen voor dat u uw afwegingen en ambities zo SMART mogelijk vastlegt in bijvoorbeeld uw interne controleplan. Wij zullen vervolgens onze aanpak hierop afstemmen. Wij maken daarbij onderscheid tussen een proces- of systeemgerichte aanpak versus een gegevensgerichte aanpak. In het vervolg gaan wij daar kort op in.

2.1 Onze controle nog transparanter (2/3)

Onderkende risico's:
- Management override
- EU-aanbestedingen
- ICT
- Opbrengst-verantwoording

Onze inschatting van de risico's

In het kader van de controle van de jaarrekening 2019 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 Veiligheidsregio Kennemerland:

- 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 gemeenschappelijke regeling 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 de IT-systemen.
- Onvolledige verantwoording van de overige baten.

Wij beoordelen de volgende processen

Onze inschatting van de belangrijkste processen

In onze aanpak is de insteek nog steeds, daar waar mogelijk te steunen op de interne beheersing in de significante processen van de gemeenschappelijke regeling. 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 proces omtrent rijks- en gemeentebijdrage
- Overige baten
- Het inkoopproces
- Aanbestedingen
- Het personeelsproces
- De beheersing van verbonden partijen
- Het proces omtrent IT/automatisering

Natuurlijk zijn er meerdere processen te onderkennen, ook met financiële gevolgen. Voorbeelden zijn het proces ten aanzien van geneeskundige hulpverlening en diverse kleinere (schattings-)processen. Wij hanteren hierbij een deels systeemgerichte controle op het personeels- en inkoopproces. Op de overige processen toetsen wij niet procesmatig / systeemgericht, maar zullen wij (achteraf) gegevensgerichte werkzaamheden uitvoeren in de vorm van steekproeven / deelwaarnemingen, cijferanalyses, verbandscontroles, etc. Bij de voorbereiding van de jaarrekeningcontrole maken wij, evenals voorgaande jaren, afspraken over de resterende werkzaamheden, aanpak en de hiervoor benodigde informatie.

In het kader van onze controle hebben wij aandacht besteed aan de Planning & Control cyclus ofwel de interne beheersing op organisatieniveau. Indien deze interne beheersing in opzet, bestaan en werking toereikend en aantoonbaar is, kunnen wij hier als accountant gebruik van maken in onze controle.

2.1 Onze controle nog transparanter (3/3)

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

De beheersorganisatie is in opzet voldoende tot goed.

Voor wat betreft onze aanpak kunnen wij 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 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 de overzichten op de volgende pagina's geven wij weer in hoeverre de processen voldoen aan de genoemde normen (zie ook hoofdstuk 3 ten aanzien van IT-omgeving) en welke 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 Kennemerland (voor zover relevant voor de controle van de jaarrekening) in opzet voldoende tot goed scoort. Omdat de AO/IB en IT General Controls niet altijd goed zijn opgezet of goed werken, kunnen wij voor wat betreft de insteek van onze controle nog niet altijd op de processen steunen.

Er zijn in onze aanpak daarom aanvullende gegevensgerichte werkzaamheden noodzakelijk, zie voor de details van onze bevindingen en aanbevelingen Bijlage A.

Hierin zijn onder meer bevindingen en aanbevelingen opgenomen ten aanzien van de maandrapportages als onderdeel van de Planning & Control cyclus en het opstellen van procesbeschrijvingen.

Het proces van de maandrapportages kent nog onvoldoende zichtbare waarborgen. Hierdoor kunnen wij geen zekerheid halen uit het proces. Er is wel sprake van potentie om het proces dusdanig te verbeteren, dat wij hier in de toekomst wel zekerheid aan kunnen ontlenen.

Wij adviseren tevens om per significant proces een procesbeschrijving op te stellen. Voor de bestaande procesbeschrijvingen adviseren wij u de aanwezige procesbeschrijvingen uit te breiden door expliciet aandacht te besteden aan de '6 w-vragen'. Het resultaat van deze verbetering is dat ook mogelijke leemtes in de processen worden onderkend en kunnen worden gerepareerd.

Door het ontbreken van procesbeschrijvingen is onze interim-controle minder efficiënt en blijven wij jaarlijks (reeds bestaande) leemtes in processen identificeren. Deze leemtes kunnen vaak niet meer hersteld worden in het boekjaar, waardoor onze gegevensgerichte werkzaamheden omvangrijk blijven.

2.2 Effectiviteit processen (2/2)

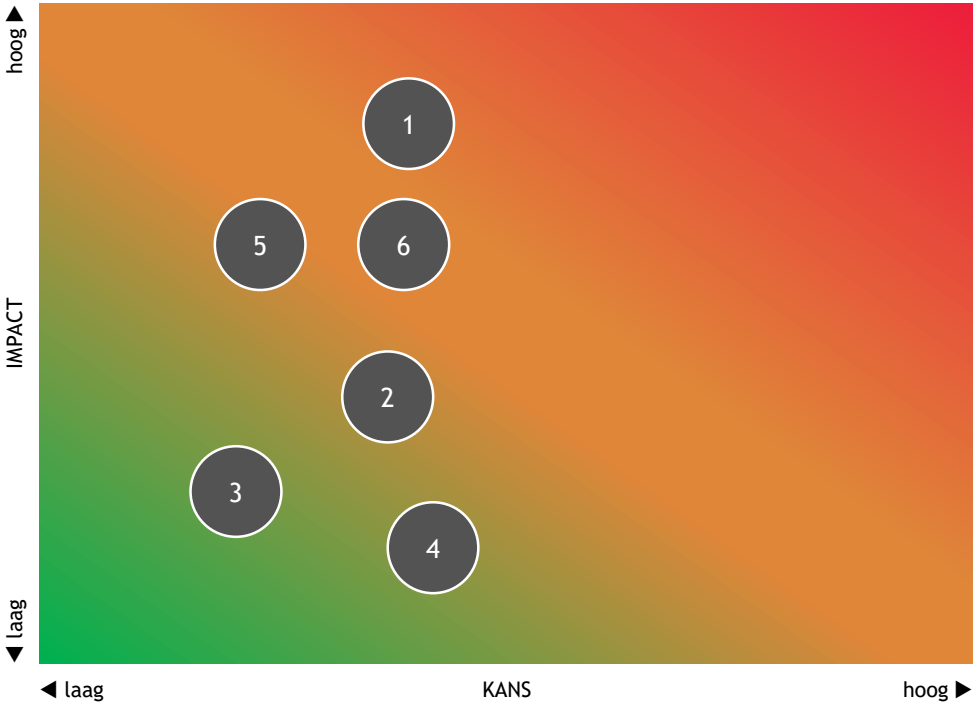
PROCES	OPZET AO/IB	WERKING AO/IB	ITGC'S	VIC	CONCLUSIE T.A.V. DE CONTROLEAANPAK
Planning & Control			N.v.t.	N.v.t.	De opzet van maandrapportages die in 2019 heeft plaatsgevonden, is een belangrijk verbeterpunt in de Planning & Control cyclus. De maandrapportages worden nog niet altijd zichtbaar afgetekend, daarnaast is de opvolging niet altijd zichtbaar.
Ontvangen bijdragen		N.v.t.	N.v.t.	N.v.t.	Geen bevindingen geconstateerd in ontvangen bijdragen van zowel Rijk als gemeenten.
Overige baten			N.v.t.	N.v.t.	De contracten met betrekking tot debiteuren worden niet geregistreerd. Daarnaast is er geen duidelijke monitoring omtrent de volledigheid van de overige opbrengsten.
Inkopen				N.v.t.	Leveringen en facturen worden geautoriseerd in het systeem.
Aanbestedingen			N.v.t.	N.v.t.	De melding vanuit Unit4 wordt niet altijd tijdig opgevolgd, daarnaast is er een gedateerd inkoopbeleid.
Personeel				N.v.t.	De personeelsmutaties > €1.000 worden gecontroleerd en akkoord bevonden door hoofd FA.
Verbonden partijen		N.v.t.	N.v.t.	N.v.t.	Vastgesteld dat niet voor alle verbonden partijen een gedegen analyse en conclusie is vastgelegd en getoetst.
ICT/automatisering			N.v.t.	N.v.t.	Ten aanzien van ICT zijn door ons net zoals voorgaande boekjaren belangrijke aandachtspunten gesignaleerd (zie hoofdstuk 3).

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.

2.3 Detailbevindingen



KORTE OMSCHRIJVING DETAILBEVINDINGEN	
1	Contractenbeheer ondersteunt aanbestedingsproces niet voldoende
2	Controles en aansluitingen in de planning & control cyclus niet altijd zichtbaar
3	Niet alle processen en verantwoordelijkheden zijn in procesbeschrijvingen vastgelegd
4	Volledigheid verbonden partijen
5	Contracten debiteuren worden niet centraal geregistreerd
6	De inkomstenstromen worden niet volledig gemonitord

3. IT-beheersing

3.1 IT-beheersing

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

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

Detailbevindingen IT weergegeven in Bijlage B

IT-werkzaamheden en onze controlerende rol

Ingevolge artikel 2:393, lid 4 BW, dient de accountant in zijn verslag aandacht te besteden aan de bevindingen die naar voren zijn gekomen uit de beoordeling van de automatiseringsomgeving wat betreft de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Wij benadrukken dat onze jaarrekeningcontrole gericht is op het geven van een oordeel omtrent de jaarrekening zelf en zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan. De IT-auditwerkzaamheden zijn geïntegreerd in de controleaanpak van de jaarrekening.

Het inzicht in de betrouwbare werking van ICT-systemen en -applicaties en het gebruik daarvan door de organisatie, vormen een onderdeel van de kwaliteit van de interne beheersing en de administratieve organisatie. Algemene IT-beheersmaatregelen rond uw kritieke systemen leveren daarnaast een belangrijke bijdrage aan het mitigeren van de risico's op onbeheerste wijzigingen, ongeautoriseerde handelingen en het optreden van verstoringen met impact op de gegevensverwerking.

De bevindingen zoals gerapporteerd in deze 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 en InPlanning. 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 2).

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

Daarna gaan wij, vanuit onze natuurlijke adviesfunctie, in op een aantal actuele ontwikkelingen ten aanzien van de Baseline Informatiebeveiliging Overheden (BIO), het project GGI- veilig en data-analyse.

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 Bijlage B

PROCES	2019	2018
1. Procedure autorisatiebeheer	verbeterpunten	verbeterpunten
2. Periodieke controle op juistheid ingerichte autorisaties	verbeterpunten	verbeterpunten
3. Identificatie van gebruikers voor toegang tot systemen en data	voldoende	voldoende
4. Wachtwoordbeleid (authenticatie)	voldoende	voldoende
5. Administrators en superusers	verbeterpunten	verbeterpunten
6. Wijzigingenbeheer updates	voldoende	voldoende
7. Gescheiden omgevingen (ontwikkel-test-productie)	voldoende	voldoende

KORTE OMSCHRIJVING RESULTATEN	
1	Ten tijde van onze audit (zomer 2019): Een normpositie van de rechten per rol is aanwezig. Verbetering nog mogelijk t.a.v. het maken van een normpositie van benodigde rollen per organisatorische functie. Na de audit is hier opvolging aan gegeven door de VRK.
2	Periodieke review autorisaties op Unit 4 BW uitgevoerd op de toegekende rollen per gebruiker, echter nog niet op de detailrechten per rol en nog niet formeel ten opzichte van de normpositie.
3	Geen opmerkingen
4	Geen opmerkingen
5	Superusers zijn beperkt, maar bevat nog wel een gebruiker uit de operationele organisatie wat wij in de basis onwenselijk achten. Na de audit is hier opvolging aan gegeven door de VRK.
6	Akkoord op hoofdlijnen, verbeteringen nog mogelijk ten aanzien van een zichtbare vastlegging van de impactanalyse vooraf en gemaakte afwegingen bij kleine changes / hotfixes. In 2019 zijn geen nieuwe Milestone updates doorgevoerd, derhalve hebben wij het bestaan van de procedure wijzigingenbeheer aan de kant van VRK niet kunnen toetsen.
7	Geen opmerkingen

onvoldoende verbeterpunten voldoende

3.3 Bevindingen IT-beheersing | VeiligheidsPaspoort

Logische toegangs-beveiliging VP (criteria 1-5) nog ontoereikend

Change management (criteria 6-7) nog ontoereikend.

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar Bijlage B

PROCES	2019	2018		KORTE OMSCHRIJVING RESULTATEN
1. Procedure autorisatiebeheer			1	Gebruikers en rechten mutaties worden nog niet structureel vastgelegd en bijgehouden. Een normpositie van de benodigde rechten per organisatorische functie is nog niet aanwezig.
2. Periodieke controle op juistheid ingerichte autorisaties			2	Een periodieke review van autorisaties binnen VP is in 2019 niet uitgevoerd. Wel heeft een opschoning van gebruikers in overleg met de leverancier plaatsgevonden (niet zichtbaar).
3. Identificatie van gebruikers voor toegang tot systemen en data			3	Er zijn een relatief groot aantal generieke accounts gevonden in VP en het bestaan van al deze generieke accounts is niet altijd verklaarbaar vanuit gebruiks- of beheerdoeleinden.
4. Wachtwoordbeleid (authenticatie)			4	Aanscherpingen in wachtwoordbeleid mogelijk. Eisen ten aanzien van periodiek wijzigen, wachtwoordhistorie en een lock-out policy zijn niet aanwezig.
5. Administrators en superusers			5	De superuser rechten zijn niet beperkt tot een strikt noodzakelijk minimum.
6. Wijzigingenbeheer updates			6	Key-users voeren testwerkzaamheden uit bij software updates. Vastleggingen hiervan zijn echter niet aanwezig en kunnen wij daardoor niet controleren. Vanuit de leverancier is er geen zekerheid over het beheerst doorvoeren van wijzigingen aangezien zij niet over een geschikte assurance verklaring beschikken.
7. Gescheiden omgevingen (ontwikkel-test-productie)			7	Geen opmerkingen

onvoldoende verbeterpunten voldoende

3.4 Bevindingen IT-beheersing | InPlanning

Logische toegangs-beveiliging InPlanning (criteria 1-5) nog deels ontoereikend;

Change management (criteria 6-7) ontoereikend;

Voor een nadere onderbouwing van de norm, bevindingen en aanbevelingen verwijzen wij naar Bijlage B

PROCES	2019	2018		KORTE OMSCHRIJVING RESULTATEN
1. Procedure autorisatiebeheer			1	Gebruikers en rechten mutaties worden nog niet structureel vastgelegd en bijgehouden. Een normpositie van de benodigde rechten per organisatorische functie is nog niet aanwezig.
2. Periodieke controle op juistheid ingerichte autorisaties			2	Een periodieke review autorisaties binnen InPlanning is in 2019 wel uitgevoerd, maar niet vastgelegd en kunnen wij derhalve niet vaststellen.
3. Identificatie van gebruikers voor toegang tot systemen en data			3	Geen opmerkingen
4. Wachtwoordbeleid (authenticatie)			4	Aanscherpingen in wachtwoordbeleid mogelijk. Eisen ten aanzien van periodiek wijzigen, wachtwoordhistorie en een lock-out policy zijn niet aanwezig.
5. Administrators en superusers			5	Geen opmerkingen
6. Wijzigingenbeheer updates			6	Key-users voeren testwerkzaamheden uit bij software updates. Vastleggingen hiervan zijn echter niet aanwezig en kunnen wij daardoor niet controleren. Vanuit de leverancier is er geen zekerheid over het beheerst doorvoeren van wijzigingen aangezien zij niet over een geschikte assurance verklaring beschikken.
7. Gescheiden omgevingen (ontwikkel-test-productie)			7	Geen opmerkingen

onvoldoende verbeterpunten voldoende

3.5 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol (1/3)

IT-werkzaamheden en onze natuurlijke adviesrol

Vanuit onze natuurlijke adviesrol willen wij u attenderen op een aantal ontwikkelingen op het gebied van IT. Deze ontwikkelingen zijn niet altijd direct gerelateerd aan onze controle van de jaarrekening, maar wel van belang voor uw bedrijfsvoering. Wij schetsen in deze managementletter de ontwikkelingen op hoofdlijnen met als doel u te attenderen op deze ontwikkelingen. Dat betekent ook dat wij geen uitgebreid onderzoek hebben uitgevoerd naar deze onderwerpen of ze specifiek hebben gemaakt voor uw organisatie.

Baseline Informatiebeveiliging Overheid

In het afgelopen jaar hebben diverse ontwikkelingen plaatsgevonden waaronder de aangescherpte privacywetgeving, de toenemende behoefte om informatie via internet uit te wisselen alsook de ontwikkelingen op het gebied van Internet of Things, Cloud, Smart Cities en een verhoogde (digitale) interactie met burgers. Deze ontwikkelingen hebben ertoe geleid dat overheidsinstanties strengere eisen moeten stellen aan informatiebeveiliging. Het hebben van een adequate informatiebeveiliging is geen vrijblijvendheid meer, maar een harde noodzaak.

Daarom dienen vanaf 1 januari 2020 alle overheidsinstanties de benodigde voorzieningen te hebben getroffen om te voldoen aan de nieuwe vereisten van Baseline Informatiebeveiliging Overheid (BIO). Met de komst van de BIO zullen de bestaande baselines voor gemeenten, provincies, waterschappen en het rijk worden vervangen en zal een actueel en uniform normenkader geïntegreerd worden binnen de gehele overheid. De baseline zorgt voor één gezamenlijk en eenduidig normenkader binnen de gehele overheid gebaseerd op de internationaal erkende en actuele ISO-normatiek (ISO 27001:2017).

In het BIO-normenkader zullen risicoafwegingen en risicomanagement de basis vormen voor de manier en diepgang van de invulling van informatiebeveiliging voor overheidsorganisaties en hun onderlinge ketensamenwerking. Daarnaast vereist de BIO een expliciete betrokkenheid en verantwoordelijkheid van het lijnmanagement voor het implementeren en monitoren van informatiebeveiliging.

Een aantal belangrijke stappen om de BIO te implementeren zijn:

- Het uitvoeren van een nulmeting (gap-analyse) waarin zowel de implementatie van de huidige baseline als de te ondernemen stappen voor de BIO in kaart worden gebracht.
- Het trainen van het lijnmanagement door middel van bijvoorbeeld workshops, om een risico gestuurde aanpak (omtrent informatie-beveiliging) te integreren in de bedrijfsvoering en bewustwording omtrent verantwoordelijkheden van informatiebeveiliging te creëren.
- Het uitvoeren van een security scan voor het bepalen van de vereiste maatregelen per proces.
- Het implementeren van de beheersingsmaatregelen die op basis van deze security scan zijn bepaald.
- Het uitvoeren van een BIO-audit om te bepalen in hoeverre uw organisatie voldoet aan de BIO vereisten.

Wij hebben van de VRK begrepen dat de organisatie bekend is met dat de BIO de BIG zal gaan vervangen. Dit is daarmee ook benoemd in het informatiebeveiligingsbeleid en Informatiebeveiligingsuitvoeringsplan (IBUP). De door ons geziene documenten komen uit het voorjaar 2019. Inmiddels is er meer bekend over het definitieve normenkader BIO en adviseren wij de VRK een gap-analyse uit te voeren naar de huidige ingerichte informatiebeveiligingsmaatregelen en de maatregelen die nodig zouden zijn vanuit de BIO. Daarnaast is de uitvoering van de BIO anders dan de BIG en vereist dit meer risicoafwegingen en risicomanagement en daarmee ook actievere betrokkenheid van proceseigenaren. Graag denken wij daarom tijdig met u mee over de juiste aanpak van de implementatie van de BIO, alsook de gevolgen van de BIO voor de interne beheersing van de processen.

3.5 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol (2/3)

Veiliger samenwerken door GGI

Landelijk project VNG op het vlak van informatiebeveiliging

Mogelijke onderzoeken en testen ten aanzien van informatiebeveiliging

GGI-Veilig

De toenemende noodzaak om informatiebeveiliging op orde te hebben, tezamen met de wens om slimmer en meer samen te werken, heeft ertoe geleid dat vanuit de Vereniging Nederlandse Gemeenten (VNG) een initiatief is gestart om een Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) op te zetten. Deze GGI creëert een veilige, samenhangende digitale infrastructuur waardoor samenwerken tussen lokale overheden en andere overheden beter, veiliger en gemakkelijker wordt.

Om ervoor te zorgen dat GGI voldoet aan de veiligheidsnormen, is landelijk het project GGI-Veilig in het leven geroepen. GGI-Veilig heeft als doel de digitale weerbaarheid van gemeenten te verhogen door op een ontzorgende manier te ondersteunen bij de invulling van informatiebeveiliging. Dit wordt gerealiseerd door onder meer de verwerving van een collectieve SIEM/SOC-voorziening (Security Information Event Management / Security Operation Center).

Om de informatiebeveiliging optimaal in te richten en te beheersen zijn daarnaast een groot aantal maatregelen en testen mogelijk zoals compliance scans, pentesten (ethical hacking) en kwetsbaarheid scans.

Compliancy
Uitvoeren van compliancy scans/ assessments/audits op aandachtsgebieden BIO, BIG, AVG, ENSIA, ISO-900x en -270x

Pentesten
Uitvoeren van Ethical Hacking tests om mogelijke kwetsbaarheden in informatie systemen inzichtelijk te maken

Netwerk hardening
Onderzoeken van en adviseren over robuustheid van ICT-infrastructuren in gebruik bij lokale overheden

Vulnerability
Uitvoeren van vulnerability scans/ assessments op (het beheer van) de ICT-infrastructuur van lokale overheid

Forensics
Levering van ondersteuning bij forensisch onderzoek n.a.v. security incidenten

SIEM
Bieden van ondersteuning bij inrichting en uitvoering van SIEM-proces binnen lokale overheden

3.5 Actuele IT-ontwikkelingen en onze natuurlijke adviesrol (3/3)

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.

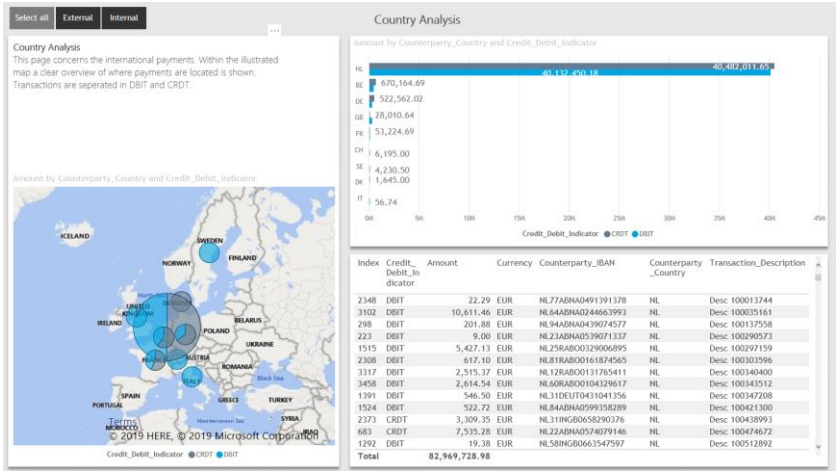
Het grote voordeel van data-analyse is dat de interne / externe controle niet plaatsvindt door middel van statistische steekproeven / deelwaarnemingen, maar dat alle data integraal kan worden geanalyseerd en gecontroleerd.

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 en veiligheidsregio's, zoals Key2Financien, Proactive, BNG en 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.



Wij gaan graag met u in gesprek over de toepasbaarheid van data-analyse, process mining, etc. in uw organisatie en uw ambities hierin.

4. Ontwikkelingen & Aandachtspunten

4.1 Actualiteiten BBV

Nog slechts 2 keer per jaar V&A van de commissie BBV

Voorziening voor achterstallig onderhoud verplicht

Meer aandacht voor registratie activa en asset management

BBV Actualiteiten

De wijzigingen in het Besluit Begroting en Verantwoording van gemeenten en provincies (BBV) lijken dit jaar beperkt. Wel gebruikt de commissie BBV vanaf 2019 een nieuwe website, wat ook gevolgen heeft voor het stellen van vragen en de beantwoording. De commissie heeft in 2018 besloten antwoorden op vragen per half jaar te publiceren. Elk halfjaar worden dan die vragen en antwoorden gepubliceerd waarvan de commissie van mening is dat deze meerwaarde bieden voor iedereen ten opzichte van de notities. Wij lichten ter voorbereiding op het jaarrekeningtraject 2019 hieronder enkele BBV ontwikkelingen kort toe.

Achterstallig onderhoud

In geval van achterstallig onderhoud waarbij sprake is van kapitaalvernietiging en/of onveilige situaties moet op basis van artikel 44 lid 1a BBV een voorziening worden gevormd. Deze richtlijn is een aanscherping ten opzichte van eerder gepubliceerde notities. Deze bepaling treedt in werking met ingang van het begrotingsjaar 2019. Derhalve ligt meer nadruk op achterstallig onderhoud en de beheerplannen met betrekking tot de gemeentelijke activa (ofwel assets). In dit kader wordt de noodzaak van een adequaat asset management (nog) zichtbaarder. Onder asset management wordt verstaan “de systematische en gecoördineerde activiteiten waarmee een organisatie haar bedrijfsmiddelen optimaal beheert (vanaf de investering) en prestaties, risico’s en kosten over de levensduur volgt met als doel een optimale bijdrage te leveren aan de strategie van de organisatie”.

Belangrijke vragen voor gemeenten (en dus ook gemeenschappelijk regelingen) vanuit het perspectief van assetmanagement en de notitie MVA betreffen:

- Zijn alle wezenlijke activa / assets geregistreerd in een activaregister, ook die eventueel off balance staan, geen boekwaarde meer hebben, in het verleden niet geactiveerd zijn en/of weinig tot geen boekwaarde meer hebben? In hoeverre zijn inventarisaties hiervan actueel?
- Bestaan er ten aanzien van deze assets actuele beheersplannen? Zo ja, van welk jaar dateren die, hoe worden die geactualiseerd en met welke frequentie?
- Leiden de beheersplannen tot een (materieel) goede inschatting van de lasten in de jaarrekening en/of begroting en wordt dit intern gemonitord?
- Zijn er adequate voorzieningen getroffen voor achterstallig onderhoud dan wel zijn de onderhoudskosten adequaat afgedekt in meerjarenperspectief?
- Zitten hier mogelijk nog (significant) risico’s en mogelijke tekorten in?

Bij de interim-controle hebben we aandacht besteed aan assetmanagement en ons is medegedeeld dat voor de jaarrekeningcontrole wordt nagegaan in hoeverre de beschikbare beheersplannen nog aansluiten op de voorzieningen. De VRK is momenteel bezig met het updaten van het onderhoudsplan MICK. Er wordt ook gewerkt aan een notitie over activa beleid zodat de VRK weer aansluit op de nieuwe BBV.
Wij verzoeken u een goede analyse (position paper) te maken ter onderbouwing van de jaarrekening, zowel ten aanzien van de voorziening achterstallig onderhoud (juistheid én volledigheid) als ten behoeve van de paragraaf onderhoud kapitaalgoederen.

4.2 Wet normering topinkomens

Belangrijkste wijzigingen 2019 WNT en algemene bevindingen vanuit controle boekjaar 2018

Wet normering topinkomens

De regelgeving omtrent de WNT wordt ieder jaar aangepast en inmiddels is de regelgeving voor 2019 gepubliceerd. Hieronder hebben wij de belangrijkste wijzigingen en onze algemene aandachtspunten vanuit de WNT-controle boekjaar 2018 op een rij gezet:

- Het bezoldigingsmaximum van een topfunctionaris in fulltime dienstverband bedraagt per 1 januari 2019 € 194.000 (was € 189.000 in boekjaar 2018).
- Sinds 1 januari 2018 is bepaald dat een functionaris ondanks het neerleggen van zijn/haar functie als topfunctionaris voor een periode van vier jaar vanaf het tijdstip dat de functie niet langer wordt vervuld toch topfunctionaris blijft, indien aan specifieke voorwaarden wordt voldaan.
- De bezoldigingscomponenten zijn aangescherpt/verduidelijkt wat onder andere betekent dat het werkgeversdeel van pensioenregelingen en het werkgeversdeel voor vervroegde uittredingen meetelt als WNT-bezoldiging en dat werkgeversbijdragen aan opleidingsfondsen en dergelijke niet meetellen als WNT-bezoldiging.
- Onderdeel van de WNT-bezoldiging zijn tevens alle belastbare onkostenvergoedingen. Uit de WNT-controle 2018 is gebleken dat niet voor alle Instellingen te allen tijde helder is wat belastbare en niet belastbare onkostenvergoedingen zijn. Belangrijk is dat de kostenvergoedingen fiscaal juist worden verwerkt. Enkel indien onkostenvergoedingen zijn aangewezen als eindheffingsloon (“onder de WKR zijn gebracht”) tellen deze niet mee als WNT-bezoldiging. Tijdige en juiste fiscale behandeling is dus essentieel.

Meer dan de helft van de WNT-verantwoordingen onjuist/ onvolledig

Uit de controles over 2018 van de aan ons aangeboden WNT-verantwoordingen van alle gemeenten en gemeenschappelijke regelingen is gebleken dat meer dan de helft onjuist of onvolledig waren. Dit betrof een mix van tekstuele, formele, maar soms ook materiële financiële fouten.

Tijdens de controle van de WNT-verantwoording 2018 van uw gemeenschappelijke regeling, hebben wij echter geen bevindingen geconstateerd.

4.3 Aanbestedingsrechtmatigheid

Landelijk blijkt dat circa 15% van de controleverklaringen 2018 ten aanzien van rechtmatigheid niet goedkeurend is als gevolg van onrechtmatige aanbestedingen.

Risicogerichte inkoopanalyse in lijn met de SDO-Notitie.

Toenemende aandacht voor aanbestedingsrechtmatigheid

In het kader van de rechtmatigheidscontrole blijft de juiste toepassing van de Europese aanbestedingsrichtlijnen een belangrijk aandachtspunt. Landelijk blijkt dat circa 15% van de controleverklaringen 2018 (2017: 13%) ten aanzien van rechtmatigheid niet goedkeurend is als gevolg van onrechtmatige aanbestedingen. Er is dan ook in toenemende mate aandacht voor de borging van aanbestedingsrechtmatigheid bij gemeenschappelijke regelingen. Ook bij Veiligheidsregio Kennemerland hebben wij bij de jaarrekeningcontrole van 2018 onrechtmatige aanbestedingen geconstateerd en meegewogen in ons oordeel. Wij vragen dan ook extra aandacht voor aanbestedingsrechtmatigheid en onderstaande aandachtsgebieden en risico's in het bijzonder.

Risicogerichte inkoopanalyse t.b.v. de rechtmatigheidscontrole

Veelal blijkt dat het door de complexiteit van de aanbestedingswetgeving en de continue stroom aan jurisprudentie niet mogelijk is om de aanbestedingsrechtmatigheid te borgen in de reguliere administratieve organisatie en interne beheersing. In het kader van de jaarrekeningcontrole betekent dit dat er via controle achteraf vastgesteld dient te worden dat er geen onrechtmatige aanbestedingen hebben plaatsgevonden. Om gemeenschappelijke regeling en accountants in de sector praktische handvatten te geven op het gebied van aanbestedingsrechtmatigheid heeft de NBA-Sectorcommissie Decentrale Overheden (SDO) de SDO-Notitie Uitvoering van de controle op aanbestedingsrechtmatigheid bij de jaarrekeningcontrole van decentrale overheden (Good practice, 17 januari 2019) uitgebracht. Naast een beschrijving van de uit te voeren werkzaamheden bij een risicogerichte inkoopanalyse zijn in de notitie eveneens de volgende aandachtsgebieden benoemd:

- Subsidies versus overheidsopdrachten
- Publiek publieke samenwerking
- Raamovereenkomsten
- ICT-contracten
- Inhuur personeel
- Onderhandelingspositie zonder aankondiging
- Dynamisch aankoopsysteem
- Openhouse / bestuurlijke aanbestedingen

Wat kan er zoal mis gaan?

Uit onze rechtmatigheidscontroles blijken de volgende punten regelmatig mis te gaan waardoor er onterecht niet Europees is aanbesteed:

- Het onterecht opknippen van opdrachten (verdelen over meerdere leveranciers / langere periode).
- Het ontbreken van een realistische raming (bijv. looptijd langer dan 4 jaar waarbij in de raming geen rekening is gehouden).
- Het onjuist aanbesteden van samengestelde / gemengde opdrachten (bv. een combinatie van investering en onderhoudscontracten).
- Een opdracht ten onrechte aanmerken als een quasi inbesteding.
- Een opdracht ten onrechte aanmerken als een sociale / specifieke dienst (Bijlage 14 bij richtlijn 2014/24).
- Een contract met een jaarlijks stilzwijgende verlengingsoptie niet aanmerken als een contract voor onbepaalde tijd.
- Het verlengen van een contract zonder verlengingsoptie.
- Het onjuist omgaan met significante wijzigingen van een contract gedurende de looptijd.

Wij adviseren u, in aanvulling op onze eerdere bevindingen en aanbevelingen, kennis te nemen van deze notitie.

4.3 Beloning vrijwillige brandweer

Vrijwillige brandweerlieden hebben in beginsel recht op dezelfde beloning als beroepsbrandweer-lieden

Advies om tot duidelijk onderscheidend takenpakket te komen

Inleiding

Het brandweerkorps bestaat in Nederland momenteel voor ongeveer 80% uit vrijwilligers. Wanneer zij worden opgeroepen voeren zij – kort gezegd - dezelfde werkzaamheden uit als de beroepsbrandweer. Hiernaast gelden voor de vrijwillige brandweer dezelfde eisen van opleiding, oefening en gezag. Desondanks ontvangen vrijwillige brandweerlieden slechts een (onkosten)vergoeding van ongeveer € 150 tot € 250 per maand. Dit is veel lager dan het minimumloon of het voor de beroepsbrandweer geldende loon. De vraag deed zich voor of dit onderscheid wel gerechtvaardigd is.

Deeltijdrichtlijn

Op grond van de Europese Deeltijdrichtlijn en de implementatie daarvan in Nederlandse regelgeving is het (overheids-)werkgevers verboden om deeltijdwerkers ongunstiger te behandelen dan voltijdwerkers op de enkele grond van een verschil in arbeidsduur. Uit onderzoek in opdracht van de Nederlandse overheid blijkt dat vrijwillige brandweerlieden hoogstwaarschijnlijk als deeltijdwerkers in de zin van de Deeltijdrichtlijn kunnen worden aangemerkt, nu er sprake is van een arbeidsverhouding en een sterke gelijkenis ten aanzien van de werkzaamheden en de opleidingseisen. Dit heeft tot gevolg dat vrijwillige brandweerlieden in beginsel recht hebben op dezelfde beloning als beroepsbrandweerlieden.

Vervolgens doet zich de vraag voor of een afwijkende beloning van de vrijwillige brandweer objectief gerechtvaardigd is. Dit lijkt niet het geval te zijn. Zoals eerder beschreven is er een sterke gelijkenis tussen de vrijwillige brandweer en de beroepsbrandweer. Bovendien is de vrijwillige brandweer in veel gevallen verplicht om gehoor te geven aan een oproep. Aldus bestaat er, buiten de arbeidsduur, bijna geen verschil tussen de vrijwillige brandweer en de beroepsbrandweer. Dit betekent dat de vrijwillige brandweer, naar rato van het aantal arbeidsuren, in beginsel recht heeft op dezelfde beloning als de beroepsbrandweer.

Gevolgen voor andere vormen van deeltijd- of vrijwilligerswerk

Voor de veiligheidsregio als werkgever is het van belang om goed voor ogen te houden dat in beginsel niet is toegestaan om vrijwilligers en deeltijdwerkers ongunstiger te belonen op de enkele grond van een verschil in arbeidsduur, in het bijzonder wanneer er sprake is van een sterke gelijkenis ten aanzien van de werkzaamheden. Wilt u toch een lagere beloning afspreken met een vrijwilliger of deeltijdwerker? Dan is het van belang om tot een duidelijk onderscheidend takenpakket te komen. Zo kan er alsnog een rechtvaardiging ontstaan voor een afwijkende beloning. Wij adviseren u dit in overweging te nemen.

Situatie VRK

Het bovenstaande is een algemeen geformuleerde notitie waarvoor landelijk aandacht is benodigd. Voor de VRK ligt de situatie wezenlijk anders. Er is voor de VRK geen sprake van 80% vrijwilligers en er is ook geen opkomstplicht voor de vrijwilligers. Omdat het gaat om een gelijke rechtspositie is het wel van belang de genoemde deelrichtlijn goed te bekijken.

5. Bevindingen interne controle

5.1 Verbijzonderde interne controle (1/2)

Met ingang van verslagjaar 2021 moet het bestuur een (onderbouwde) mededeling doen omtrent rechtmatig handelen

Mededeling door bestuur vraagt om aanscherpingen in de interne beheersing t.a.v. rechtmatigheid

Vernieuwing accountantscontrole - rechtmatigheidsverklaring bestuur

In het VNG-rapport 'Vernieuwing accountantscontrole gemeenten' (juli 2015) is benadrukt dat het bestuur primair verantwoordelijk is voor de naleving van wet- en regelgeving en dat het bestuur verantwoordelijk is voor het toezicht hierop. In de huidige situatie, waarin de accountant een rechtmatigheidsverklaring verstrekt, lijkt de verantwoordelijkheid bij de accountant te liggen of lijkt het erop dat het bestuur zich moet verantwoorden aan de accountant. Om daar verandering in aan te brengen heeft commissie Depla de aanbeveling gedaan dat het bestuur een rechtmatigheidsverklaring opneemt in de jaarrekening. Vanuit de overleggen van het SDO, Ministerie en gemeenten leeft de verwachting dat de rechtmatigheidsverklaring met ingang van verslagjaar 2021 zal worden ingevoerd.

Belangrijk argument om de bedoelde vernieuwing door te voeren is het democratisch proces. Het bestuur is immers uiteindelijk verantwoordelijk voor de naleving van de wet- en regelgeving en dan is het zinvol de discussie over de rechtmatigheid hiervan te laten plaatsvinden tussen dagelijks bestuur enerzijds en het algemeen bestuur anderzijds. Het ministerie wil dit najaar starten met een pilot. Mede afhankelijk van de resultaten van de pilot wordt besloten of en op welke wijze de rechtmatigheidsverantwoording zal worden ingevoerd. Het ministerie van Binnenlandse Zaken zal de commissie BBV, de VNG, het IPO en de NBA betrekken in de nadere uitwerking van deze verplichting.

Om deze verplichting te kunnen invoeren moet de Gemeentewet, het Besluit Accountantscontrole Decentrale Overheden (BADO), de Kadernota rechtmatigheid, etc. nog worden aangepast. Uitgaande van de invoeringsdatum 2021, betekent dit dat er nog ruim twee jaren zijn om dit voor te bereiden. Dat betekent ook dat voor wat betreft de accountantscontrole de rechtmatigheidscontrole nog tenminste tot en met het boekjaar 2020 in scope zal zijn.

De wijziging in de verantwoordelijkheden ten aanzien van rechtmatigheid betekent niet dat er minder rechtmatigheidscontroles moeten worden uitgevoerd, maar dat het bestuur deze zelfstandig/intern moet inrichten, uitvoeren, controleren en rapporteren. In feite wordt de verklaring van het bestuur daarmee een zogenaamde In Control Statement (ICS) ten aanzien van rechtmatigheid. Als accountant zullen wij die werkzaamheden vervolgens toetsen, teneinde te kunnen controleren en verklaren dat de rechtmatigheidsverklaring van het bestuur een getrouw beeld geeft.

5.1 Verbijzonderde interne controle (2/2)

BADO notitie verbijzonderde interne controle decentrale overheid inclusief de vier varianten van VIC.

Verbijzonderde Interne Controle

De afgelopen jaren is veel discussie geweest over de eisen die gesteld moeten worden aan de onafhankelijkheid, positie en kwaliteit van de Verbijzonderde Interne Controle (VIC) en de wijze waarop accountants gebruik kunnen maken van de VIC. De commissie Bedrijfsvoering, Auditing Decentrale Overheden (BADO) heeft op 14 februari 2019 de notitie De verbijzonderde interne controle bij decentrale overheid uitgebracht met als doel een handreiking te bieden aan decentrale overheden ten aanzien van de inrichting van de verbijzonderde interne controle en de mogelijkheden voor de accountant om hiervan gebruik te kunnen maken.

Samenvattend worden in de notitie vier varianten beschreven:
1. de VIC als instrument om de aanlevering van stukken aan de accountant te verbeteren;
2. de VIC als onderdeel van het interne beheersingskader om toezicht te houden op de uitvoering van interne beheersingsmaatregelen;
3. de VIC als interne beheersingsmaatregel, waarop de accountant kan steunen bij zijn organisatiegerichte werkzaamheden;
4. de VIC als interne auditfunctie (IAF, zoals bedoeld in Standaard 610).

Ons beeld van de VIC

Ons beeld van de VIC

De VIC beoogt het vergroten van de transparantie met betrekking tot de wijze waarop de VRK haar bedrijfsvoering ingericht heeft. De VIC is gericht op de werking van de financiële bedrijfsprocessen en heeft als primair doel 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, materieel niet afwijkt van de werkelijkheid en dat wordt voldaan aan de van toepassing zijnde wet- en regelgeving.

Binnen de VRK was er tot en met medio 2019 een onafhankelijke positie voor de VIC functie, daar deze vanuit een onafhankelijke positie haar onderzoeken uit kon voeren en hierover rapporteerde. De VIC functie is sinds medio 2019 echter vacant. Voorheen werd al een deel van de VIC werkzaamheden door medewerkers uitgevoerd van verschillende afdelingen. Nu wordt de vacante functie verder opgevangen door de Finance-afdeling. De betreffende medewerkers hebben echter geen onafhankelijke positie. Daardoor is er vanuit de theorie beschouwd geen optimale onafhankelijkheid geborgd in de organisatie zoals gesteld in de NV COS 610.

De eisen die Standaard 610 stelt aan de externe accountant bij de beoordeling van de objectiviteit en competentie van de internal audit functie zijn hoog. Volgens Standaard 610 moet de VIC voldoen aan het kwaliteitsniveau dat ook voor de controlerend accountants zelf geldt. Wij concluderen dat het (op dit moment) niet realistisch is om te voldoen aan de eisen van de COS 610 c.q. dit op korte termijn ook niet het streven is. Wel kan de VIC ondersteunen bij de accountantscontrole.

Aanbevelingen

Wij constateren dat er momenteel geen VIC aanwezig is bij de Veiligheidsregio Kennemerland. Afhankelijk van de ambitie van de VRK, kan de meerwaarde van de VIC voor de organisatie worden vergroot de VIC onafhankelijk van de Finance-afdeling te laten opereren. Hierbij is het van belang dat de VIC deskundig genoeg is om controlewerkzaamheden uit te voeren om zo als interne beheersingsmaatregel te fungeren en deze te toetsen. Daarnaast kan de VIC ‘aan de voorkant’ expliciete aandacht geven aan de opzet en inrichting van de AO/IB per proces alsmede de advisering daaromtrent (systeem-procesgericht). Wij hebben begrepen dat de organisatie zich naar aanleiding van de vacante VIC functie heroriënteert op de wijze waarop deze functie het beste kan worden ingevuld. Hierbij dienen eerst de doelstellingen in het kader van de beheersing van de bedrijfsvoering per afdeling te worden geformuleerd. Wij onderschrijven het belang van een dergelijke heroriëntatie en analyse, maar benadrukken ook het belang van een onafhankelijke VIC functie.

6. Bijlagen

A. Detailbevindingen processen

Bevinding 1	Contractenbeheer ondersteunt aanbestedingsproces niet voldoende	KANS: Midden
Jaar van constatering	2016 - 2019	IMPACT: Midden

Onze bevinding / constatering	Lopende contracten worden geregistreerd in het contractenregister in Unit4. Unit4 geeft 2 tot 3 maanden voorafgaand aan de opzegtermijn een automatische melding aan budgethouders indien het contract zal gaan verlopen. Sommige budgethouders ondernemen niet (tijdig) actie op de automatische melding uit het systeem. Daarnaast hebben sommige aanbestedingsprocedures een langere looptijd dan 2 tot 3 maanden en zullen daardoor niet tijdig zijn afgerond. Wij hebben tevens vastgesteld dat er geen procesbeschrijving is waaruit blijkt wanneer en hoe er met (mogelijk aanbestedingsplichtige) inkopen omgegaan moet worden. De Veiligheidsregio beschikt echter wel over een inkoopkalender en inkoopbeleid. Dit inkoopbeleid is wel gedateerd (2014-2015).
Geconstateerde opvolging in 2019	In 2019 is dit proces niet gewijzigd.
Risico/gevolg	Het risico bestaat dat aanbestedingstrajecten niet of niet tijdig worden opgestart. Mogelijk kunnen inkopen worden gedaan zonder dat daar een geautoriseerd inkoopcontract aan ten grondslag ligt (contracten vervallen). Hierdoor kunnen onrechtmatigheden in de aanbestedingen optreden.
Ons advies/ uw aanvullende werkzaamheden	Wij adviseren zorg te dragen voor een adequate en tijdige opvolging van de meldingen uit het systeem. Hierbij adviseren wij de signaleringsdatum in Agresso op een vroeger moment op te nemen. Tevens adviseren wij u een adequate procesbeschrijving inzake het aanbestedingsproces op te stellen en het inkoopbeleid te actualiseren. Iedere functionaris binnen de organisatie zou op basis van deze beschrijving kunnen achterhalen wanneer en hoe er aanbesteed dient te worden. Als gevolg van de bovenstaande bevinding hebben wij in onze controleaanpak de werkzaamheden rond de spendanalyse gepland.

Bevinding 2	Controles en aansluitingen in de planning & control cyclus niet altijd zichtbaar	KANS: Midden
Jaar van constatering	2019	IMPACT: Midden

Onze bevinding/ constatering

In het kader van onze controle hebben wij aandacht besteed aan de Planning & Control cyclus ofwel de interne beheersing op organisatieniveau. Indien deze interne beheersing in opzet, bestaan en werking toereikend en aantoonbaar is, kunnen wij hier als accountant gebruik van maken in onze controle.

Middels een gesprek en door het opvragen van onderliggende documenten hebben wij de volgende onderdelen beoordeeld:
1. Inrichting organisatie ten aanzien van financiën en control.
2. Totstandkoming en (zichtbare) autorisatie van de begroting(-swijzigingen).
3. Totstandkoming tussentijdse rapportages (en zichtbaarheid van interne reviews).
4. Het proces van de totstandkoming van de jaarrekening.

Wij hebben geconstateerd dat er onvoldoende zichtbare waarborgen in het proces van opstellen van de planning & control documenten zijn opgenomen. Wij hebben tijdens onze interim-controle vastgesteld dat voorafgaand aan het opstellen van de bestuursrapportages een structureel proces wordt doorlopen. Wij onderschrijven de toepassing van maandrapportages in het huidige jaar, echter is geen sprake van zichtbare tussentijdse aansluitingen met subadministraties en tussenrekeningen worden vooralsnog niet zichtbaar tussentijds geanalyseerd. Er is niet altijd sprake van zichtbare aftekeningen. Verder is er geen sprake van een procedurebeschrijving inzake het planning & control proces (behalve voor de maandrapportages).

Risico/gevolg

Het risico bestaat dat (tussentijdse) rapportages een onjuist beeld geven. Als gevolg hiervan wordt mogelijk gestuurd door het (dagelijks) bestuur op onjuiste informatie en bestaat het risico dat afwijkingen van de begroting te laat worden geconstateerd om bij te kunnen sturen.

Ons advies/ uw aanvullende werkzaamheden

Afhankelijk van de ambitie van Veiligheidsregio Kennemerland, adviseren wij om bij de planning en control cyclus duidelijke procesbeschrijvingen op te stellen met daarin de verantwoordelijkheden van de verschillende medewerkers. Het is hierbij van belang om duidelijk vast te leggen waar gegevens vandaan komen, wie de stukken opstelt en wie de review uitvoert. Daarnaast adviseren wij u het volgende:
- Bij de maandrapportages dient zichtbaar te zijn wie wat uitvoert (middels aftekeningen), inclusief zichtbare aansluiting op de leadsheet.
- De maandrapportages dienen zichtbaar afgetekend te worden door hoofd FA bij de controle.
- Bij de notulen dient eveneens te worden opgenomen wat de opvolging is van de voorgaande maand besproken actiepunten.
- De notulen van de bespreking dienen afgetekend te zijn.
- Deze verbeterpunten ook mee te nemen bij de totstandkoming van de begroting en bestuursrapportages.

De maandrapportages geven daarnaast inzicht in mogelijk leemtes in de processen en kunnen daarmee leiden tot actiepunten voor de processen.

Doordat het proces onvoldoende zichtbare waarborgen kent, kunnen wij geen zekerheid halen uit het proces. Deze zekerheid behalen wij nu door onze overige werkzaamheden uit te breiden, dit leidt tot omvangrijkere steekproeven en aanvullende controles. Er is wel sprake van potentie om het proces dusdanig te verbeteren, dat wij hier in de toekomst wel zekerheid aan kunnen ontlenen.

Reactie management/ opvolging

Van de maandrapportage hebben we maandelijks een digitale map waarin alle aansluitingen e.d. gearchiveerd worden. We zijn het eens dat de maandrapportage als document strakker en volledieger moet en gaan inderdaad werken met aftekenen en actielijsten op afloop e.d. Ook bij een bestuursrapportage worden de resultaten betrokken vanuit het financieel systeem zodat er geen risico is dat onderdelen per abuis buiten beschouwing worden gelaten. Verder worden bij alle B&V producten overal aansluitingen, diverse controles e.d. vastgelegd en gearchiveerd.

Bevinding 3	Niet alle processen en verantwoordelijkheden zijn in procesbeschrijvingen vastgelegd	KANS: Laag
Jaar van constatering	2019	IMPACT: Laag

Onze bevinding/ constatering	De Veiligheidsregio heeft de diverse aanwezige werkprocessen vastgelegd in procesbeschrijvingen middels de ‘6 W-vragen’ *(maandrapportages en salarisverwerking). Echter is dit niet voor alle processen het geval zoals voor de processen: inkopen, aanbestedingen en overige opbrengsten.
Risico/gevolg	Het risico bestaat dat de gewenste interne controles niet aanwezig zijn, niet bekend zijn bij de medewerker en dus niet worden nageleefd. Deze ontbrekende controls verhogen het risico op onjuiste/ onrechtmatige kosten, verantwoordingen en/of onvolledige opbrengsten. Daarnaast bestaat ook de mogelijkheid dat door onvoldoende inzicht in de risico’s en getroffen beheersingsmaatregelen doublures zijn opgenomen in de processen, waardoor de processen minder efficiënt worden uitgevoerd.
Ons advies/ uw aanvullende werkzaamheden	Wij adviseren u om per significant proces een procesbeschrijving op te stellen. Voor de bestaande procesbeschrijvingen adviseren wij u de aanwezige procesbeschrijvingen uit te breiden door expliciet aandacht te besteden aan de ‘6 w-vragen’. Het resultaat van deze verbetering is dat ook mogelijke leemtes in de processen worden onderkend en kunnen worden gerepareerd. Door het ontbreken van procesbeschrijvingen is onze interim-controle minder efficiënt en blijven wij jaarlijks (reeds bestaande) leemtes in processen identificeren. Deze leemtes kunnen vaak niet meer hersteld worden in het boekjaar, waardoor onze gegevensgerichte werkzaamheden omvangrijk blijven.
Reactie management/ opvolging	Een aantal beschrijvingen zijn nog op de oude manier opgenomen in het kwaliteitshandboek maar we willen alle beschrijvingen omzetten in de matrixvorm. De beschrijving van inkoop tot factuur is aangehouden omdat er een nieuwe wijze van inkooporders invoeren geïmplementeerd gaat worden en we dan de beschrijving hierop aanpassen.

Bevinding 4	Volledigheid verbonden partijen	KANS: Laag
Jaar van constatering	2019	IMPACT: Laag

Onze bevinding/ constatering	Tijdens de controle hebben wij geconstateerd dat er sprake is van een omissie bij de identificatie van verbonden partijen. Vorig jaar is niet geconstateerd dat het Instituut Fysieke Veiligheid (IFV) een verbonden partij betreft en derhalve toegelicht dient te worden in de jaarrekening. Er is sprake van een verbonden partij, omdat sprake is van bestuurlijke verbondenheid: De 25 voorzitters van de veiligheidsregio's vormen samen het algemeen bestuur van het IFV. Voor 2019 is Brandweerschool Noord-Holland een nieuw opgerichte verbonden partij. Derhalve dient deze net als het IFV in de jaarrekening 2019 te worden toegelicht.
Risico/gevolg	Het risico bestaat dat de verslaggeving omtrent verbonden partijen, rechten- en verplichtingen materiële onjuistheden bevat en dit leidt tot vragen van het ministerie van BZK.
Ons advies/ uw aanvullende werkzaamheden	Wij adviseren om de monitoring en controle op compliance formeel in te richten en verantwoordelijkheden te beleggen bij medewerkers met de juiste competenties/aanverwante verantwoordelijkheden. Zij zouden, op basis van opgestelde richtlijnen en afspraken de compliance kunnen bewaken. Zo heeft de VIC de verantwoordelijkheid voor het identificeren, analyseren en vastleggen van de verbonden partijen. De BBV geeft duidelijke richtlijnen omtrent het identificeren van de verbonden partijen. Zolang geen sprake is van een VIC, dit dient dan bij ander verantwoordelijk persoon te worden neergelegd.

Bevinding 5	Contracten debiteuren niet centraal geregistreerd	KANS: Laag
Jaar van constatering	2019	IMPACT: Midden

Onze bevinding/ constatering	De volledigheid van de opbrengsten kan niet met zekerheid worden vastgesteld doordat niet alle contracten met afnemers/debiteuren centraal worden geregistreerd. Tijdens de controle van het proces omtrent de overige opbrengsten is vastgesteld dat de contracten met afnemers niet volledig centraal worden geregistreerd. Bij de controle ging het specifiek om het contract met de politie omtrent de prijzen bij forensische geneeskunde.
Risico/gevolg	Het risico bestaat dat niet de afgesproken prijs wordt gefactureerd waardoor de omzet niet volledig wordt verantwoord. Wanneer contracten niet worden geregistreerd bestaat ook het risico dat de opbrengsten geheel niet worden gefactureerd.
Ons advies/ uw aanvullende werkzaamheden	Wij adviseren u om de getekende contracten door een bevoegd persoon te laten registreren. Hierbij hebben wij nog de volgende aanbevelingen: - Functiescheiding tussen contract tekenen en registratie van het contract. - Zichtbare controle op de registratie/wijzigingen van het contract bijvoorbeeld middels workflow in Unit4. - Indien er geen automatische koppeling is bij facturatie, dient er zichtbare controle op de gemaakte factuur te worden verricht waarbij aansluiting wordt gemaakt met de prijzen in het systeem. Deze leemte kan niet meer worden hersteld in het boekjaar, waardoor er een gegevensgerichte aanpak zal worden toegepast bij de eindejaarscontrole.
Reactie management/ opvolging	Contracten kunnen ook bij de sector (vakafdeling) zelf zijn geregistreerd, zoals bijv. forensisch. Maandelijks wordt hiervoor gefactureerd en wordt een aansluiting gemaakt tussen Formatus (waarin de jaarlijkse tarieven opgenomen staan) en de financiële administratie. Dit waarborgt dat de juiste tarieven worden gebruikt.

Bevinding 6	De overige inkomstenstromen worden niet volledig gemonitord	KANS: Laag
Jaar van constatering	2018 - 2019	IMPACT: Midden

Onze bevinding/ constatering	De volledigheid van de opbrengsten kan niet met zekerheid worden vastgesteld doordat de werkzaamheden die leiden tot de overige opbrengsten niet volledig kunnen worden gemonitord. Tijdens de controle is geconstateerd dat er geen planning is omtrent het geven van cursussen en andere werkzaamheden die vervolgens worden gefactureerd. Hierdoor is er binnen de organisatie geen zicht op welke werkzaamheden gefactureerd zouden moeten worden en welke werkzaamheden daadwerkelijk zijn gefactureerd. Medewerkers die dergelijke werkzaamheden uitvoeren, geven aan de financiële administratie door wat er gefactureerd dient te worden.
Geconstateerde opvolging in 2019	In 2019 is er geen wijziging in het proces ten opzichte van vorig jaar geconstateerd.
Risico/gevolg	Dit leidt tot een risico dat medewerkers vanuit eigen naam de werkzaamheden factureren dan wel niet alle werkzaamheden doorgeven en daardoor niet alles wordt gefactureerd. Dit leidt daardoor mogelijk tot een onvolledige opbrengstverantwoording.
Ons advies/ uw aanvullende werkzaamheden	Wij adviseren om iemand verantwoordelijk te maken voor de planning van de overige werkzaamheden. Deze persoon plant, in samenspraak met de FA verschillende medewerkers op deze werkzaamheden. Bij afronding geven deze medewerkers dit door aan de planning waarna planning bij de FA aangeeft dat er gefactureerd kan worden. Bij het maken van deze planning is de FA dus betrokken om zo de volledigheid van de facturatie te waarborgen. Daarnaast adviseren wij nog het volgende: - Een koppeling tussen de voorraad uitgifte van de vaccinaties en de gerealiseerde opbrengsten uit hoofde van vaccinaties. - Monitoring van inkomende subsidies waarbij wordt gekeken naar de gevraagde informatie in de beschikkingen en de informatie welke beschikbaar is binnen de organisatie. Deze leemte kan niet meer worden hersteld in het boekjaar, waardoor er een gegevensgerichte aanpak zal worden toegepast bij de eindejaarscontrole.
Reactie management/ opvolging	Als dit op het voorbeeld van cursussen is gebaseerd zoals wordt beschreven, heeft dat wel nuance nodig. Nu lijkt het alsof we niets monitoren maar dat doen we juist wel bijv. bij elke bestuursrapportage kijken we organisatie breed of er vreemde afwijkingen zijn ten opzichte van begroting, wat er nog mist e.d. Daarnaast controleren uiteraard de adviseurs regelmatig de inkomsten in de begroting en realisatie bij het afgeven van hun prognoses richting budgethouders.

B. Detailbevindingen ICT

Bevinding	PROCEDURE AUTORISATIEBEHEER & PERIODIEKE CONTROLE OP JUISTHEID INGERICHTE AUTORISATIES (1/2)	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: middel

Bevindingen:

Autorisatiebeheer

Unit 4 Business World

Voor Unit 4 Business World hebben wij vastgesteld dat een normpositie van toegekende rechten per rol aanwezig is. Een normpositie waarin is beschreven welke organisatorische functie binnen de VRK mag beschikken over welke Unit 4 rol was ten tijde van onze audit nog niet beschikbaar. Na onze auditwerkzaamheden heeft de VRK hier opvolging aan gegeven middels het opstellen van deze normpositie.

Het loggen van gebruikers- en autorisatiemutaties in Unit 4 Business World is door de VRK opgevolgd (bevinding 2018). Een periodieke beoordeling van deze logging door de VRK zelf wordt nog niet uitgevoerd.

VP & InPlanning:

Voor het aanmaken en wijzigen van gebruikers en autorisaties in de applicatie InPlanning en VP wordt geen gebruik gemaakt van een formeel door het management geaccordeerde normpositie waarin de rollen en rechten in de applicatie per organisatorische functie zijn gespecificeerd. Rechten worden momenteel op basis van kennis en ervaring van de applicatiebeheerder toegevoegd. Er worden daarnaast nog niet structureel vastleggingen gemaakt van alle mutaties rondom toekennen, wijzigen, en het intrekken van rechten, waardoor dit niet (volledig) voor ons controleerbaar is.

Periodieke reviews van autorisaties:

Voor Unit 4 Business World vastgesteld dat in 2019 een review heeft plaatsgevonden naar de gebruikers en toegekende rollen. Een periodieke review naar de juistheid van onderliggende autorisaties per rol (a.d.h.v. de normpositie) is in 2019 nog niet uitgevoerd.
Voor InPlanning heeft in 2019 een periodieke review van autorisaties plaatsgevonden, maar is deze niet vastgelegd en derhalve kunnen wij dit niet vaststellen.
Voor VP heeft in 2019 geen zichtbare periodieke review van autorisaties plaatsgevonden. In overleg met de leverancier heeft wel een opschoning van gebruikers plaatsgevonden welke lang niet zijn ingelogd. Deze review is niet vastgelegd en daarmee niet aantoonbaar.

Risico/gevolg

Als autorisaties niet op basis van een formele normpositie worden toegekend, bestaat het risico dat gebruikers over autorisaties komen te beschikken die niet passen bij de functie van de medewerker en waardoor controletechnische functiescheiding kan worden doorbroken. Dit kan leiden tot ongeautoriseerde handelingen in het systeem. Het risico van het niet tijdig blokkeren van accounts van medewerkers uit dienst is dat er mogelijk ongeautoriseerde handelingen door de medewerker zelf, of andere medewerkers in bezit van het wachtwoord, kunnen worden uitgevoerd.

Door het ontbreken van controleerbare periodieke controles op de toegekende autorisaties binnen de applicaties, bestaat het risico dat gebruikers meer rechten in deze applicaties hebben dan nodig uit hoofde van hun functie, dan wel dat dit niet of te laat wordt gedetecteerd. De in de applicaties aangebrachte functiescheiding kan hierdoor worden doorbroken met mogelijk ongeautoriseerde handelingen tot gevolg.

Bevinding	PROCEDURE AUTORISATIEBEHEER & PERIODIEKE CONTROLE OP JUISTHEID INGERICHTE AUTORISATIES (2/2)	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: middel

Ons advies/ uw aanvullende werkzaamheden

Wij adviseren om:

- Voor Unit 4 Business World: Een normpositie op te stellen waarbij wordt aangegeven welke organisatorische functie over welke basisrol in Unit 4 mag beschikken, rekening houdend met functiescheiding. Deze normpositie dient tevens te worden gebruikt bij het proces van in dienst en het toekennen van autorisaties. Daarnaast adviseren wij deze normpositie jaarlijks te herzien en door het management te laten accorderen.
    - Noot: Deze aanbeveling rondom het opstellen van de rollen per organisatorische functie is reeds door VRK opgepakt na onze auditwerkzaamheden.
- Voor InPlanning en VP: De organisatorische functiescheiding te vertalen in functie-/rolautorisatiematrices (normposities) waarin de benodigde autorisaties per applicatie per organisatorische functie zijn benoemd. Deze normposities dienen tevens te worden gebruikt bij het toekennen van autorisaties en kunnen als uitgangpunt dienen voor de periodieke controle op autorisaties.
- Logging vanuit het systeem op gebruikers- en autorisatiemutaties is geactiveerd voor Unit 4 Business World. Wij adviseren ook te onderzoeken of logging binnen de applicaties VP en InPlanning is te activeren op alle gebruikers- en autorisatiemutaties. Daarnaast adviseren wij deze logging ook periodiek te beoordelen aan de hand van geautoriseerde verzoeken.
- Ten aanzien van uit dienst en het intrekken van accounts, waarborgen in het proces in te bouwen dat gebruikersaccounts tijdig worden geblokkeerd op zowel het netwerk als in de applicaties (uiterlijk laatste werkdag) en dit ook achteraf te kunnen aantonen.
- De periodieke controles op actualiteit en juistheid van toegekende autorisaties vast te leggen en daarbij te waarborgen dat de volgende onderdelen worden afgedekt:
    - de controle wordt uitgevoerd op de werkelijke situatie uit het systeem (IST) ten opzichte van de opgestelde normpositie (SOLL);
    - de controle zich richt op zowel actieve gebruikers, rechten per rol, alsmede de juistheid van toegekende autorisaties / rollen aan gebruikers;
    - de opvolging van bevindingen uit reviews zichtbaar is uitgevoerd.

Reactie management/ opvolging

Bevinding	IDENTIFICATIE & SUPERUSERS (1/2)	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: hoog

Identificatie

Unit 4 Business World & InPlanning:
Generieke accounts zijn beperkt en verklaarbaar.

VP:
Er zijn 32 generieke gebruikersaccounts aangetroffen binnen VP. Deze zijn niet op basis van naamgeving of gekoppeld e-mailadres terug te herleiden naar een individueel persoon. Het betreft een relatief groot aantal generieke accounts en het bestaan van deze generieke accounts is niet altijd verklaarbaar vanuit gebruiks- of beheerdoeleinden. Tevens stellen wij vast dat bepaalde gebruikers met verhoogde rechten in de applicatie kunnen inloggen “als een andere gebruiker” (login als). Deze functionaliteit is niet wenselijk aangezien identificatie van handelingen naar een individuele gebruiker onmogelijk wordt.

Superusers

Unit 4 Business World:
Vastgesteld dat superuser rechten binnen Unit 4 Business World beperkt zijn tot 6 accounts. Drie van deze accounts zijn van de leverancier of betreffen technische accounts en drie accounts betreffen medewerkers van de VRK. Twee van deze drie VRK medewerkers zijn verklaarbaar uit hoofde van functie en betreffen de applicatiebeheerders. Een derde medewerker betreft een medewerker welke ook betrokken is bij de operationele bedrijfsvoering van de VRK, waarbij het in basis onwenselijk is om deze persoon superuser rechten te geven. Na onze auditwerkzaamheden heeft de VRK aangegeven dat hier opvolging aan is aangegeven en de superuser rechten bij deze medewerker zijn ingetrokken.

InPlanning:
Gebruikers met superuser rechten binnen InPlanning zijn beperkt zijn tot 2 bevoegde gebruikers (applicatiebeheerders).

VP:
Er zijn 15 gebruikersaccounts met beheerrechten in VP aangetroffen. Dit betreffen ook gebruikers uit de operationele organisatie van de VRK, waaronder enkele generieke accounts en accounts waarvan niet duidelijk is waarom zij beheerrechten hebben. De superuser rechten zijn niet beperkt tot een strikt noodzakelijk minimum.

Risico/gevolg

Met betrekking tot het gebruik van generieke gebruikersaccounts bestaat het risico dat transacties die zijn uitgevoerd niet kunnen worden herleid tot een bepaald individu. Dientengevolge kunnen medewerkers niet of beperkt verantwoordelijk worden gesteld voor, bewuste of onbewuste, ongewenste acties in de systemen.

Superusers hebben vanuit hun aard ruime rechten in de applicatie en brengen hierdoor het risico met zich mee dat controletechnische functiescheidingen worden doorbroken. Derhalve is het van belang dat superuser rechten alleen beschikbaar zijn voor een beperkte groep van (geautoriseerde) gebruikers voor wie dat strikt noodzakelijk is vanuit beheerdoeleinden.

Bevinding	IDENTIFICATIE & SUPERUSERS (2/2)	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: hoog

Ons advies/ uw aanvullende werkzaamheden	Wij adviseren om de generieke accounts binnen VP kritisch door te nemen en deze zoveel mogelijk te minimaliseren tot strikt noodzakelijk en te waarborgen dat er geen gedeelde accounts aanwezig die in gebruik zijn bij meerdere medewerkers. Wij adviseren om superuser rechten alleen toe te kennen aan personen van de IT-afdeling of afdeling applicatiebeheer om functiescheiding tussen de beheerorganisatie en de gebruikersorganisatie te waarborgen. Het aantal superuser accounts dient beperkt te zijn tot een strikt noodzakelijke groep van IT-medewerkers of applicatiebeheerders, en indien mogelijk, dienen superuser handelingen te worden gemonitord.
Reactie management/ opvolging	

Bevinding	WACHTWOORDBELEID - VP & INPLANNING	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: hoog

Voor Unit 4 Business World hebben wij geen bevindingen aangezien er voldoende sterke wachtwoordvereisten zijn ingericht.
Voor het inloggen op InPlanning en VP zijn beperkte wachtwoordeisen van kracht en behoeft dit nog aanscherping in het kader van onze jaarrekeningcontrole.

Op basis van systeemwaarnemingen hebben wij vastgesteld dat de volgende wachtwoordvereisten worden afgedwongen voor de applicaties VeiligheidsPaspoort en InPlanning:

WACHTWOORDINSTELLINGEN	VeiligheidsPaspoort	InPlanning
Minimale wachtwoordlengte	6 karakters	8 karakters
Wachtwoordcomplexiteit	ingesteld	ingesteld
Maximale wachtwoordleeftijd (verplichting tot periodiek wijzigen)	**niet ingesteld**	**niet ingesteld**
Minimaal de laatste 5 wachtwoorden mogen niet hergebruikt worden	**niet ingesteld**	**niet ingesteld**
Het account wordt na een beperkt aantal foutieve inlogpogingen geblokkeerd	**niet ingesteld**	**niet ingesteld**
Initiële wachtwoordwijziging	**niet ingesteld**	ingesteld

NB. De rode dikgedrukte rode tekst in de tabel behoeft verbetering.

Risico/gevolg

Als gevolg van de gesignaleerde bevindingen met betrekking tot het wachtwoordbeheer bestaat het risico dat wachtwoorden bekend raken of worden geraden, en dat ongeoorloofd gebruik wordt gemaakt van gebruikersaccounts. Hierdoor kan functiescheiding ongemerkt worden doorbroken: een gebruiker kan mogelijk toegang krijgen tot kritieke transacties waartoe hij uit hoofde van interne beheersing geen toegang zou moeten hebben. Daarnaast is niet zeker dat de gebruiker zoals geïdentificeerd door de applicatie ook verwijst naar de medewerker die de handeling daadwerkelijk heeft verricht. Dientengevolge kunnen medewerkers niet of beperkt verantwoordelijk worden gesteld voor, bewuste of onbewuste, ongewenste acties in de systemen.

Ons advies/ uw aanvullende werkzaamheden

Het verdient aanbeveling om de wachtwoordinstellingen te evalueren. Wij bevelen aan om te beoordelen in hoeverre de in rood genoemde elementen aangescherpt kunnen worden. Minimale vereisten die wij in het kader van de jaarrekeningcontrole zouden verwachten zijn: Wachtwoorden periodiek te laten wijzigen na maximaal 180 dagen, een wachtwoordhistorie van minimaal 5 (laatste 5 wachtwoorden onthouden), gebruikersaccounts te laten blokkeren na maximaal 7 foutieve inlogpogingen en gebruikers bij de eerste keer inloggen het wachtwoord te laten wijzigen naar een eigen gekozen wachtwoord.

Reactie management / opvolging

Bevinding	WIJZIGINGENBEHEER UPDATES (1/2)	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: middel

Er is geen formele procedurebeschrijving change management voor de applicaties in scope van onze controle aanwezig.

Unit 4 Business World:
Er zijn gedurende 2019 tot het moment van onze audit geen nieuwe Milestones doorgevoerd op Unit 4 Business World, derhalve hebben wij het bestaan van de wijzigingenbeheerprocedure aan de kant van de VRK niet vast kunnen stellen. Wel zijn er enkele hotfixes doorgevoerd door de leverancier. Hotfixes worden op impact beoordeeld door de applicatiebeheerder en afhankelijk daarvan wordt bepaald of er getest wordt. Een zichtbare beoordeling van deze impactanalyse en risico afweging hebben wij niet kunnen waarnemen omdat dit niet wordt vastgelegd. De leverancier van Unit 4 beschikt over een SOC 1 type 2 assuranceverklaring waarin ook deels maatregelen rondom wijzigingsbeheer worden afgedekt. Een interne beoordeling van de verklaring is nog niet door de VRK uitgevoerd maar dit is wel gepland zodra de verklaring over 2019 beschikbaar komt.

InPlanning:
Op basis van de SLA met de leverancier stellen wij vast dat zij op iedere nieuwe versie een systeemtest uitvoeren. Dit is niet aantoonbaar aangezien de leverancier niet beschikt over een geschikte assurance rapportage. Tevens staat in de SLA benoemd dat, bij versie upgrades, de opdrachtgever (VRK) zelf een Acceptatietest dient uit te voeren op een eigen testomgeving met als doel het vaststellen of de nieuwe versie aan alle eisen voldoet om deze beheerst in productie te kunnen nemen. Wij hebben op basis van interview met de applicatiebeheerder bij VRK vastgesteld dat: 1) De releasenotes op impact worden doorgenomen; 2) Testen worden uitgevoerd in de testomgeving.
Echter zijn hiervan geen vastleggingen beschikbaar waarmee dit kan worden aangetoond. Wel hebben wij op basis van inspectie van 1 update vastgesteld dat een vastlegging wordt gemaakt van het akkoord voor het in productie nemen van de wijziging.

VP:
Op basis van interview stellen wij vast dat de leverancier niet beschikt over een geschikte assurance rapportage waarmee zekerheid wordt verschaft over een adequate change management procedure. Wij hebben op basis van interview vastgesteld dat testen door key-users worden uitgevoerd, maar vastleggingen hiervan niet aanwezig zijn.

Risico/gevolg

Onbeheerste of niet tijdig doorgevoerde wijzigingen in de functionele werking van geautomatiseerde gegevensverwerkende systemen, waardoor mogelijk de betrouwbare werking niet is gewaarborgd.

Bevinding	WIJZIGINGENBEHEER UPDATES (2/2)	KANS: middel
Jaar van constatering	2018 + update 2019	IMPACT: middel

Ons advies/ uw aanvullende werkzaamheden	Wij adviseren u om de procedure wijzigingsbeheer te formaliseren, opdat deze werkzaamheden door alle medewerkers in uw organisatie op dezelfde wijze worden uitgevoerd en dat de uitgevoerde controles aantoonbaar zijn. Wijzigingsverzoeken, problemen of incidenten dienen op een gestructureerde manier te worden gerapporteerd, en verzoeken tot wijziging dienen door de juiste persoon/personen te worden geautoriseerd. Op deze manier is duidelijk waar de verantwoordelijkheden liggen met betrekking tot het wijzigingsbeheer. In de praktijk adviseren wij in uw organisatie een procedure wijzigingsbeheer voor de jaarrekening relevante applicaties te hanteren waarin: - Het proces rondom het beheer van software updates wordt gedocumenteerd. - Updates vooraf worden geautoriseerd voor ontwikkeling of implementatie in de testomgeving, na een zichtbare analyse op impact op basis van de beoordeling van releasenotes. - Updates worden getest en geaccepteerd door de gebruikersorganisatie in een aparte, gescheiden testomgeving. - Updates naar productie worden verplaatst na formele acceptatie door de gebruikersorganisatie. Voor applicaties waarbij de beheersingsmaatregelen rondom change management en / of continuïteit aan de leverancier zijn overgedragen is het van belang dat door de VRK actief wordt toegezien op het adequaat inrichten en voldoen aan deze maatregelen. Een van de mogelijkheden is dat jaarlijks wordt verzocht om een assurance rapportage van deze partijen, teneinde zekerheid te krijgen over een juiste inrichting en uitvoering van deze beheersingsmaatregelen. Een veelvoorkomende assurance rapportage in dit kader is de ISAE 3402 of SOC Type II. Hiermee kan de leverancier aantoonbaar aan de relevante uitbestede maatregelen rondom change management & continuïteit voldoen, zoals afgesproken in de SLA en / of contracten met de VRK. Wij adviseren de VRK de leveranciers van SaaS-oplossingen te vragen een ISAE 3402 of SOC assurance rapport te overleggen.
Reactie management/ opvolging	

Bevinding	IT-CONTINUÏTEIT (1/2)	KANS: laag
Jaar van constatering	2018 + update 2019	IMPACT: hoog

Er is geen formele procedurebeschrijving back-up / recovery (continuïteitsplan) voor de applicaties in scope van onze controle aanwezig.

Unit 4 Business World:
De data van Unit 4 Business World staat fysiek gehost bij Microsoft Azure. Microsoft Azure beschikt over een assurance rapportage om zekerheid te geven over controls rondom de fysieke beveiliging van het datacenter. Back-ups worden door de leverancier Unit 4 gemaakt en gemonitord. Unit 4 beschikt over een ISAE 3402 Type II assurance rapportage. De VRK heeft nog geen zichtbare controle uitgevoerd op deze assurance rapportages van de leveranciers waaraan een deel van de beheersing is uitbesteed en is van plan om dit, bij het beschikbaar komen van de verklaring over 2019 (begin 2020), nog uit te voeren.

Vanuit de VRK is in 2019 richting de leverancier geen verzoek gedaan tot het uitvoeren van een full restoretest op Unit 4 Business World, om te testen of vanuit een back-up weer een volledig en juist werkende productieomgeving kan worden opgesteld.

InPlanning:
De data voor InPlanning is ondergebracht bij leverancier Fundaments. Fundaments beschikt over een ISAE 3402 assurance rapportage. Dit betreft nog een type 1 verklaring (opzet/bestaan). Derhalve kan er met deze ISAE 3402 rapportage geen zekerheid worden verkregen over de werking van ingerichte beheersmaatregelen omtrent fysieke toegangsbeveiliging van het datacenter waar InPlanning wordt gehost. Wij adviseren de VRK om zelf inzage te krijgen in waar de data voor InPlanning wordt gehost en of het datacenter beschikt over een adequate en dekkende assurance rapportage om (aantoonbaar) te waarborgen dat maatregelen rondom fysieke beveiliging zijn getroffen.

Leverancier Intus beschikt niet over een ISAE 3402 of SOC assurance rapportage, waarmee aantoonbaar verantwoording wordt afgelegd over de afspraken zoals gemaakt in de SLA, waaronder back-up & recovery maatregelen. Uit navraag bij de leverancier blijkt dat er back-ups worden gemaakt en restoretesten worden uitgevoerd. Echter is hiervan geen bewijs aangeleverd om dit aan te tonen. Derhalve kunnen wij niet vaststellen of back-ups daadwerkelijk worden gemaakt, conform de SLA. VRK voert ook geen eigen monitoring uit op de back-ups van InPlanning.

VP:
De fysieke hosting van VP wordt uitgevoerd door Previder. Previder beschikt over een SOC2 assuranceverklaring om zekerheid te geven over controls rondom de fysieke beveiliging van het datacenter. De VRK heeft nog geen zichtbare controle uitgevoerd op deze assurance rapportage van de leverancier. Wij adviseren de VRK om zelf inzage te krijgen in waar de data voor VP wordt gehost en of het datacenter beschikt over een adequate en dekkende assurance rapportage om (aantoonbaar) te waarborgen dat maatregelen rondom fysieke beveiliging zijn getroffen.

Voor back-up en recovery maatregelen worden deze door de leverancier van VP uitgevoerd (Magenta). Er is vanuit de VRK beperkt inzicht in hoeverre er back-up en recovery maatregelen zijn ingericht door Magenta. Stukken zoals een SLA en / of informatie in hoeverre een assurance rapportage aanwezig is zijn niet beschikbaar. Op basis van interview hebben wij vastgesteld dat leverancier Magenta niet over een ISAE 3402 of SOC assurance rapportage beschikt. Zij geven wel aan dat er back-ups worden gemaakt en deze ook periodiek worden ingelezen op een acceptatieomgeving. Echter is hiervan geen bewijs aangeleverd om dit aan te tonen. Derhalve kunnen wij niet vaststellen of back-ups daadwerkelijk worden gemaakt en gemonitord. VRK voert ook geen eigen monitoring uit op de back-ups van VP.

Bevinding	IT-CONTINUÏTEIT (1/2)	KANS: laag
Jaar van constatering	2018 + update 2019	IMPACT: hoog

Risico/gevolg	Back-up en recovery-maatregelen beperken het risico dat bij uitval van het geautomatiseerde systeem de bedrijfsprocessen stilvallen. Door het ontbreken van een periodieke restore en/of uitwijktest bestaat het risico dat bij een calamiteit blijkt dat de herstelmogelijkheden van de back-up oplossingen niet functioneren.
Ons advies/ uw aanvullende werkzaamheden	Wij adviseren u om: - Zekerheid te verkrijgen over adequate beheersingsmaatregelen fysieke beveiliging en een juiste en volledige uitvoer en monitoring van back-ups voor Unit 4 Business World, InPlanning en VP. Dit kan bijvoorbeeld middels het verzoeken om een ISAE 3402 Type II of SOC assuranceverklaring, zoals ook opgenomen onder onze aanbeveling bij change management, dan wel om eigen monitoring activiteiten in te richten. - Voor alle jaarrekeningrelevante applicaties, minimaal jaarlijks een periodieke full restoretest uit te voeren en vast te leggen om zodoende de bruikbaarheid (integriteit) van de back-up vast te stellen.
Reactie management/ opvolging	