30 januari 2024

MANAGEMENTLETTER 2023

Veiligheidsregio Limburg-Noord

Aanbiedingsbrief

Aan het dagelijks bestuur van de
gemeenschappelijke regeling
Veiligheidsregio Limburg-Noord
Postbus 11
5900 AA VENLO

Eindhoven, 30 januari 2024
Kenmerk: 1053616/DMe/IBi/240039

Geacht dagelijks bestuur,

In het kader van de aan ons verstrekte opdracht tot de controle van de jaarrekening 2023 van de gemeenschappelijke regeling Veiligheidsregio Limburg-Noord 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 de overige afspraken verwijzen wij naar de opdrachtbevestiging 2023.

In deze rapportage richten wij ons met name op de mogelijke verbeterpunten in de bedrijfsvoering en de processen die wij hebben onderzocht in het kader van de controle van de jaarrekening. Dit heeft tot doel een bijdrage te leveren aan de interne beheersing en het zelf controlerend vermogen van uw organisatie.

Wij willen uw medewerkers bedanken voor de prettige samenwerking.

Wij vertrouwen erop u met deze managementletter van dienst te zijn geweest. Wij zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,

BDO Audit & Assurance B.V.
namens deze,

Digitaal ondertekend door:
Dennis Meeuwissen
30 januari 2024 14:42 +01:00...

drs. D.O. Meeuwissen RA
Partner en extern accountant Veiligheidsregio Limburg-Noord

Inhoudsopgave

1. Dashboard interim-controle

1.1 Dashboard interim-controle

RECHTMATIGHEIDSVERANTWOORDING

- In de controleverklaring bij de jaarrekening 2023 geven wij geen oordeel over de rechtmatigheid van de jaarrekening met uitzondering van de SiSa-bijlage. Met ingang van het boekjaar 2023 neemt u een rechtmatigheidsverantwoording op in de jaarrekening. Deze rechtmatigheidsverantwoording is onderdeel van ons getrouwheidsoordeel. U dient ook een rechtmatigheidsverklaring bij de SiSa-bijlage te verstrekken.
- Uw (ambtelijke) organisatie is voorbereid voor het opstellen van de rechtmatigheidsverantwoording in de jaarrekening 2023. De verantwoordingsgrens is door het algemeen bestuur vastgesteld op 1% van de totale lasten inclusief de stortingen in de reserves. De rapporteringsgrens is hierbij vastgesteld op 10% van de verantwoordingsgrens.

AANDACHTSPUNTEN

- De landelijke kaders voor de rechtmatigheidsverantwoording zijn nog deels in ontwikkeling. Bij het schrijven van de managementletter zijn diverse documenten gepubliceerd, ter consultatie aangeboden of onderhanden. Wij adviseren u de ontwikkelingen nauw te volgen en hierop te anticiperen.
- Over- en onderschrijdingen van baten of onderschrijdingen van lasten/investeringen zijn op zichzelf geen begrotings-onrechtmatigheden maar het kan wel onrechtmatig zijn als deze afwijkingen niet tijdig in de bijgestelde begroting zijn verwerkt. Wat tijdig en acceptabel is, wordt bepaald door de interne afspraken tussen het algemeen en dagelijks bestuur over het rapporteren van afwijkingen en het aanpassen van de begroting.

INTERNE BEHEERSING

- Wij komen tot de conclusie dat uw administratieve organisatie en interne beheersing, voor zover relevant voor de controle van de jaarrekening, in opzet voldoende en in bestaan (nog) deels niet voldoende is. Dit betekent niet dat uw organisatie niet in control is. Wij kunnen echter voor wat betreft de insteek van onze controle niet volledig op de processen steunen en derhalve is onze controle overwegend gegevensgericht. Deze situatie is ongewijzigd ten opzichte van voorgaand controlejaar.
- Wij hebben geconstateerd dat de gebruikers in de bank-applicatie van ING en Rabobank een zelfstandige betalings-bevoegdheid hebben. Naar aanleiding van de controle van de ‘Af’-mutaties van januari tot en met medio november 2023 hebben wij geen niet-zakelijke transacties geïdentificeerd.

TUSSENTIJDSE CONTROLE

- Wij hebben tussentijdse controlewerkzaamheden verricht ten aanzien van:
  - de memoriaalboekingen;
  - de inkopen van goederen en diensten;
  - de salarissen en sociale lasten;
  - de bijdragen van het Rijk en de gemeenten.
- Naar aanleiding van deze gegevensgerichte werkzaamheden hebben wij geen bijzonderheden van materieel belang geconstateerd.
- Over de resterende werkzaamheden, de aanpak en de benodigde controledocumentatie hebben wij afspraken gemaakt met de adviseur AO/IC.

IT-BEHEERSING

- Onze conclusie is dat de algemene IT-beheersmaatregelen in opzet en bestaan deels niet voldoende scoren. Voor onze accountantscontrole kunnen wij derhalve nog geen systeem-gerichte controle verrichten en dienen wij gegevensgericht de getrouwheid van uw jaarrekening vast te stellen.
- Wij hebben van uw chief information security officer en functionaris gegevensbescherming vernomen dat er in de periode van 1 januari 2023 tot en met 15 november 2023 28 informatieveiligheidsincidenten, waarvan geen datalekken, hebben plaatsgevonden. Op grond van uw inschatting op een nihil risico op een privacy-inbreuk van de betrokkenen heeft u geen melding bij de Autoriteit Persoonsgegevens gedaan.

VOORUITBLIK JAARREKENNG 2023

Wij vragen uw aandacht voor de volgende onderwerpen in de voorbereiding op het jaarrekeningtraject 2023:

- de aanlevering van een spendanalyse over de gehele vier-jaarsperiode 2020-2023 met een toetsing op de naleving van de Europese aanbestedingsregels met een specifieke aandacht voor de aandachtspunten uit de SDO-notitie ‘Uitvoering van controle op aanbestedingsrechtmatigheid bij jaarrekeningcontrole van decentrale overheden’, in het bijzonder wezenlijke wijzigingen en ontoelaatbare overschrijdingen;
- de berekening van de voorziening voor bovenmatige (boven-wettelijke) verlofuren resp. verlofsparen per 31-12-2023;
- de aansluiting tussen het saldo in de onderhoudsvoorziening per 31-12-2023 en het onderliggende beheerplan (inclusief een verschillenanalyse).

2. Ontwikkelingen & Actualiteiten

2.1 Rechtmatigheidsverantwoording (1/4)

Geen apart oordeel over rechtmatigheid in controleverklaring

Verantwoordingsgrens is vastgesteld op 1% van totale lasten incl. stortingen in reserves

Diverse wet- en regelgeving wordt nog geactualiseerd

Invoering rechtmatigheidsverantwoording met ingang van 2023

Vanaf dit boekjaar geeft het dagelijks bestuur de rechtmatigheidsverantwoording af voor wat betreft de financiële rechtmatigheid (het begrotingscriterium, voorwaardencriterium en misbruik en oneigenlijk gebruik) af. De rechtmatigheidsverantwoording zorgt voor meer bewustwording bij het dagelijks bestuur van haar verantwoordelijkheid voor een goed financieel beheer. De kaders en uitgangspunten voor de rechtmatigheidsverantwoording liggen enerzijds vast in wet- en regelgeving en worden anderzijds bepaald door het algemeen bestuur. Deze opzet stimuleert het dualisme waarin het algemeen bestuur een kaderstellende en controlerende rol inneemt. De rechtmatigheidsverantwoording maakt onderdeel uit van de jaarrekening. De accountant geeft een getrouwheidsoordeel af bij de jaarrekening en daarmee ook bij de rechtmatigheidsverantwoording. Dit betekent dat de accountant vanaf het boekjaar 2023 in zijn controleverklaring geen apart oordeel meer afgeeft over de rechtmatigheid. Ten aanzien van de SiSa-bijlage geeft de accountant nog wel een oordeel over de rechtmatigheid. De SiSa-bijlage wordt niet alleen een onderdeel van de rechtmatigheidsverantwoording in de jaarrekening, maar ook van de accountant wordt verwacht dat deze rapporteert over de rechtmatigheid van de SiSa-verantwoording. Dat doen wij in het accountantsverslag en in de controleverklaring bij de jaarrekening als geheel.

De totstandkoming van de rechtmatigheidsverantwoording is een proces met interactie tussen de verschillende gremia dat start bij het bepalen van de verantwoordingsgrens door het algemeen bestuur. Deze verantwoordingsgrens ligt tussen de 0% en 3% en uw algemeen bestuur heeft deze vastgesteld op 1% van de totale lasten inclusief de stortingen in de reserves. Dit is gelijk aan de wettelijke materialiteit die in het kader van de jaarrekeningcontrole over 2023 door ons wordt gehanteerd. Tevens heeft het algemeen bestuur de rapporteringsgrens voor de toelichting van de rechtmatigheidsfouten in de paragraaf bedrijfsvoering vastgesteld op 10% van de verantwoordingsgrens.

Wijzigingen wet- en regelgeving

Bij het schrijven van de managementletter zijn diverse documenten nog onderhanden, ter consultatie aangeboden of reeds gepubliceerd:

- Het Besluit accountantscontrole decentrale overheden en de aanpassing van het BBV zijn ter consultatie gepubliceerd.
- De NBA-Handreiking 1152 ‘Rechtmatigheidstoelichting decentrale overheden’ is ter consultatie gepubliceerd.
- De Kadernota rechtmatigheid van de commissie BBV is na de zomer geactualiseerd. Eind november 2023 heeft de commissie BBV een nadere toelichting gegeven over de begrotingsrechtmatigheid ten aanzien van onderschrijdingen en de definitie van het begrip ‘tijdig’.
- De notitie rechtmatigheidsverantwoording van de commissie BADO is onlangs gepubliceerd.

Vanaf het boekjaar 2023 geldt de nieuwe Kadernota rechtmatigheid. Onder andere ten aanzien van de foutenevaluatie zijn belangrijke wijzigingen doorgevoerd. In de rechtmatigheidsverantwoording worden alle afwijkingen boven de verantwoordingsgrens gerapporteerd. In de nieuwe Kadernota rechtmatigheid vallen ‘afwijkingen’ uiteen in fouten en onduidelijkheden. Onduidelijkheden doen zich voor in een situatie met complexe wet- en regelgeving, waarin de normstelling niet eenduidig uitlegbaar is. De Kadernota rechtmatigheid bevat geen mogelijkheid om afwijkingen als onzekerheid op te nemen. Daarnaast wordt in de nieuwe Kadernota rechtmatigheid nadere duiding aan het onderscheid tussen getrouwheids- en rechtmatigheidsfouten en (mogelijk) herstel van (door de VIC) geconstateerde fouten gegeven. De beslisboom in bijlage 6 van de Kadernota rechtmatigheid biedt handvatten om vast te stellen of een bevinding op een getrouwheids- of rechtmatigheidsfout toeziet.

Nadere duiding van Kadernota rechtmatigheid 2023

Nadere duiding Kadernota rechtmatigheid 2023

De commissie BBV publiceerde eind november 2023 een nadere duiding van de Kadernota rechtmatigheid 2023. Deze nadere duiding heeft betrekking op:

- Het al dan niet tijdig melden van afwijkingen van de begroting voor zowel de baten, lasten als kredieten. Wat 'niet tijdig' concreet betekent, wordt bepaald door de 'spelregels' tussen het algemeen bestuur en het dagelijks bestuur over het informeren en vaststellen van de begrotingswijzigingen bij onderschrijdingen van de lasten of investeringsbudgetten en/of lagere of hogere baten dan begroot. Deze spelregels zijn veelal in de financiële verordening art. 212 Gemeentewet opgenomen.
- Met de invoering van de rechtmatigheidsverantwoording, waarbij het toelichten en verantwoorden meer centraal staat, is het mogelijk om vóóraf afspraken te maken tussen het algemeen bestuur en het dagelijks bestuur welke begrotingsonrechtmatigheden als acceptabel worden beschouwd (wel onrechtmatig, maar acceptabel). Deze afspraken kunnen in de financiële verordening art. 212 Gemeentewet worden opgenomen.

Gezien de nadere duiding door de commissie BBV geven wij u ter overweging de financiële verordening aan te scherpen c.q. te nuanceren waar nodig. Wij vragen u voorafgaand aan de jaarrekeningcontrole 2023 een analyse op te stellen van de begrotingsrechtmatigheid waarbij bijlage 3 van de Kadernota rechtmatigheid 2023 een handreiking kan bieden.

2.1 Rechtmatigheidsverantwoording (3/4)

Proces totstandkoming rechtmatigheids-verantwoording

Proces totstandkoming rechtmatigheidsverantwoording

Hieronder hebben wij het proces van de totstandkoming van de rechtmatigheidsverantwoording in een afbeelding opgenomen.

- De ambtelijke organisatie voert de controles van het VIC-plan uit op basis van de werklijsten en legt de bevindingen vast in het VIC-verslag.
- Het dagelijks bestuur stelt de rechtmatigheidsverantwoording op, waarin de bevindingen van het VIC-verslag zijn verwerkt en waarop toelichting plaats-vindt in de paragraaf bedrijfsvoering.
- De accountant controleert of de rechtmatigheidsverantwoording getrouw is weergegeven in de jaarrekening.

- Het algemeen bestuur bepaalt de verantwoordingsgrens (1%) en rapportagegrens.
- Het algemeen bestuur stelt het normenkader vast.

- De ambtelijke organisatie stelt op basis van het VIC-plan werklijsten op.
- De ambtelijke organisatie stemt het VIC-plan én de werklijsten af met de accountant ter borging van de juistheid en volledigheid van de uitgevoerde VIC-controles.

- De ambtelijke organisatie operationaliseert het normenkader in een toetsingskader. *Dit toetsingskader ontbreekt momenteel nog.*
- De ambtelijke organisatie stelt een verbijzonderde interne controleplan (VIC-plan) op met hierin de aspecten vanuit het toetsingskader.

2.1 Rechtmatigheidsverantwoording (4/4)

Veiligheidsregio Limburg-Noord is (bijna) gereed voor rechtmatigheids-verantwoording

Belangrijke coördinerende rol ligt bij verbijzonderde interne controle

Tijdige uitvoering van werkzaamheden van verbijzonderde interne controle is van groot belang

Verdiepingsslag bij VIC op naleving van EU-aanbestedingsregels

Status voorbereidingen op rechtmatigheidsverantwoording

Binnen de organisatie is er voldoende bewustzijn over de impact van de rechtmatigheidsverantwoording op de inrichting van interne beheersingsmaatregelen in de processen. De organisatie heeft de nodige voorbereidende acties uitgevoerd en de geldende beleidskaders voor de rechtmatigheidsverantwoording voorgelegd aan het algemeen bestuur. De herziene financiële verordening is onlangs vastgesteld door het algemeen bestuur. Het controleprotocol 2023 (inclusief het normenkader) zal begin 2024 worden vastgesteld door het algemeen bestuur. Wij concluderen dat u organisatorisch (bijna) gereed bent voor de rechtmatigheidsverantwoording over het jaar 2023.

Mogelijke doorontwikkeling VIC in kader van rechtmatigheidsverantwoording

Er is een belangrijke coördinerende rol voor de verbijzonderde interne controle (VIC) weggelegd ten aanzien van de rechtmatigheids-verantwoording. Bij uw organisatie zijn de processen zo ingericht dat met name de VIC-werkzaamheden, -vastleggingen en -uitkomsten de basis zijn voor de onderbouwing van de rechtmatigheidsverantwoording. De verantwoordelijkheden voor de rechtmatigheidsverantwoording liggen echter veel breder; alle organisatieonderdelen en het voltallige dagelijks bestuur zijn hiervoor verantwoordelijk. Het toetsen op de werking van systemen of het eventueel aanvullen met gegevensgerichte werkzaamheden kan ook bij de teams zelf (eerste lijn) of in de tweede lijn worden belegd. Dan kan de VIC meer acteren als derde lijn waarbij het diens taak is de betrouwbaarheid van de informatie-voorziening van de eerste en tweede lijn te beoordelen. Er vindt dan een verschuiving plaats van ‘de VIC als onderbouwing van de recht-matigheidsverantwoording’ naar ‘de VIC als bevestiging van de getrouwheid van de rechtmatigheidsverantwoording van de verschillende teams’. Dit is een ontwikkeling die uw organisatie in de toekomst nog kan maken.

Samenwerking met VIC

De accountant maakt zo veel als mogelijk gebruik van de uitgevoerde (verbijzonderde) interne controlewerkzaamheden van de organisatie. De ambtelijke organisatie dient het normenkader in een toetsingskader te operationaliseren. Dit zichtbare toetsingskader ontbreekt nog. Een tijdige uitvoering van de werkzaamheden van de VIC is hierbij van groot belang. In het kader van een goede samenwerking hebben wij onder andere ons werkprogramma ten aanzien van de grondexploitatie met uw organisatie gedeeld.

De spendanalyse over de gehele vierjaarsperiode 2020-2023 met een interne toetsing op de naleving van de Europese aanbestedingsregels is een aandachtspunt. Hierbij dient rekening te worden gehouden met de aandachtspunten uit de notitie ‘Uitvoering van controle op aanbestedingsrechtmatigheid bij jaarrekeningcontrole van decentrale overheden’ van de NBA-SDO, in het bijzonder de bepaling van de opdrachtwaarde en de wezenlijke wijzigingen en/of ontoelaatbare overschrijdingen. Verder vragen wij uw specifieke aandacht voor de opvolging van de rechtmatigheidsfouten uit 2022 en de betrouwbaarheid van het gehanteerde lijstwerk om de volledigheid van de uitgevoerde spendanalyse te waarborgen. Noodzakelijk is om in de spendanalyse per crediteur de punten uit de SDO-notitie expliciet vast te leggen waarbij een conclusie wordt gevormd over de aanbestedingsrechtmatigheid. Aandachtspunt is dat alle toetspunten uit de SDO-notitie zichtbaar worden gecontroleerd door de VIC. Om de toetspunten zichtbaar vast te leggen conform de SDO-notitie ondersteunen wij jullie door ons intern werkprogramma (EU)-aanbestedingen te delen.

3. Interne beheersing en tussentijdse controle

3.1 Inrichting van onze controle (1/2)

Transparantie over controleaanpak

Onderkende aandachtspunten:
- Management override
- Ongeautoriseerde handelingen
- Getrouwheid rechtmatigheids-verantwoording

Inleiding

Wij vinden het van groot belang dat wij inzicht geven in de normen en verwachtingen ten aanzien van onze controle en de vertaling hiervan specifiek voor de Veiligheidsregio Limburg-Noord. In deze managementletter hebben wij daarom meer in detail uitgelegd op welke wijze wij de controle hebben ingericht en welke afwegingen wij hierbij hebben gemaakt. Wij doen dat door in deze paragraaf onze risico-inschatting, de belangrijkste processen, de controle-aanpak en de afwegingen te beschrijven.

Onze inschatting van belangrijkste aandachtspunten

In het kader van de controle van de jaarrekening 2023 en onze controle-aanpak hebben wij een inschatting van de belangrijkste aandachtspunten gemaakt. Wij zien de volgende aandachtspunten in de controle van de jaarrekening 2023 van uw veiligheidsregio:

- In onze controlestandaarden wordt expliciet het risico van management override of controls (= de bewuste beïnvloeding door het bestuur of management van de jaarcijfers) als een belangrijk aandachtspunt genoemd. Als accountant moeten wij in onze werkzaamheden specifiek aandacht hieraan besteden. Wij zijn van mening dat binnen uw organisatie de mogelijkheden om buiten de getroffen interne beheersmaatregelen invloed uit te uitoefenen op de in de jaarrekening gepresenteerde cijfers beperkt zijn. Het verrichten van een fictieve dan wel onjuiste memoriaalboeking zien wij als enige mogelijkheid en derhalve beoordelen wij de memoriaalboekingen in detail.
- Meer bevoegdheden in de financiële applicatie Unit4 Business World en de bankapplicatie van de BNG, ING en Rabobank dan noodzakelijk vanuit een functie kunnen tot ongeautoriseerde handelingen leiden. Onze focus ligt op de juiste autorisatie van de inkoopfacturen en de juiste IBAN bij de betalingen.
- Het risico dat de rechtmatigheidsverantwoording niet getrouw is gezien de Veiligheidsregio Limburg-Noord voor het eerst een rechtmatigheidsverantwoording opstelt als gevolg van een landelijke wetswijziging.

3.1 Inrichting van onze controle (2/2)

Belangrijkste processen

Onze inschatting van belangrijkste processen

In het kader van onze controle hebben wij de volgende processen onderkend:

- het memoriaalboekingenproces;
- het inkoopproces (incl. aanbestedingen);
- het personeelsproces;
- de opbrengstenprocessen;
- het proces omtrent IT-beheer.

Natuurlijk zijn er meer processen te onderkennen, ook met financiële gevolgen, waaronder de veelal kleinere (schattings)processen. Op basis van onze ervaring, de kwaliteit en omvang van de kleinere processen en om efficiency-redenen hebben wij deze processen echter niet procesmatig c.q. systeemgericht getoetst, maar voeren wij gegevensgerichte werkzaamheden uit in de vorm van cijferanalyses, verbandscontroles en steekproeven dan wel deelwaarnemingen.

Per proces toetsen wij:

- Controletechnische functiescheiding
- Interne beheers-maatregelen
- IT-beheers-maatregelen
- Verbijzonderde interne controle

Uitwerking controlestrategie per proces

Voor elk proces beoordelen wij de volgende onderdelen:

- **CTFS:** Is binnen de belangrijkste processen sprake van voldoende (controletechnische) functiescheiding?
- **AO/IB:** Is er sprake van een toereikende administratieve organisatie met toereikende beheersmaatregelen?
- **ITGC:** Zijn er in en rondom het systeem voldoende waarborgen getroffen t.a.v. de betrouwbaarheid van de gegevensverwerking?
- **VIC:** Heeft de verbijzonderde interne controle de interne beheersmaatregelen getoetst en kunnen wij hiervan gebruik maken?

Indien al deze vragen positief kunnen worden beantwoord, is de organisatie optimaal in control en kunnen ook wij gebruik maken van uw interne beheersing. De vaak tijdrovende en gedetailleerde gegevensgerichte werkzaamheden (die ook nog eens achteraf plaatsvinden), kunnen dan beperkt blijven tot een minimum. Indien wij deze vragen niet geheel positief kunnen beantwoorden en niet op uw interne beheersing kunnen steunen, betekent niet dat uw organisatie niet in control is, maar wel dat de interne beheersmaatregelen niet altijd aantoonbaar in de processen en IT-systemen zijn verankerd conform de daaraan te stellen eisen vanuit onze accountantscontrole. Het gevolg hiervan is dat wij in onze controleaanpak een overwegend gegevensgerichte aanpak zullen hanteren.

3.2 Effectiviteit processen

Voor wat betreft onze aanpak kunnen wij (nog) niet (volledig) steunen op interne beheersing; onze aanpak is hoofdzakelijk gegevensgericht

Zelfstandige betalings-bevoegdheden bij ING en Rabobank

Samenvatting van effectiviteit van processen

In het overzicht hiernaast geven wij samengevat weer in welke mate de belangrijkste processen voldoen aan de normen en verwachtingen ten aanzien van onze controle.

Op basis van onze uitgevoerde werkzaamheden komen wij momenteel tot de conclusie dat de interne beheersorganisatie van uw veiligheids-regio in de lijn (voor zover relevant voor de jaarrekeningcontrole) in opzet voldoende maar in bestaan deels niet voldoende scoort. De (controle)handelingen in de processen worden niet voldoende zichtbaar vastgelegd, waardoor achteraf niet kan worden vastgesteld of, en hoe, de (controle)handelingen zijn uitgevoerd. Deze situatie vloeit voort uit uw bewuste keuze voor de inrichting van de interne beheersing, zijnde het gebruik van soft controls in plaats van hard controls, en is hiermee ook ongewijzigd ten opzichte van voorgaand controlejaar.

Voor de werkzaamheden en conclusie ten aanzien van de algemene IT-beheersmaatregelen verwijzen wij u naar hoofdstuk 4.

Betalingsbevoegdheden bij ING en Rabobank

Inzake de rechtentoekenning binnen de bankapplicatie van de ING en de Rabobank brengen wij onder uw aandacht dat alle 4 gebruikers van de ING bankapplicatie en beide gebruikers van de Rabobank bankapplicatie een zelfstandige betalingsbevoegdheid hebben. Gezien deze rechten-toekenning verrichten wij aanvullende controlewerkzaamheden op de ‘af-mutaties’ van de ING-rekening en de Rabobank-bankrekeningen. Wij hebben de ‘af-mutaties’ op de zakelijkheid van de transacties van januari tot medio november 2023 gecontroleerd. Hierbij hebben wij geen niet-zakelijke transacties geconstateerd. Wij zullen tijdens de eindejaarscontrole de ‘af-mutaties’ van medio november tot en met december 2023 op zakelijkheid controleren.

PROCES	CTFS	AO/IB	IT	T.O.V. 2022
Bedrijfsvoering				
Memoriaalboekingen	●	●	●	→
Inkopen	●	●	●	→
Aanbestedingen	●	●	○	→
Personeel	●	●	●	→
Opbrengsten:				
- rijks en gemeentelijke bijdragen	●	●	●	→
- Covid-19 declaratie	●	●	●	→
- opbrengsten GGD	●	●	●	→
- opbrengsten brandweer	●	●	●	→
ICT / automatisering	Zie hoofdstuk 4.2 en de bijlage.			

● onvoldoende ● verbeterpunten ● voldoende

● geen waarneming ○ niet van toepassing

3.3 Bevindingen tussentijdse controle

Bevindingen naar aanleiding van tussentijdse gegevensgerichte werkzaamheden

Tussentijdse gegevensgerichte controlewerkzaamheden

Tijdens de interim-controle hebben wij naast het vaststellen van de opzet, het bestaan en/of de werking van de interne beheersing binnen de processen ook tussentijdse gegevensgerichte controlewerkzaamheden verricht. Onderstaand geven wij een korte samenvatting van de belangrijkste werkzaamheden en onze bevindingen hierbij:

- *Memoriaalboekingen*
  Wij hebben een analyse verricht op de memoriaalboekingen tot en met oktober 2023. Ten aanzien van de verrichte memoriaal-boekingen in de financiële administratie hebben wij geen ongebruikelijke memoriaalboeking(en) geconstateerd. Wij hebben wel vastgesteld dat bij de controle van een memoriaalboeking sprake is van zelfcontrole en het vierogenprincipe in de lijn ontbreekt. Uw adviseur AO/IC heeft de memoriaalboekingen groter dan € 500.000 tot en met oktober 2023 gecontroleerd en hierbij geen bijzonderheden geconstateerd.

- *Inkopen goederen en diensten*
  Gezien de omvang van de inkopen van de goederen en diensten tot en met oktober 2023 hebben wij een deelwaarneming verricht op de factuurverwerking en -betaling. Denk hierbij aan: zijn de inkoopfacturen juist in de crediteurenadministratie geregistreerd, door de juiste budgethouder geautoriseerd, op de juiste IBAN betaald en zijn de prestaties geleverd. Hierbij hebben wij enkele bijzonderheden geconstateerd die door de organisatie worden geanalyseerd.

- *Salarissen en sociale lasten*
  Wij hebben deelwaarnemingen verricht op de in-/uitdiensttredingen en de declaraties van de brandweerlieden tot en met oktober 2023. Wij hebben hierbij geen bijzonderheden geconstateerd die van materieel belang zijn voor onze jaarrekeningcontrole. De personeelsmutaties zijn juist verwerkt in de salarisadministratie en de declaraties zijn juist verwerkt in Veiligheidspaspoort.

Bij de voorbereiding van de jaarrekeningcontrole maken wij, evenals voorgaande jaren, nog afspraken over de resterende werkzaamheden, de aanpak en de hiervoor benodigde controle-informatie met uw concern controller en adviseur AO/IC.

4. IT-beheersing

4.1 IT-beheersing

Wij beoordelen betrouwbaarheid en continuïteit IT voor zover relevant voor jaarrekeningcontrole

Beoordeelde systemen:
- Unit4 Business World

Detailbevindingen IT weergegeven in bijlage A

Datalekken

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 de algemene IT-beheersmaatregelen. Wij hebben in samenwerking met onze IT-auditors deze maatregelen beoordeeld om de impact van de risico's vanuit IT te kunnen vaststellen voor die systemen en applicaties die zijn gekoppeld aan de voor ons relevante processen en posten (zie hoofdstuk 3). In dit kader hebben wij de applicatie Unit4 Business World beoordeeld.

In de volgende hoofdstukken geven wij een samenvatting van de status van de opzet en het bestaan van de door ons in het kader van de jaarrekeningcontrole onderzochte algemene IT-beheersmaatregelen in het huidige en voorgaande controlejaar. De scope van de relevante algemene IT-beheersmaatregelen wordt jaarlijks beoordeeld en kan hierdoor afwijken van de scope van het voorgaande jaar. De detailbevindingen rondom deze systemen zijn opgenomen in bijlage A.

Op het moment dat de intern getroffen algemene IT-beheersmaatregelen rondom de systemen en applicaties in scope niet (aantoonbaar) voldoende aanwezig zijn, heeft dit mogelijk invloed op de interne beheersingsmaatregelen in de applicaties en de rapportages vanuit de applicaties. De impact van de bevindingen met betrekking tot de algemene IT-beheersmaatregelen worden bij de betreffende processen behandeld.

Datalekken

In onze controle hebben wij de maatregelen rond het meldproces van datalekken, zoals vereist vanuit de Wet meldplicht datalekken, geïnventariseerd. Wij hebben vastgesteld dat u een proces heeft ingericht voor het registreren van de beveiligingsincidenten waaruit datalekken naar voren kunnen komen en de afwikkeling hiervan tot en met een (eventuele) melding bij de Autoriteit Persoonsgegevens en het informeren van de betrokkenen. Wij hebben van uw chief information security officer en functionaris gegevensbescherming vernomen dat er 28 informatieveiligheidsincidenten, waarvan geen datalekken, hebben plaatsgevonden in de periode van 1 januari 2023 tot en met 15 november 2023. Op grond van uw inschatting op een nihil risico op een privacy-inbreuk van de betrokkenen heeft u geen melding bij de Autoriteit Persoonsgegevens gedaan.

Logische toegangs-beveiliging nog deels (on)toereikend

Change management nog deels (on)toereikend

Continuïteit deels ontoereikend

Voor nadere onderbouwing van norm, bevindingen en aanbevelingen verwijzen wij naar bijlage A

PROCES	2023	2022	KORTE OMSCHRIJVING BEVINDINGEN
Logische toegangsbeveiliging			
1. Procedure indienst en autorisatiewijzigingen	🟠	🟠	Autorisatiebeheer wordt inzichtelijk vastgelegd in TOPdesk en er worden standaard rollen gebruikt. De rechtentoekenning vindt echter niet plaats op basis van de normpositie maar op basis van de kennis en ervaring van de applicatiebeheerder.
2. Procedure uitdienst	🟢	🟢	Geen bevindingen.
3. Periodieke controle op toegang en juistheid ingerichte autorisaties	🟠	🟠	Er is een controle uitgevoerd op de juistheid van het procuratieschema maar niet op alle rechten in de applicatie. Er is verder een controle uitgevoerd op de actualiteit van de gebruikersaccounts, maar hiervan zijn geen vastleggingen beschikbaar.
4. Identificatie van gebruikers voor toegang tot de applicatie	🟢	🟢	Geen bevindingen.
5. Authenticatie	🟢	🟢	Geen bevindingen.
6. Administrator- en superuser-accounts	🔴	🟠	Twee gebruikers uit de lijnorganisatie beschikken over beheerrechten. Het principe van de controletechnische functiescheiding wordt hierdoor doorbroken.
Wijzigingsbeheer			
7. Wijzigingsbeheer en gescheiden omgevingen *	🟠	○	Voor de SaaS-applicatie Unit4 Business World is het wijzigingsbeheer een gedeelde verantwoordelijkheid van zowel de softwareleverancier Unit4 als uw organisatie. O.b.v. de ISAE3402-verklaring van Unit4 blijkt dat de gebruikersorganisatie zelf verantwoordelijk is voor het testen van de wijzigingen op haar eigen omgeving. Uw organisatie neemt de wijzigingen ad hoc door maar legt de testwerkzaamheden niet aantoonbaar vast.
Continuïteit			
8. Fysieke toegangscontrole, back-up, monitoring en restoretest *	🟠	○	Continuïteitsmaatregelen zijn de verantwoordelijkheid van de softwareleverancier Unit4. Unit4 beschikt over een ISAE3402 type II-verklaring waarin de beheersmaatregelen zijn opgenomen over de back-up en restorevoorzieningen. Het is tevens niet bekend of een restoretest is uitgevoerd om vast te stellen of een werkende productie-omgeving kan worden hersteld vanaf een back-up.

** Dit punt behoeft nuancering aangezien het bestaan en de werking van maatregelen pas beoordeeld kan worden zodra de nieuwe ISAE-verklaring beschikbaar komt in 2024.*

🔴 onvoldoende 🟠 verbeterpunten 🟢 voldoende ● geen waarneming ○ niet onderzocht

4.3 Digitale Bestuurskracht (1/2)

Resultaten basisscan Digitale Bestuurskracht

Basisscan Digitale Bestuurskracht

Vanwege het toenemende belang van digitalisering hebben wij een inventarisatie gedaan naar het volwassenheidsniveau van de Digitale Bestuurskracht van uw organisatie. Deze inventarisatie maakt inzichtelijk wat het vermogen van uw organisatie is om door middel van digitalisering uw opgaven te kunnen uitvoeren en wat hierin kan worden geoptimaliseerd. Dit is geen uitgebreid onderzoek geweest, maar een inventarisatie op basis van een vragenlijst aangevuld met interviews. Dit heeft ten doel om vanuit onze natuurlijke adviesfunctie mee te denken over dit belangrijke onderwerp, onze observaties te delen, de uitkomsten in de branche te benchmarken en ervaringen te delen. Vanzelfsprekend zijn wij graag bereid met u hierover verder van gedachten te wisselen. De resultaten van de volwassenheidsscan zijn op de volgende pagina weergegeven. Hieronder hebben wij de belangrijkste observaties beknopt uitgewerkt.

Overall beeld

Op basis van bovengenoemde werkzaamheden valt het ons op dat uw organisatie druk bezig is met het onderwerp Informatievoorziening (IV). Er is een I-strategie opgesteld en diverse initiatieven ter invulling van deze strategie zijn in gang gezet. Wij onderschrijven deze ontwikkelingen en inspanningen. Punt van aandacht is de afstemming van de I-strategie en bijbehorende gevolgen in het algemeen en dagelijks bestuur. Gezien het toenemende belang en de complexiteit van het onderwerp informatievoorziening leert onze ervaring dat betrokkenheid van het algemeen en dagelijks bestuur noodzakelijk is en deze noodzaak alleen maar zal toenemen. De aansluiting tussen de organisatie, het dagelijks bestuur en het algemeen bestuur op het onderwerp Informatievoorziening, dat in alle beleidsvelden vervlochten is, is cruciaal om succesvol te zijn. Daarom adviseren wij het dagelijks en algemeen bestuur om zich hierop voor te bereiden door het onderwerp structureel terug te laten komen op de agenda en periodiek te worden bijgepraat door de chief information officer. Daarnaast adviseren wij het dagelijks en algemeen bestuur om hun huidige en toekomstige rol met betrekking tot de informatievoorziening te inventariseren, te bepalen waar eventuele bijscholing wenselijk is en hierop actie te ondernemen.

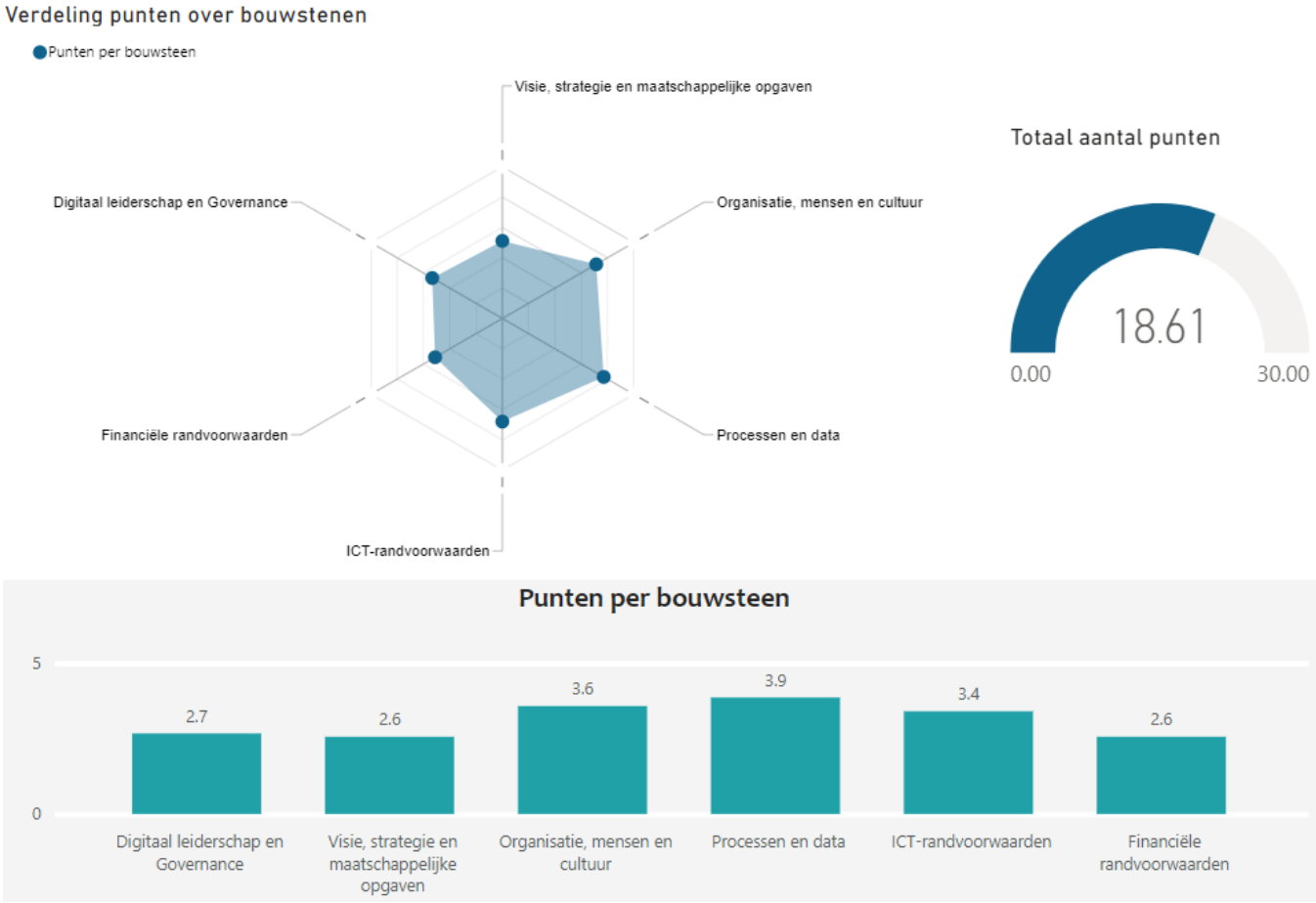
Datamanagement

Een wendbare organisatie is alleen mogelijk met de vierde bouwsteen; de basis van processen en data op orde hebben. Dit gaat verder dan het beschrijven van de processen en het inrichten van werkprocessen in de systemen. Het gaat hierbij erom dat organisaties het eigenaarschap van de processen hebben ingericht en actief gebruik maken van data om tot stuurinformatie te komen. Stuurinformatie voor de beleidsontwikkeling, die toegankelijk en begrijpelijk is voor medewerkers en bestuurders. Data-gedreven werken en data-gestuurde beleidsontwikkeling betekenen een verandering van werken in de organisatie. Wij merken op dat uw organisatie een eerste aanzet voor een data-strategie heeft beschreven, maar dit nog verder moet worden uitgewerkt en geconcretiseerd. IT wordt nog primair gebruikt voor registrerende doeleinden. De stap naar data-gedreven werken, ofwel het werken met voorspellende data ter input voor de verschillende beleidskaders, moet nog worden gezet. Wij vragen hiervoor aandacht temeer, omdat dit in de toekomst steeds belangrijker gaat worden.

4.3 Digitale Bestuurskracht (2/2)

Financiële randvoorwaarden

De bouwsteen ‘Financiële randvoorwaarden’ richt zich op de benodigde investeringen. De kosten voor de digitalisering en informatie-voorziening zullen de komende jaren alleen maar toenemen. Dat is naar onze mening een onomkeerbaar proces. De uitdaging is deze toenemende uitgaven zodanig in te zetten dat uw organisatie de voordelen van de digitalisering, de innovatie en het data-gedreven werken kan benutten. Dan is dit geen steeds hoger wordende kostenpost, maar een bewuste investering in een betere digitale sturing en beheersing van de organisatie. Wij hebben begrepen dat bij uw organisatie de huidige investeringen momenteel afdoende zijn om de informatievoorzieningsprojecten te bekostigen. Wel verwachten wij een toename van de benodigde investeringen, gelet op de razend-snelle ontwikkelingen in de markt. Daarom adviseren wij u zoveel als mogelijk de komende jaren rekening te houden met deze verwachte toename van de benodigde investeringen.



4.4 IT-ontwikkelingen (1/3)

Verhoogde aandacht voor cybersecurity bij management en toezichthouder

Ransomware kan bedrijfscontinuïteit in gevaar brengen

Veranderingen in digitale domein vragen van uw organisatie dat cybersecurity risico's periodiek worden geëvalueerd om vast te stellen of deze voldoende worden geadresseerd

Informatiebeveiliging en cybersecurity

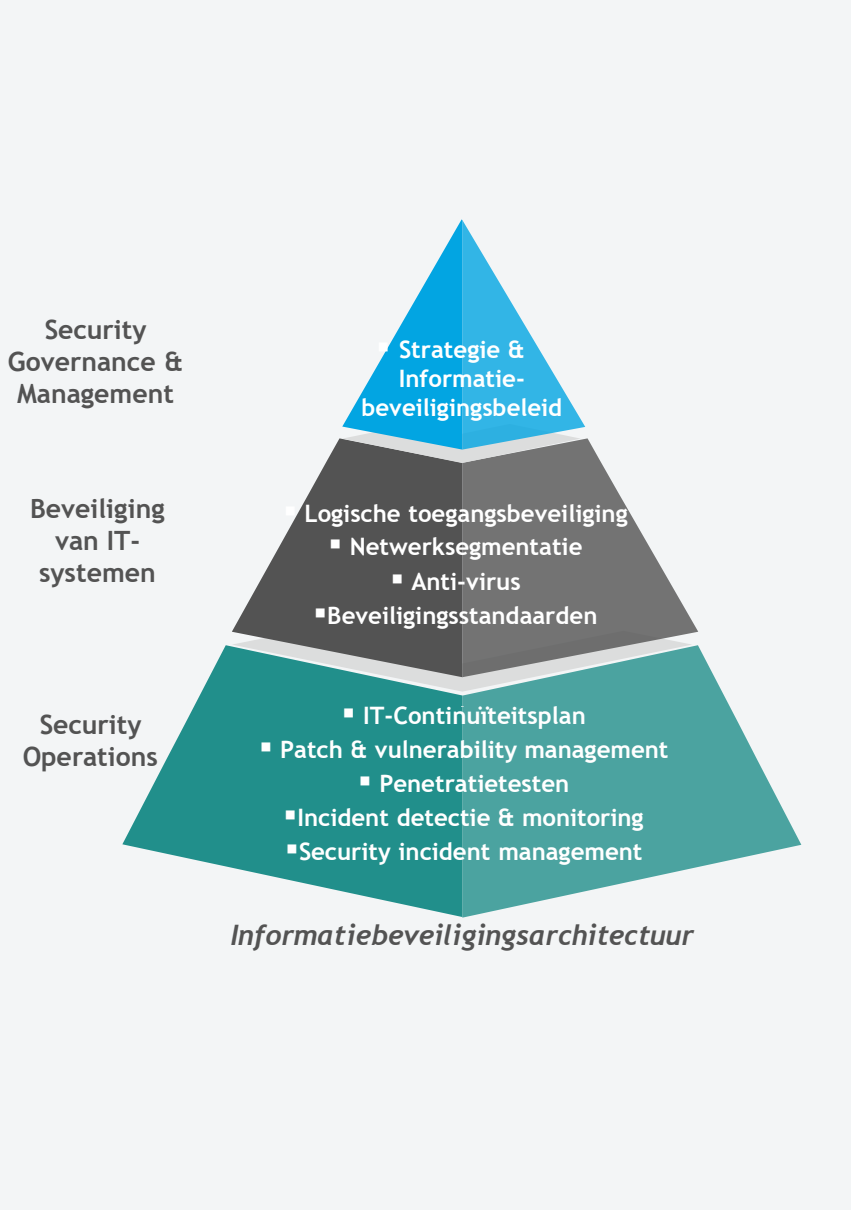
Vanuit onze natuurlijke adviesrol attenderen wij u graag op enkele ontwikkelingen op het gebied van IT. De afgelopen jaren is er meer aandacht voor cybersecurity risico's ontstaan, mede door verhoogde (media)aandacht voor cybersecurity incidenten. Deze toegenomen aandacht voor cybersecurity risico's leeft bij zowel management, toezichthouders als ook het maatschappelijk verkeer. Organisaties zijn in sterke en toenemende mate afhankelijk van de continuïteit van IT-systemen. Zelfs zodanig dat bij het uitvallen of gijzeling (via ransomware) van de IT-systemen de bedrijfscontinuïteit kan worden geraakt. Dit kan daarmee een continuïteitsrisico in het kader van de jaarrekening met zich meebrengen.

Ook kan een cybersecurity incident leiden tot ongeautoriseerde toegang tot gevoelige gegevens waardoor er niet voldaan wordt aan de privacywetgeving (AVG).

Een cybersecurity incident, een incident als gevolg van activiteiten / calamiteiten in het cyberdomein (digitale domein) kan resulteren in:

- verstoringen in bedrijfsvoering (en daarmee eventueel continuïteit);
- datalekken door ongeautoriseerde toegang tot gegevens;
- fraude (beïnvloeding/manipulatie van gegevens);
- aanzienlijke reputatieschade;
- diefstal.

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



Informatiebeveiligingsarchitectuur

4.4 IT-ontwikkelingen (2/3)

Inzicht in cybersecurity maatregelen

Op basis van onze werkzaamheden ten aanzien van cybersecurity binnen de jaarrekeningcontrole, zien wij dat uw organisatie inzicht heeft in haar kritieke IT-systemen en zich bewust is van de risico's rondom informatiebeveiliging en cybersecurity. De organisatie beschikt over een actueel informatiebeveiligingsbeleid en heeft ook een IT-continuïteitsplan opgesteld waarin de maatregelen rondom de IT-continuïteit in geval van calamiteiten zijn beschreven. Wij adviseren u het IT-continuïteitsplan jaarlijks te testen.

Uw organisatie hanteert een security incident management proces, zodat beveiligingsincidenten worden beheerst en tijdig kunnen worden opgevolgd. Voorts steekt de organisatie de nodige moeite in het vergroten van het bewustzijn van de medewerkers met betrekking tot de informatiebeveiliging middels toetsing en awareness-modules.

In 2022 heeft uw organisatie een penetratietest laten uitvoeren op de (kritieke) IT-systemen binnen het IT-landschap. Wij adviseren u na de opvolging van de bevindingen die hieruit zijn voortgekomen een nieuwe penetratietest uit te (laten) voeren om vast te stellen dat de destijds geconstateerde kwetsbaarheden thans afdoende zijn gemitigeerd.

4.4 IT-ontwikkelingen (3/3)

Kwaliteit van gegevensverwerking door derden vraagt om contractuele afspraken

Gebruik van cloud-omgeving en software as a service

IT-leveranciers bieden steeds meer oplossingen en diensten aan als software as a service. Dit betekent dat de software niet meer bij de organisatie staat, maar bij de IT-leverancier of een derde. Ook bij het werken met software as a service geldt dat uw organisatie verantwoordelijkheid draagt voor de beheersing van de kwaliteit van de gegevensverwerking in de software die bij de IT-leverancier of een derde ligt.

Dit vraagt inzicht in hoe het beheer op die systemen is geregeld en vereist duidelijke afspraken met de IT-leverancier of derde over de te leveren kwaliteit. Dit geldt ook voor de door de IT-leverancier en/of derde te treffen IT-beheers- en beveiligingsmaatregelen.

Bij uw organisatie worden in Unit4 Business World gegevens voor de jaarrekening verwerkt. Wij adviseren u met Unit4 afspraken te maken over een ISAE 3402- of SOC1-assuranceonderzoek waarmee de leverancier jaarlijks een bevestiging kan overhandigen dat de interne beheersing voldoet.

5. Vooruitblik jaarrekening 2023

5.1 Vooruitblik jaarrekening 2023

Aandachtspunten voor jaarrekeningcontrole 2023

Gemaakte afspraken voor jaarrekeningcontrole 2023

Wij hebben afgesproken om net als voorgaand jaar (ruim) voorafgaand aan de accountantscontrole een scan uit te voeren op het (digitale) jaarrekeningdossier ter beoordeling of de opgevraagde controledocumentatie is opgeleverd en een goede basis biedt voor de aanvang van onze werkzaamheden.

Wij onderkennen de volgende aandachtspunten voor de jaarrekeningcontrole 2023:

- analyse van de vastgestelde investeringskredieten versus de gerealiseerde investeringsuitgaven tot en met controlejaar 2023 (bron: bijlage investeringen begroting c.q. bestuursrapportage);
- aansluiting tussen het saldo in de onderhoudsvoorziening per 31-12-2023 en het onderliggende beheerplan (inclusief verschillenanalyse);
- berekening van de voorziening voor bovenmatige (bovenwettelijke) verlofuren respectievelijk verlofsparen per 31-12-2023;
- aanlevering van de spendanalyse over de gehele vierjaarsperiode 2020-2023 met een interne toetsing op de naleving van de Europese aanbestedingsregels. Hierbij dient rekening te worden gehouden met de aandachtspunten uit de notitie ‘Uitvoering van controle op aanbestedingsrechtmatigheid bij jaarrekeningcontrole van decentrale overheden’ van de NBA-SDO en in het bijzonder de opdrachtwaarde en de wezenlijke wijzigingen en/of ontoelaatbare overschrijdingen. Verder vragen wij uw specifieke aandacht voor de opvolging van de rechtmatigheids-fouten uit 2022 en de betrouwbaarheid van het gehanteerde lijstwerk om de volledigheid van de spendanalyse te waarborgen;
- aanlevering van de ‘tax letter’ waarin de relevante informatie rondom de fiscaliteiten (Vpb, btw en LB) wordt vermeld. Wij zullen u hiervoor de template nog aanreiken;
- aanlevering van de WNT-verantwoording en onderliggende brondocumentatie;
- aanlevering van een volledige (concept) jaarrekening welke reeds intern is getoetst op de naleving van het BBV. Wij zullen u hiervoor de checklist 2023 nog aanreiken.

Het is van belang dat uw organisatie stuurt op een tijdige realisatie van bovengenoemde afspraken. Dit komt ten goede aan de efficiëntie van het jaarrekeningproces en de jaarrekeningcontrole.

Bijlagen

A. Detailbevindingen IT-beheer

A. Detailbevindingen IT-beheer

A.1 Procedure autorisatiebeheer

Bevinding	PROCEDURE AUTORISATIEBEHEER & PERIODIEKE CONTROLE OP JUISTHEID INGERICHTE AUTORISATIES	KANS: gemiddeld
Jaar van constatering	2021-2023	IMPACT: gemiddeld

Onze bevinding	**Autorisatiebeheer** Uw organisatie maakt gebruik van standaard rollen in Unit4 Business World en het autorisatiebeheer wordt in TOPdesk vastgelegd. In het indienst ticket is zichtbaar dat een voorbeeldgebruiker wordt benoemd voor het toekennen van autorisaties. Er wordt hierbij geen gebruik gemaakt van een geformaliseerde normpositie. **Periodieke review** In 2023 heeft er een interne controle plaatsgevonden op de juistheid van het totale procuratieschema in Unit4 Business World. Dit betreft derhalve een deelcontrole en geen totaalcontrole op alle ingerichte autorisaties per gebruiker van Unit4 Business World. Er is ook een controle uitgevoerd op de actualiteit van de gebruikersaccounts, maar hiervan zijn geen vastleggingen beschikbaar.
Risico	Door het ontbreken van een adequate naleving op de gebruikersbeheerprocedures bestaat het risico dat personen teveel of onterechte rollen/rechten bezitten en hierdoor het principe van de functiescheiding mogelijk kan worden doorbroken met het risico op ongeautoriseerde handelingen.
Onze aanbeveling	Wij adviseren u een formele normpositie voor Unit4 Business World op te stellen welke applicatie-overstijgend is, zodat de belangrijkste gewenste functiescheidingsprincipes zichtbaar zijn gemaakt. Om administratieve lasten te voorkomen, raden wij u aan om hierbij voornamelijk te focussen op de belangrijkste functiescheidingen in de systemen. In navolging hiervan raden wij u aan om de normpositie jaarlijks vooraf door het management te laten goedkeuren, zodat deze organisatiebreed wordt gedragen en een juiste grondslag voor het autorisatiebeheer biedt. Aan de hand van deze normpositie dienen de verzoeken tot het aanvragen en muteren van gebruikers met rollen en rechten te worden beoordeeld alvorens deze autorisatiegroep/rechten worden toegekend. Tevens verdient het de aanbeveling om een periodieke review (bijv. halfjaarlijks of jaarlijks) uit te voeren waarin achteraf tegen de bovengenoemde normpositie wordt nagegaan of de gebruikers teveel rollen/rechten toegekend hebben gekregen. Voorts adviseren wij u om de actualiteitscontrole van de gebruikersaccounts vast te leggen.
Reactie management	De organisatie heeft geen formele normpositie voor Unit4 Business World en de organisatie van het financieel systeem is ook niet van zodanige aard om een formele normpositie op te stellen. Wij zullen periodieke fysieke controles uitvoeren welke toezien op de juistheid van de ingerichte autorisaties. Deze controles zullen wij ook laten aansluiten op de interne audits autorisatiebeheer welke door het team informatiemanagement worden uitgevoerd.

A.2 Administrator- en superuser-accounts

Bevinding	SUPERUSERS	KANS: gemiddeld
Jaar van constatering	2023	IMPACT: HOOG

Onze bevinding	In Unit4 Business World beschikken twee financiële medewerkers over beheerrechten: één functioneel beheerder en één medewerker als achtervang voor de functioneel beheerder vanuit capaciteitsoverwegingen. In opzet wordt dit gecompenseerd doordat uw organisatie controleert op ongeautoriseerde handelingen in Unit4 Business World. Doordat twee medewerkers uit de lijnorganisatie (financiële administrateur) beschikken over beheerrechten, is de functiescheiding tussen de lijnorganisatie en IT-organisatie doorbroken.
Risico	Accounts met beheerrechten bezitten alle rechten en kunnen hiermee de gewenste functiescheidingen doorbreken en eventueel ongeautoriseerde wijzigingen (bijvoorbeeld stamgegevens of financiële transacties) doorvoeren. Dit is een inherent risico van een beheeraccount. Echter wordt dit risico nog aanzienlijk verhoogd door deze accounts te beleggen in de lijnorganisatie. Tevens bestaat het risico op generiek genaamde en/of verouderde accounts waarmee ongeautoriseerde wijzigingen worden doorgevoerd waarbij op basis van de naamgeving niet is te achterhalen wie deze wijzigingen heeft doorgevoerd.
Onze aanbeveling	Wij adviseren u om een duidelijke functiescheiding aan te brengen tussen het gebruik en het (IT-)beheer van de applicatie Unit4 Business World. Dit kan bijvoorbeeld door de kritische applicatiebeheerprocessen (zoals het aanmaken, verwijderen en wijzigen van gebruikers en rechten, het wijzigen van systeeminstellingen (o.a. wachtwoordinstellingen, logginginstellingen en workflows) en het installeren van updates) te centraliseren bij de ICT-afdeling.
Reactie management	De organisatie heeft het functioneel beheer binnen de lijnorganisatie belegd. Het is voor de organisatie niet praktisch om het functioneel beheer op de benoemde processen bij de ICT-afdeling te organiseren. Wij hebben aandacht voor het benoemde risico en zullen daarom beheersmaatregelen nemen. Van alle wijzigingen door de superuser-accounts kan een loggingsbestand worden opgevraagd in Unit4 Business World. Wij zullen periodiek fysieke controles uitvoeren. Deze controles zullen worden uitgevoerd door een medewerker welk niet belast is met een superuser-account.

A.3 Wijzigingsbeheer

Bevinding	Wijzigingsbeheer updates	KANS: laag
Jaar van constatering	2023	IMPACT: laag

Onze bevinding	De verantwoordelijkheid voor het wijzigingsbeheer ligt zowel bij de softwareleverancier van Unit4 Business World als uw organisatie. Unit4 beschikt over een ISAE3402 type II-assuranceverklaring. Uw organisatie voert geen aantoonbare beoordeling uit op de assuranceverklaring van Unit4. In deze assuranceverklaring zijn zogeheten *user entity controls* opgenomen waarin wordt gesteld dat de gebruiksorganisatie zelf verantwoordelijk is voor het testen van de wijzigingen op haar eigen omgeving. Uw organisatie neemt de wijzigingen ad hoc door. maar legt geen testwerkzaamheden vast.
Risico	In algemene zin bestaat het risico dat testwerkzaamheden niet op basis van specifieke criteria vanuit de lijnorganisatie worden uitgevoerd. Hierdoor wordt mogelijk niet effectief en efficiënt getest wat ten koste kan gaan van de kwaliteit van de testwerkzaamheden en de productiviteit. Indien de testresultaten voor het in productie nemen van de wijziging niet structureel worden vastgelegd, bestaat het risico dat achteraf niet kan worden vastgesteld of een softwarewijziging terecht in de productieomgeving is geplaatst.
Onze aanbeveling	Wij raden u aan om per jaareinde de assuranceverklaring op te vragen bij de softwareleverancier Unit4 en na te gaan: • wat de scope van de assuranceverklaring betreft en of dit overeenkomt met de afgenomen diensten bij Unit4; • wat de periode van de assuranceverklaring betreft (gehele boekjaar of gedeelte van het boekjaar); • in hoeverre de controlemaatregelen rondom wijzigingsbeheer toereikend zijn; • welke aanvullende controlemaatregelen (lees: beheersmaatregelen bij de klantorganisatie) worden verwacht van uw organisatie. Wij raden u aan om bijzonderheden ten opzichte van bovengenoemde aandachtspunten te bespreken met de softwareleverancier Unit4. *Dit punt behoeft nuancering vanwege het feit dat de ISAE3402-verklaring van 2023 gepubliceerd wordt aan het begin van 2024.*
Reactie management	De organisatie heeft hiervoor aandacht en zal jaarlijks de ISAE3402 type II verklaring bij Unit4 opvragen. De benoemde bevindingen uit dit rapport zullen worden meegenomen in onze interne beheersing.

A.4 Continuïteit

Bevinding	Back-up & restore	KANS: laag
Jaar van constatering	2023	IMPACT: gemiddeld

Onze bevinding	De verantwoordelijkheid voor de continuïteitsmaatregelen ligt bij de softwareleverancier Unit4. Unit4 beschikt over een ISAE3402 type II-assuranceverklaring. Uw organisatie voert geen aantoonbare beoordeling uit op de assuranceverklaring van Unit4. Het is bij uw organisatie niet bekend of er een restoretest is uitgevoerd om vast te stellen of een werkende productie-omgeving kan worden hersteld.
Risico	Doordat er bij uw organisatie geen inzicht in de werking van de uitbestede beheersmaatregelen omtrent continuïteit is, bestaat het risico dat de uitbestede beheersmaatregelen bij de softwareleverancier Unit4 niet in lijn zijn met de vereisten vanuit uw organisatie. Wanneer de restore-testen nog niet zijn uitgevoerd, bestaat het risico dat de back-up data niet te restoren is in geval van nood. Het risico is echter beperkt vanwege het feit dat er tot op heden nog geen verstoringen hebben voorgedaan.
Onze aanbeveling	Wij raden u aan om per jaareinde de assuranceverklaring op te vragen bij de softwareleverancier Unit4 en na te gaan: • wat de scope van de assuranceverklaring betreft en of dit overeenkomt met de afgenomen diensten bij Unit4; • wat de periode van de assuranceverklaring betreft (gehele boekjaar of gedeelte van het boekjaar); • in hoeverre de controlemaatregelen rondom continuïteit toereikend zijn; • welke aanvullende controlemaatregelen (lees: beheersmaatregelen bij de klantorganisatie) worden verwacht van uw organisatie. Wij raden u aan om bijzonderheden ten opzichte van bovengenoemde aandachtspunten te bespreken met de softwareleverancier Unit4. *Dit punt behoeft nuancering vanwege het feit dat de ISAE3402-verklaring van 2023 gepubliceerd wordt aan het begin van 2024.*
Reactie management	De organisatie heeft hiervoor aandacht en zal jaarlijks de ISAE3402 type II verklaring bij Unit4 opvragen. De benoemde bevindingen uit dit rapport zullen worden meegenomen in onze interne beheersing.

bdo.nl