belastingsamenwerking
Gouwe-Rijnland

Rapportage
Verbijzonderde Interne Controle 2023

Inhoud

Managementsamenvatting

Gewijzigde wetgeving (verwachting bekrachtiging in 2024) zal ervoor zorgen dat niet de accountant maar het Dagelijks Bestuur degene wordt die verantwoording aflegt over de (financiële) rechtmatigheid van het gevoerde beleid. Dit zal het Dagelijks Bestuur doen in de vorm van een rechtmatigheidsverantwoording in de jaarrekening specifiek gericht op het begrotings-, voorwaarden-, en misbruik- en oneigenlijk gebruik criterium. De accountant zal vervolgens de rechtmatigheidsverantwoording op getrouwheid controleren. Om te kunnen komen tot een rechtmatigheidsverantwoording is het bestuur verplicht om zorg te dragen voor de toetsing van de rechtmatigheid van het financiële beheer. Deze toetsing vindt bij BSGR plaats middels een verbijzonderde interne controle op de bedrijfsprocessen binnen BSGR. Bij de interne controle op de processen is voor 2023 gekozen voor een risicogerichte aanpak op basis van opgestelde risico-controlematrices per proces. Per jaareinde is tevens in het kader van risicobeheersing een frauderisicoanalyse uitgevoerd. Hierbij wordt per significant proces beoordeeld of de geïdentificeerde frauderisico's voldoende worden gemitigeerd door de aanwezige beheersmaatregelen. De fraude risico's vormen een onderdeel van de risico-controlematrices.

In deze rapportage wordt gerapporteerd over de belangrijkste bevindingen inzake de verbijzonderde interne controle (VIC) over 2023 en de uitkomsten uit de frauderisicoanalyse. Deze bevindingen hebben een adviserend karakter, zodat in overweging kan worden genomen of deze maatregelen van belang zijn om het proces verder in control te brengen of te houden. De adviespunten in deze rapportage zijn gebaseerd op zowel interviews (opzet) met medewerkers als geraadpleegde documentatie (bestaan/ werking).

Om de verdeling van taken en verantwoordelijkheden binnen de organisatie voldoende ingericht te hebben hanteert BSGR het "Three Lines of Defence-Model". Dit model maakt gebruik van 3 verdedigingslinies om de risico's binnen de processen in beeld te brengen en beheersbaar te houden. De "three lines" bestaan uit het lijnmanagement, team financiën en control. De verbijzonderde interne controle werkzaamheden zijn uitgevoerd door de controller in samenspraak met lijnmanagement.

Aan hand van de uitgevoerde werkzaamheden op de significante processen is een beoordeling van het risico per proces tot stand gekomen. Het risico per proces wordt gemeten door de kans en impact van de significante risico's per proces te evalueren. De risicobeoordeling geeft aan in welke mate de bestaande beheersingsmaatregelen de significante risico's per proces mitigeren. De werkzaamheden zijn uitgevoerd op twee momenten (interim en jaareinde) en hebben geleid tot de volgende risicobeoordelingen per proces:

Proces	Risicobeoordeling (interim)	Risicobeoordeling (jaareinde)
Personeel	Laag	Voldoende
Inkopen	Voldoende	Voldoende
(Europese) aanbestedingen	Voldoende	Voldoende
Betalingsverkeer	Laag	Laag
Afsluitprocedures & totstandkoming begroting	Voldoende	Voldoende
Treasury	Uitvoering jaareinde	Voldoende
IT omgeving	Voldoende	Voldoende

Hoog	Ruim onvoldoende beheersing van risico's Maatregelen direct vereist en monitoring door verantwoordelijke proceseigenaar
Medium	Onvoldoende beheersing van risico's Maatregelen vereist en monitoring door verantwoordelijke proceseigenaar
Voldoende	Voldoende beheersing van risico's Maatregelen overwegen (niet noodzakelijk) en monitoring door verantwoordelijke proceseigenaar wel nodig
Laag	Ruim voldoende beheersing van risico's Maatregelen niet noodzakelijk en reguliere monitoring door verantwoordelijke proceseigenaar wel nodig

Uit de werkzaamheden is naar voren gekomen dat er geen bevindingen zijn die de financiële rapporteringstoleranties overschrijden. De gerapporteerde bevindingen en aanbevelingen zijn voornamelijk gericht op procesverbeteringen en hebben geen materiële financiële impact. In het hoofdstuk “uitvoering” wordt een nadere toelichting gegeven op de detailbevindingen per proces.

Scope

Binnen de BSGR worden twee financiële hoofdstromen onderscheiden. Dit betreft enerzijds de eigen bedrijfsvoering waarover verantwoording wordt afgelegd in de reguliere P&C documenten. Anderzijds betreft dit de belastingopbrengsten waarover verantwoording wordt afgelegd in de belastingrapportage. De VIC werkzaamheden concentreren zich op de verantwoording over de eigen bedrijfsvoering.
De belastingprocessen omtrent het heffen en innen van de belastingen ten behoeve van deelnemers worden separaat getoetst door de IT auditor Audit Connect. Hiervan wordt verslag gedaan in de vorm van de ISAE type II rapportage.

Risicobeheersing BSGR

Jaarlijks worden de risico's binnen BSGR geëvalueerd door de controller en hoofd bedrijfsvoering. Hierbij worden per proces de risico's geïdentificeerd waarbij de kans en mogelijke impact is uitgewerkt in een risico-controle matrix. Belangrijke risicocategorieën hierin zijn de geïdentificeerde frauderisico's en de significante risico's per proces. Op basis van de identificatie van de risico's zijn de beheersmaatregelen gedefinieerd die de risico's zouden moeten mitigeren (de zogenaamde bruto benadering).
Uit de evaluatie kunnen ook onderwerpen extra aandacht krijgen buiten de borging van de reguliere processen. Dit zullen voornamelijk onderwerpen zijn waarvoor in beginsel een meer dan normaal risico geldt voor het borgen van de getrouwheid en rechtmatigheid van daarmee samenhangende baten, lasten en balansmutaties. Processen die een meer dan normaal risico hebben of die qua omvang materieel zijn, worden niet gerouleerd maar jaarlijks getoetst. Daarnaast kunnen ook onderwerpen die bestuurlijk relevant zijn extra aandacht krijgen.

VIC processen

Op basis van de begroting/ realisatie en de significante risico's bepalen we de materiële transactiestromen binnen BSGR. Hierbij is rekening gehouden met de baten, lasten en balansmutaties. Aan hand van deze beoordeling zijn de significante processen geïdentificeerd. In het lopende boekjaar zal op basis van de uitgevoerde werkzaamheden nagegaan worden of bijstelling van de scope benodigd is. Onderstaand geeft de significante processen weer inclusief de timing van de uit te voeren werkzaamheden:

Proces	**Timing**
Personeel	Interim periode & Jaareinde
Inkopen	Interim periode & Jaareinde
(Europese) aanbestedingen	Interim periode & Jaareinde
Betalingsverkeer	Interim periode & Jaareinde
Afsluitprocedures & totstandkoming begroting	Interim periode & Jaareinde
Treasury	Uitvoering jaareinde
IT omgeving	Interim periode & Jaareinde

Controle- en rapporteringstoleranties

Controletolerantie

De controletolerantie is het maximale bedrag dat de som van fouten in de jaarrekening of onzekerheden in de controle aangeeft, zonder dat de bruikbaarheid van de jaarrekening voor de oordeelsvorming door de gebruikers kan worden beïnvloed. De Nota van toelichting bij het Besluit Accountantscontrole Decentrale Overheden (BADO) bepaalt dat de minimumeisen voor de goedkeuringstolerantie ten aanzien van fouten in de jaarrekening 1% van de totale lasten na toevoegingen reserves bedraagt en ten aanzien van onzekerheden in de controle 3% van de totale lasten na toevoegingen reserves. Het gaat om de grenswaarde waar beneden de in aanmerking te nemen fouten (< 1 %) of onzekerheden (< 3 %) moet blijven om een goedkeurende controleverklaring te kunnen krijgen. Onderstaand geeft schematisch de toleranties weer:

Minimumeisen t.b.v. strekking controleverklaring				
Goedkeuringstolerantie	Goedkeurend	Beperking	Oordeelonthouding	Afkeurend
Fouten in de jaarrekening (% lasten)	≤ 1%	> 1% - < 3%	-	≥ 3%
Onzekerheden in de controle (% lasten)	≤ 3%	> 3%< 10%	≥ 10%	-
Benoeming fouten		Van materieel belang	Van wezenlijk belang	

Processen c.q. deelprocessen die een totaal aan transacties genereren die op jaarbasis op of boven deze controletolerantie uitkomen zijn dus kwantitatief materieel voor de uitvoering van de VIC controlewerkzaamheden en worden ook als zodanig behandeld in de uit te voeren werkzaamheden.

Verantwoordingsgrens

De verantwoordingsgrens voor bevindingen vanuit de VIC werkzaamheden volgt de toleranties zoals opgenomen in het controleprotocol/ normenkader en is bepaald op 1% van de totale lasten van BSGR, inclusief de toevoegingen aan de reserves. Als het totaal van de afwijkingen van fouten/ onzekerheden boven deze grens uitkomt dan moet het bestuur een overzicht van de afwijkingen opnemen in de rechtmatigheidsverantwoording. Fouten en onzekerheden mogen niet bij elkaar opgeteld worden.

Rapporteringtoleranties

Het bestuur heeft een rapporteringstolerantie waarboven zij individuele fouten of onzekerheden gerapporteerd wil krijgen voortkomend uit de VIC werkzaamheden (conform het controleprotocol/ normenkader). Voor de rapporteringstolerantie stelt het bestuur als maatstaf dat elke fout of onzekerheid ≥ 10% van de goedkeuringstolerantie wordt gerapporteerd. Alle bevindingen die boven deze tolerantie uitkomen zullen worden vermeld in de periodieke rapportage aan het bestuur. Tevens zullen de bevindingen worden gerapporteerd die kunnen leiden tot procesverbeteringen.

Uitvoering

De werkzaamheden zijn uitgevoerd op twee momenten (interim en jaareinde). In de onderstaande rapportering van de VIC werkzaamheden is onderscheid gemaakt tussen de interim bevindingen per proces met daarin de opvolging per jaareinde en de bevindingen naar aanleiding van de werkzaamheden per jaareinde.

Opvolging interim bevindingen

Proces	Bevindingen interim rapportage dd 9 november 2023	Aanbeveling	Opvolging per jaareinde	Risicobeoordeling
Inkopen	Het mandaatbesluit dient te worden geactualiseerd naar aanleiding van de nieuwe functie van afdelingshoofd bedrijfsvoering;	Wij bevelen u aan om het mandaatbesluit te updaten naar de actuele situatie.	In 2024 zal het mandaatbesluit aangepast worden naar de actuele situatie.	Voldoende
Inkopen	De verplichtingen worden geregistreerd in de applicatie Elvy, momenteel ontbreekt een aansluiting met het contractenregister.	Wij bevelen u aan om te onderzoeken of de contracten kunnen worden geregistreerd in Elvy, waarbij een aansluiting gemaakt kan worden met de opgenomen verplichtingen.	In 2024 zal het registreren van contracten en de koppeling aan verplichtingen in Elvy onderzocht worden.	Voldoende
Inkopen	De verplichtingen per kostenplaats per afdeling zijn niet opgenomen in maandrapportages, waardoor de afdelingshoofden niet het volledig overzicht hebben over de bestedingen.	Wij bevelen u aan om de verplichtingen per kostenplaats per afdelingen inzichtelijk te maken.	In 2024 zal de procedure omtrent het uitsplitsen van verplichtingen nader onderzocht worden.	Voldoende
Inkopen	Uit de deelwaarneming is geconstateerd dat voor een aantal geselecteerde inkopen, waarbij een verplichting verwacht wordt, deze verplichting niet is opgenomen in Elvy.	Wij bevelen u aan om richtlijnen op te stellen voor het opnemen van verplichtingen.	In 2024 zal de procedure omtrent de verwerking van verplichtingen nader worden uitgewerkt.	Voldoende
Personeel	Wij hebben geconstateerd dat geen zichtbare controle heeft plaatsgevonden op de gehanteerde premiepercentages per begin van het jaar.	Wij adviseren om bruto-netto berekeningen in januari uit te voeren om de gehanteerde premies percentages zichtbaar te toetsen	Per 2024 worden bruto-netto berekeningen uitgevoerd tbv controle op juiste premiepercentages.	Voldoende
Memoriaal boekingen	Up-to-date maken van de procedurebeschrijvingen inzake memoriaalboekingen.	Wij bevelen u aan om de procedures omtrent memoriaalboeking te updaten.	Naar aanleiding van de bevinding is de procedure verder aangescherpt.	laag
Memoriaal boekingen	Controle op juiste verwerking van memoriaalboekingen middels vier-ogen principe ontbreekt.	Wij bevelen aan om de verantwoordelijkheid van de uitvoering en controle op memoriaal boekingen bij twee verschillende functionarissen te beleggen, zodat de juiste/ tijdige en volledige verwerking van de memoriaalboekingen is geborgd.	Naar aanleiding van de bevinding is de procedure gewijzigd, waarbij bij elke memoriaalboeking zichtbaar het 4-ogen principe wordt gehanteerd.	laag
		Wij bevelen aan om te onderzoeken of voor de memoriaal boekingen inzake afschrijvingen materiële vaste activa, gebruik kan worden gemaakt van geautomatiseerde verwerking in Exact (MVA-module).	In 2024 zal hier nader onderzoek naar plaatsvinden.	Voldoende
Memoriaal boekingen	Onderbouwingen van de memoriaalboekingen worden momenteel niet integraal opgeslagen op een centrale locatie.	Wij bevelen u aan om duidelijke afspraken te maken welke onderbouwingen van de memoriaal boekingen worden opgeslagen en welke locatie hiervoor wordt gehanteerd.	Naar aanleiding van de bevinding is de procedure verder aangescherpt.	laag
Automatisering (wijzigingsbeheer)	Nieuwe releases worden uitgevoerd door de leverancier van de applicatie (in 2023 enkel releases van Elvy). De release vindt ten eerste plaats in de test omgeving. Voordat de nieuwe release wordt doorgevoerd naar productie vindt geen formele afstemming plaats met de gebruiker (BSGR).	Wij bevelen u aan om in overleg te gaan met softwareleverancier Elvy, met als doel het formaliseren van de procedures omtrent het doorvoeren van nieuwe releases naar productie. Hierin is met name van de belang de afstemming tussen Elvy en applicatiebeheer/ verantwoordelijke afdelingen bij het doorvoeren van nieuwe releases (afstemming testplan en testwerkzaamheden).	Naar aanleiding van de bevinding is de procedure aangescherpt en vindt bij nieuwe releases formele afstemming plaats tussen beheerder en BSGR.	laag

Bevindingen jaareinde procedures

Inkopen & aanbestedingen

De rechtmatigheid van inkopen binnen BSGR kan alleen worden aangetoond indien de onderliggende onderbouwing van de geleverde prestatie aanwezig is. Deze onderbouwing bestaat uit bijvoorbeeld een urenstaat bij geleverde diensten of opleverdocumentatie. Een inkoop wordt als onrechtmatig gekwalificeerd indien deze onderbouwingen ontbreken. Daarnaast wordt op een aantal andere onderdelen getoetst.

Jaareinde werkzaamheden

Voor het proces inkopen & aanbestedingen heeft een controle plaatsgevonden op de volgende sub-processen:

- Inkopen zijnde inkomende facturen (12 facturen geselecteerd),
- Mutatie stamgegevens (2 mutaties geselecteerd),
- Aanbestedingen; per jaareinde controle hebben alleen enkelvoudige aanbestedingen plaatsgevonden, onderbouwende documentatie inzake de enkelvoudige aanbestedingen zijn beoordeeld in het reguliere proces van inkopen.
- Maandelijkse bewaking van de voortgang van bestaande (Europese) aanbestedingen aan de hand van de crediteurenscan (crediteurenscan per jaareinde geselecteerd).

Bevindingen

Met betrekking tot de procedures omtrent inkopen & aanbestedingen hebben wij de volgende bevindingen:

- Uit de deelwaarneming is geconstateerd dat voor een aantal geselecteerde inkopen, waarbij een verplichting verwacht wordt, deze verplichting niet is opgenomen in Elvy.
- Uit de deelwaarneming is voor 1 Europees aanbestede dienst een overbesteding geconstateerd ten opzichte van de contractuele voorwaarden. Rekening houdend met toegestane afwijking van 10% van de waarde ten opzichte van de oorspronkelijke opdracht resteert een onrechtmatige dienst ad EUR 10K. BSGR was hiervan op de hoogte en heeft dit tevens gemeld. De afwijking is ontstaan door in rekening gebracht meerwerk.

Aanbevelingen

Naar aanleiding van de werkzaamheden per jaareinde, hebben wij de volgende aanbevelingen:

- In overeenstemming met de bevinding vanuit de interim controle bevelen wij u aan om richtlijnen op te stellen voor het opnemen van verplichtingen.

Risicobeoordeling proces per Jaareinde controle

Voldoende	Voldoende beheersing van risico's Maatregelen overwegen (niet noodzakelijk) en monitoring door verantwoordelijke proceseigenaar wel nodig

Personeel

De salarisadministratie wordt uitgevoerd door een externe partij ADP. De afdeling P&O voert de interne controles uit op de juistheid en tijdigheid van de mutaties zoals verwerkt in de salarisadministratie.

Jaareinde werkzaamheden

Voor het proces personeel heeft een controle plaatsgevonden op de volgende sub-processen:

- personeel in dienst tredende medewerker (1 dossier geselecteerd),
- personeel uit dienst tredende medewerker (1 dossier geselecteerd),
- mutaties inzake stamgegevens SA (1 maand geselecteerd),
- Overige salarismutaties waaronder declaraties, ouderschapsverlof.

Bevindingen

Met betrekking tot de procedures omtrent personeel hebben wij de volgende bevindingen:

- We hebben vastgesteld dat voor personeel de werkbeschrijvingen geactualiseerd dienen te worden.
- Mutaties die niet in ADP rechtstreeks worden verwerkt (bijvoorbeeld ouderschapsverlof) moeten worden opgenomen in de checklist “mutatie salarisgegevens” en worden voorzien van een vier-ogenprincipe.
- Controle op mutaties stamgegevens salarissen (indienst, uitdienst en overig) wordt beoordeeld op basis van de salarisstroken en niet op basis van een mutatieverslag vanuit de salarisverwerker.
- Voortgang inzake onboarding van vaste medewerkers wordt momenteel niet bewaakt in een standenregister veroorzaakt door krappe bezetting op de afdeling. Per 1 januari 2024 is deze procedure weer opgepakt en zal worden getoetst in de VIC 2024.
- Vastgesteld is dat voor de deelwaarneming indienst en uitdienst de checklisten nog niet volledig zijn afgewerkt (zichtbare controle).

Aanbevelingen

Naar aanleiding van de werkzaamheden per jaareinde, hebben wij de volgende aanbevelingen:

- Wij adviseren de werkbeschrijvingen inzake personeel te actualiseren.
- Wij adviseren u om de personeelsmutaties welke niet rechtstreeks worden verwerkt in ADP op te nemen in de controle checklist “mutatie salarisgegevens” en te voorzien van een vier-ogenprincipe.
- Wij adviseren u om te onderzoeken of controle op mutatie stamgegevens salarissen middels een mutatieverslag vanuit ADP kan worden uitgevoerd.
- Wij adviseren u de status van de indienst en uitdienst procedures tijdig af te wikkelen in de aanwezige checklists.

Risicobeoordeling proces per interim controle

Voldoende	Voldoende beheersing van risico's Maatregelen overwegen (niet noodzakelijk) en monitoring door verantwoordelijke proceseigenaar wel nodig

Betalingsverkeer

De reguliere en incidentele betalingen worden wekelijks uitgevoerd. Voor het reguliere betalingsproces wordt in belangrijke mate gesteund op de geautomatiseerde gegevensverwerking. Indien sprake is van handmatige betalingen worden deze onderbouwd met onderliggende specificaties, waarbij verwerking handmatig wordt toegevoegd in de bankieromgeving. De salarisbetalingen worden maandelijks uitgevoerd, waarbij tevens in hoge mate wordt gesteund op de geautomatiseerde gegevensverwerking.

Jaareinde werkzaamheden

Voor het proces betalingsverkeer heeft een controle plaatsgevonden op de volgende sub-processen:

- Betaling van inkomende facturen (reguliere betalingen van 2 weken geselecteerd)
- Betaling van salarissen (salarisbetaling van 1 maand geselecteerd)
- Incidentele (handmatige) betalingen (incidentele betaling van 3 weken geselecteerd)

Bevindingen

Wij hebben aan de hand van de uitgevoerde deelwaarneming geen tekortkomingen vastgesteld in de procedures omtrent reguliere-, incidentele- en salarisbetalingen.

Aanbevelingen

Geen aanbevelingen geconstateerd

Risicobeoordeling proces per interim controle

Laag	Ruim voldoende beheersing van risico's Maatregelen niet noodzakelijk en reguliere monitoring door verantwoordelijke proceseigenaar wel nodig

Afsluitprocedures per jaareinde

De afsluitprocedures omvatten onder andere de werkzaamheden ten aanzien de maandrapportages, memoriaalboekingen en schattingsposten. Memoriaalboekingen worden uitgevoerd door de administrateur voor een aantal elementen: inboeken van afschrijvingslasten MVA, salaris gerelateerde items (loonheffing, pensioenpremies etc.), overlopende posten en eventuele correcties.

Jaareinde werkzaamheden

Voor de afsluitprocedures heeft een controle plaatsgevonden op de volgende sub-processen:

- Financiële maandrapportages (2 items geselecteerd)
- Memoriaalboekingen (selectie van 2 items opgesplitst naar de diverse soorten memoriaalboekingen geselecteerd).

Bevindingen

Met betrekking tot de afsluitprocedures hebben wij de volgende bevindingen:

- De procedures (zichtbare controle momenten) omtrent de afsluiting per maandeinde zijn momenteel nog niet voldoende vastgelegd.

Aanbevelingen

Naar aanleiding van de werkzaamheden per jaareinde, hebben wij de volgende aanbevelingen:

- Wij bevelen u aan om de processtappen ten aanzien van de maandafsluitingen zichtbaar weer te geven, waarbij een duidelijke relatie wordt gelegd met de controle momenten.

Risicobeoordeling proces per interim controle

Voldoende	Voldoende beheersing van risico's Maatregelen overwegen (niet noodzakelijk) en monitoring door verantwoordelijke proceseigenaar wel nodig

Treasury

De BSGR heeft een treasurybeleid opgesteld waarin de uitgangspunten, doelstellingen, richtlijnen en voorwaarden zijn opgenomen voor de uitvoering van de treasury functie. In algemene zin zal het financiële beleid bij dienen te dragen en ondersteuning te bieden aan het uitvoeren van de taken van de gemeenschappelijke regeling. Meer specifiek zal de continuïteit van de gemeenschappelijke regeling op korte en lange termijn gewaarborgd dienen te worden. Per jaareinde is het treasury beleid beoordeeld aan de hand van de wet- en regelgeving en interne richtlijnen (treasury statuut). De treasury werkzaamheden omvatten tevens de procedures omtrent deelnemersbijdragen.

Bevindingen

Met betrekking tot de procedures omtrent treasury hebben wij de volgende bevindingen:

- Wij hebben geconstateerd dat een gestructureerd overzicht ontbreekt van de toekomstige inkomsten en uitgaven ingedeeld naar aard en tijdseenheid.

Aanbevelingen

Wij adviseren u om inzicht te verkrijgen in de toekomstige geldstromen middels het opstellen van een liquiditeitsprognose en deze periodiek te bespreken in het MT.

Voldoende	Voldoende beheersing van risico's Maatregelen overwegen (niet noodzakelijk) en monitoring door verantwoordelijke proceseigenaar wel nodig

Automatisering

BSGR maakt ten behoeve van de kantooradministratie gebruik van een aantal systemen, namelijk:

- Elvy ten behoeve van de autorisatie van facturen
- Exact Globe ten behoeve van de financiële administratie
- ADP ten behoeve van de personeelsadministratie

Het beheer van de IT infrastructuur is ondergebracht bij KPN. De migratie naar KPN vanuit Centric SMC is in twee fasen uitgevoerd namelijk de migratie van de kantoorautomatisering (uitgevoerd in december 2022) en de migratie van de IT infrastructuur van Centric naar KPN (medio maart 2023).

Logische toegangsbeveiliging Elvy en Exact Globe

Voor de financiële administratie wordt gebruik gemaakt van de webapplicaties Elvy en Exact Globe.

Jaareinde werkzaamheden logische toegangsbeveiliging

Ten aanzien van exact globe is sprake van een single sign on. Voor Elvy Web vindt seperate inlog plaats. Voor logische toegangsbeveiliging heeft een controle plaatsgevonden op de procedures omtrent logische toegang voor de systemen Elvy en Exact.

Bevindingen

Wij hebben aan de hand van de uitgevoerde deelwaarneming geen tekortkomingen vastgesteld in de procedures omtrent logische toegangsbeveiliging.

Aanbevelingen

Geen aanbevelingen geconstateerd

Laag	Ruim voldoende beheersing van risico's Maatregelen niet noodzakelijk en reguliere monitoring door verantwoordelijke proceseigenaar wel nodig

Wijzigingsbeheer Elvy en Exact Globe

Wijzigingenbeheer heeft als doel dat wijzigingen op een beheerste wijze worden vastgelegd, geëvalueerd, geautoriseerd, getest en geïmplementeerd. De kwaliteit van wijzigingenbeheer vormt daarmee een belangrijke randvoorwaarde om een betrouwbare gegevensverwerking te realiseren.

Nieuwe releases van de leveranciers (Elvy & Exact Globe) worden beoordeeld op de noodzaak van doorvoeren. Indien een nieuwe release wordt doorgevoerd, wordt deze eerst in een testomgeving uitgevoerd en vervolgens doorgeleid naar productie.

Bevindingen

Met betrekking tot de procedures omtrent wijzigingsbeheer hebben wij de volgende bevindingen:

- Aan de hand van de uitgevoerde werkzaamheden is geconstateerd dat de reeds uit dienst getreden controller nog is opgenomen in de actieve gebruikers accounts van exact.
- Aan de hand van de uitgevoerde werkzaamheden is geconstateerd dat het wijzigingsbeheer van Elvy web momenteel is belegd bij de controller.

Aanbevelingen

Met betrekking tot de procedures omtrent wijzigingsbeheer hebben wij de volgende bevindingen:

- Wij adviseren u om periodieke afstemming te maken tussen de controller/ hoofd bedrijfsvoering en de ICT coördinator inzake de actieve gebruikers in Elvy en Exact. Het risico van de aanwezigheid van de reeds uit dienst getreden controller in de gebruikersaccounts is gemitigeerd doordat het daaraan gekoppelde netwerkaccount reeds inactief was bij uitdiensttreding.
- Wij adviseren u om het wijzigingsbeheer van Elvy web onder te brengen bij de ICT coördinator.

Voldoende	Voldoende beheersing van risico's Maatregelen overwegen (niet noodzakelijk) en monitoring door verantwoordelijke proceseigenaar wel nodig

Continuïteit Elvy en Exact Globe

De back-up en recovery procedures zijn belegd bij de externe partij KPN. Dagelijks wordt een back-up gemaakt van de bij BSGR in gebruik zijnde applicaties (elke dag een back-up, archive-log files worden elk kwartier weggeschreven). De back-ups worden opgeslagen bij twee fysiek gescheiden datacenters. De procedures omtrent back-up en recovery vormen een onderdeel van de ISAE 3402 type II werkzaamheden. Voor eventuele bevindingen verwijzen wij naar de rapportage inzake ISAE 3402 type II.

Automatisering ADP

ADP heeft een ISAE 3402 type II verklaring waarop na beoordeling gesteund kan worden in het kader van logische toegangsbeveiliging, wijzigingsbeheer en continuïteit van het systeem.

Uitwerking frauderisicoanalyse

In dit hoofdstuk is een beknopte toelichting opgenomen van de frauderisicoanalyse die is uitgevoerd. Frauderisicoanalyse is één van de preventieve elementen binnen het frauderisicomanagementmodel. De frauderisicoanalyse dient ter identificatie van bestaande frauderisico's binnen de verschillende processen. Het onderkennen van een frauderisico betekent niet dat dit risico zich daadwerkelijk manifesteert in de praktijk. Dit is een belangrijk onderscheid tussen een frauderisico en een fraude-incident.

Definitie frauderisico's

In iedere organisatie zijn factoren aanwezig die het plegen van fraude kunnen veroorzaken.

De aanwezigheid van deze zogenoemde frauderisicofactoren kan leiden tot frauderisico's. Het al dan niet identificeren van een frauderisico hangt af van organisatie-specifieke omstandigheden. Bij het identificeren van de frauderisico's op basis van de geïdentificeerde frauderisicofactoren wordt in eerste instantie geen rekening gehouden met de opzet, bestaan en werking van interne beheersingsmaatregelen. Wanneer interne beheersingsmaatregelen namelijk relevant zijn voor de mitigatie van het frauderisico, dient bijzondere aandacht te worden besteed aan de opzet, bestaan en werking van dit deel van de interne beheersing. De interne beheersing kan leiden tot het mitigeren van een frauderisico, echter dient men zich ervan bewust te zijn dat het frauderisico daarmee niet (geheel) verdwijnt.

Gehanteerde definitie van fraude

"een opzettelijke handeling door een of meer leden van het management, met governance belaste personen, werknemers of derden, waarbij gebruik wordt gemaakt van misleiding teneinde een onrechtmatig of onwettig voordeel te verkrijgen".

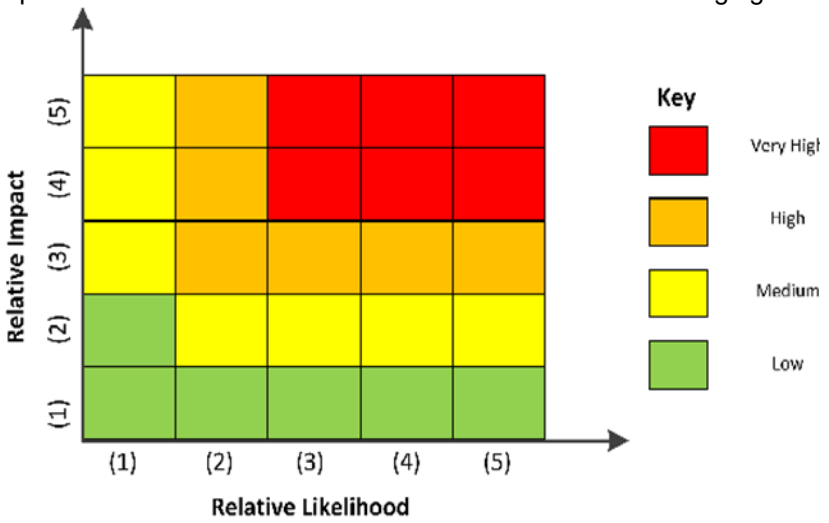
Categorieën van fraude

In hoofdlijnen kan fraude in drie categorieën worden verdeeld, deze categorieën sluiten elkaar niet uit:

- oneigenlijke toe-eigening van activa: het stelen of misbruiken van middelen (bijv. geldmiddelen, voorraden of andere activa) van de organisatie;
- frauduleuze financiële verslaggeving: het manipuleren van bedragen of toelichtingen in de financiële overzichten om de gebruikers van de financiële overzichten te misleiden; en
- corruptie: dit heeft met name betrekking op omkoping en belangenverstrengeling, waarbij BSGR (financieel) wordt benadeeld.

Initiële frauderisicoanalyse per proces

De BSGR heeft een initiële frauderisicoanalyse opgezet en zal naar aanleiding van de eerste resultaten in de toekomst verdere verfijning kunnen aanbrengen. Deze verfijning zal voortkomen uit nadere procesaudits dan wel onderzoeken gericht op specifieke items. De uitkomsten hiervan zullen mogelijk impact hebben op de onderkende en te onderkennen frauderisico's en afwegingen rondom kans-maal-impact (zoals opgenomen in onderstaande tabel)



Onderstaand geeft de frauderisicoanalyse weer per proces met daarin opgenomen de initiële kans-impact analyse en de eventuele bevindingen. Uit de analyse volgt een uiteindelijke risico-beoordeling.

Fraude en integriteitsrisico's

nr	Proces	Beschrijving	Kans	Impact	Procedure	Bevindingen	Risico beoordeling
1	Personeel	In de personeels- en salarisadministratie zijn personen opgenomen die niet in dienst zijn.	Onwaarschijnlijk	Medium	Maandelijkse controle door de P&O Coördinator op volledigheid van het aantal medewerkers middels een aansluiting van de medewerkers in het HR systeem met de aanwezige netwerkaccounts.	Wij hebben vastgesteld dat de aansluiting van personeelsleden uit het HR systeem momenteel niet worden aangesloten met de aanwezige netwerkaccounts	Laag
2	Personeel	Frauduleus (te hoge) salarissen, persoonele toeslagen en/of (bijzondere) beloningen in de salarisadministratie worden opgenomen/niet worden beeïndigd en worden uitbetaald	Mogelijk	Laag	Maandelijks controleert de P&O- coördinator op juiste en volledige verwerking van alle mutaties aan de hand van checklist en standenregister. De procedure vormt een onderdeel van de VIC werkzaamheden	Zie bevindingen personeel (hoofdstuk Uitvoering)	Medium
3	Personeel	Frauduleuze declaraties worden ingediend (bv. niet gemaakte kosten, privé-uitgaven of reeds gedeclareerde kosten worden gedeclareerd).	Mogelijk	Laag	Er geldt een vier-ogenprincipe inzake gedeclareerde kosten. Gedeclareerde kosten dienen in het salarispakket ADP te worden ingevoerd door de medewerker, waarbij een goedkeuring is vereist van de leidinggevende. De procedure vormt een onderdeel van de VIC werkzaamheden	Geen	Laag
1	Inkopen	Belangenverstrengeling (Onvoldoende functiescheiding in het inkoopproces bestelling, budgethouder, prestatielevering)	Mogelijk	Medium	Ingekomen facturen worden ingescand in Elvy en geregistreerd door de administrateur op de juiste kostenplaats. De verantwoordelijke budgethouder controleert en accordeert de factuur in Elvy inclusief inkooporder (volgens mandaat).	Wij hebben vastgesteld dat er geen jaarlijkse inventarisatie plaatsvindt op de MVA	Laag
2	Inkopen	Openstaande crediteurenposities worden frauduleus (gedeeltelijk) afgeboekt (bv. terugvorderingen).	Mogelijk	Medium	Periodiek beoordeelt de controller de memoriaal boekingen middels een uitdraai van alle memoriaalboekingen (controle op afwijkende beschrijvingen, bedragen, periodiciteit)	Geen	Laag
3	Inkopen	Het verrichten van privé inkopen	Mogelijk	Laag	Alle betalingsopdrachten worden geaccordeerd door twee bevoegde personen. Achter elke betaling dient een onderbouwing aanwezig te zijn. De procedure vormt een onderdeel van de VIC werkzaamheden	Geen	Laag
4	Inkopen	Accorderen van facturen zonder de geleverde prestaties	Mogelijk	Laag	De controller beoordeelt periodiek de resultaten/ afwijkingen (actual vs budget) en bespreekt dit in het MT. Tevens worden alle binnengekomen facturen opgenomen in het registratiesysteem Elvy ter goedkeuring van de afdelingshoofden. De facturen dienen voorzien te zijn van een inkooporder/ contract. De procedure vormt een onderdeel van de VIC werkzaamheden	Geen	Laag
5	Inkopen	Bewust afwijken van lokale/ interne regelgeving	Mogelijk	Laag	Om te voldoen aan wet en regelgeling wordt door de controller jaarlijks het normenkader en aanpassingen in de BBV beooordeeld. Het normenkader wordt in het bestuur geaccordeerd.	Geen	Laag
6	Inkopen	Foutieve/ Ongeautoriseerde aanpassingen van crediteuren stamgegevens	Mogelijk	Medium	Mutatie stamgegevens worden verwerkt door de administrateur obv onderbouwende stukken, controle/akkoord van de mutatie vindt plaats door controller. De procedure vormt een onderdeel van de VIC werkzaamheden	Geen	Laag

Fraude en integriteitsrisico's

nr	*Proces*	*Beschrijving*	*Kans*	*Impact*	*Procedure*	*Bevindingen*	*Risico beoordeling*
1	Aanbesteding	Samenspanning bij inkoopcontract/ (europese) aanbesteding (bv. opdrachtgunning aan bekenden, tegen te hoge prijzen)	Onwaarschijnlijk	Zeer hoog	In 2023 hebben geen Europese aanbestedingen plaatsgevonden, waardoor voor 2023 geen audit procedures zijn uitgevoerd inzake europese aanbestedingen.	NVT	NVT
2	Aanbesteding	Bewust afwijken van EU aanbestedingsregels, bijv. door het versnipperen van opdrachten.	Onwaarschijnlijk	Hoog	De controller stelt periodiek een crediteurenscan op, waarin alle uitgaven aan crediteuren van de afgelopen vier jaar worden meegenomen. De resultaten (uitnutting tov contractwaarde) worden beoordeeld door de controller op juiste hantering van de aanbestedingsrichtlijnen. bespreking van de scan vindt plaats in het MT.	Geen	Laag
3	Aanbesteding	Eigen bevoordeling bij aanbestedingsprocedure (valse/te hoge facturen frauduleus worden ingediend, geaccordeerd en uitbetaald)	Onwaarschijnlijk	Medium	Aanbestede diensten dienen te worden goedgekeurd door zowel budgethouder als directie	Geen	Laag
1	Betaalverkeer	Handmatige betalingen zonder autorisatie cf mandaatregeling en/of ontbreken van onderbouwende stukken	Mogelijk	Medium	Incidentele betalingen worden klaargezet in de bankapplicatie door de administrateur. De tekeningsbevoegden (twee accorderingen cf mandatering) controleren de betaling adhv onderbouwende documetatie voorafgaand aan accordering	Geen	Laag
2	Betaalverkeer	Betaalbatches kunnen na autorisatie van bevoegden aangepast worden	Mogelijk	Zeer Hoog	De geaccordeerde adviеslijst wordt door de administrateur ingelezen in de bankapplicatie en na inlezing in de bankapllicatie gecontroleerd door de controller. Het betalingsvoorstel in de bankapplicatie wordt door de tekeningsbevoegden (twee accorderingen cf. mandatering) gecontroleerd op hashtotals voorafgaand aan accordering van betaling.	Geen	Laag
1	Afsluitproces	Beïnvloeden van begrotingsposten ter voorkoming van onrechtmatigheden	Mogelijk	Medium	Overschrijdingen tov begrotingen worden gesignaleerd door de controller in de maandrapportage. Eventuele overschrijdingen worden gemitigeerd door voorstellen van begrotingswijzigingen (drie maal per jaar opgesteld door de controller). Bestuur accordeert deze wijzigingen.	Geen	Laag
2	Afsluitproces	Beïnvloeding van het management betreffende de financiële verantwoording	Mogelijk	Medium	De controller beoordeelt periodiek de afwijkingen van uitgaven tov budget middels een rapportage. De resultaten worden besproken in het MT. De directie legt op twee momementen in het jaar financiële verantwoording af aan het bestuur.	Geen	Laag
3	Afsluitproces	Handmatige boekingen zijn verwerkt ter sturing van de financiële verantwoording	Mogelijk	Medium	Memoriaal boekingen worden ingevoerd door de administrateur en gecontroleerd door de controller. Periodiek worden in het MT de cijfers besproken inclusief analyse op afwijkingen.	Geen	Laag

Fraude en integriteitsrisico's								
nr	***Proces***	***Beschrijving***	***Kans***	***Impact***	***Procedure***	***Bevindingen***	***Risico beoordeling***
2	Treasury	Bewust afwijken van de regelgeving zoals opgenomen in het treasury statuut	Onwaarschijnlijk	Laag	De controller beoordeelt periodiek de afwijkingen van uitgaven tov budget middels een rapportage. De resultaten worden besproken in het MT. De directie legt op twee momementen in het jaar financiële verantwoording af aan het bestuur.	Geen	Laag
1	IT omgeving	Het risico dat fysieke vertrouwelijke (persoons)gegevens frauduleus worden gebruikt of verstrekt (bv. bedrijfskritische gegevens, beleid, contractgegevens of andere gegevens relevant voor derden).	Mogelijk	Hoog	De BSGR beschikt over gedragsregels rondom integriteit, het verstrekken van gegevens (Besluit gegevensverstrekking), wettelijke plicht van geheimhouding en eedaflegging (ambtenarenwet 2017). Tevens zijn de bedrijfskritische gegevens en contractgegevens enkel toegankelijk voor de daartoe bevoegde personen.	Geen	Laag
2	IT omgeving	Het risico dat digitale vertrouwelijke (persoons)gegevens frauduleus worden gebruikt of verstrekt.	Mogelijk	Medium	De BSGR beschikt over gedragsregels rondom integriteit, het verstrekken van gegevens (Besluit gegevensverstrekking), wettelijke plicht van geheimhouding en eedaflegging (ambtenarenwet 2017)	Geen	Laag
1	Algemeen	Niet handelen in overeenstemming met de interrne gedragscodes BSGR	Mogelijk	Medium	Gedragscode integriteit BSGR & Regeling melden vermoeden misstand en inbreuk op Unierecht zijn beschikbaar voor medewerkers	Geen	Laag