

Assurance-rapport

Van de onafhankelijke accountant

Servicepunt71

Boekjaar 2021

29 maart 2022

Servicepunt71
t.a.v. mevrouw K. Kensen
Postbus 171
2300 AD LEIDEN

Referentie: 2203-13863

Betreft: Assurance-rapport 2021

Geachte mevrouw Kensen,

In het kader van onze opdracht om een assurance-rapport uit te brengen bij de beheersactiviteiten die Servicepunt71 uitvoert ten behoeve van de deelnemende klantorganisaties, brengen wij u hierbij verslag uit omtrent onze bevindingen naar aanleiding van de toetsing van de realisatie van beheersdoelstellingen in relatie tot bedrijfsvoeringsprocessen van Servicepunt71.

Onze bevindingen vloeien voort uit ons onderzoek naar de opzet, het bestaan en de werking van de AO/IB in relatie tot de beheersdoelstellingen die in de interne controleplannen per bedrijfsvoeringsproces zijn geformuleerd. Dit onderzoek is gericht op het vaststellen of de door Servicepunt71 geformuleerde "key controls" zoals opgenomen in het control framework (CFW) 2021 in opzet borgen dat gegevens en informatie uit processen rechtmatig, volledig, juist en tijdig tot stand komen, feitelijk bestaan en effectief werken. Indien nodig zijn aanvullende gegevensgerichte controlewerkzaamheden uitgevoerd om een redelijke mate van zekerheid te verkrijgen over de beheersdoelstellingen.

De rapportage is uitsluitend bedoeld voor Servicepunt71 en de deelnemende klantorganisaties en hun accountants om een oordeel te kunnen vormen over de opzet, het bestaan en de werking van de AO/IB.

Onze rapportage mag niet zonder onze voorafgaande schriftelijke toestemming onder anderen dan de genoemde gebruikersgroep verspreid worden.

Wij bedanken de medewerkers van Servicepunt71 voor de open en constructieve samenwerking bij het verrichten van onze controlewerkzaamheden en de totstandkoming van onze rapportage.

Tot het verstrekken van nadere toelichting zijn wij graag bereid.

Met vriendelijke groet,

Baker Tilly (Netherlands) N.V.

drs. S. (Stefan) Turenhout RA
Director Audit

Den Haag, 29 maart 2022

Inhouds- opgave

1. Management samenvatting	4
2. Doel en reikwijdte opdracht	9
3. Ons oordeel	14
4. Bevindingen per proces	16

Bijlagen:

Bijlage 1: Uitgebreide omschrijving key controls	41
--	----

1. Management samenvatting

1. Management samenvatting

1.1 Onze opdracht

Wij hebben tijdens het onderzoek, conform de overeengekomen opdracht, werkzaamheden verricht ter beoordeling van de opzet, het bestaan en de werking van de key controls in de bedrijfsvoeringsprocessen die Servicepunt71 uitvoert ten behoeve van de eigen organisatie en de deelnemende klantorganisaties. Het doel van het onderzoek is het verschaffen van een redelijke mate van zekerheid dat de door Servicepunt71 geformuleerde beheersdoelstellingen per proces worden gerealiseerd.

In lijn met de uitkomsten uit de managementletter 2021 van 15 oktober 2021, betekent dat dat wij in sommige gevallen aanvullende gegevensgerichte werkzaamheden hebben moeten verrichten.

Het control framework (CFW) 2021 – en daarmee de scope van de opdracht – is grotendeels gelijk gebleven ten opzichte van dat uit 2020. Op enkele tekstuele wijzigingen na, zijn er geen wijzigingen doorgevoerd. Een vijftal processen staat in 2021 centraal: Rekeningschema Decade, Crediteurenbeheer, Betalingsverkeer, Purchase2Pay (P2P) en Personele lasten.

Voor het proces Bevoegdheden Decade geldt, net als in 2020, dat dit niet meer als separaat proces in het CFW is opgenomen, maar onderdeel uitmaakt van het IT-gedeelte. Ten aanzien van het proces P2P geldt dat wij in dit controlejaar géén (gegevensgerichte) werkzaamheden uitvoeren met betrekking tot de prestatielevering. In afwijking van 2019 en 2020, zullen deze werkzaamheden volledig door de individuele accountants van de klantorganisaties worden uitgevoerd. Onze werkzaamheden zijn beperkt tot het beoordelen van de opzet en het bestaan van de betreffende key control. Dit betekent dus ook dat wij géén zekerheid verschaffen op dit punt.

1.2 Opbouw van ons rapport

In dit rapport doen wij enerzijds een uitspraak over de opzet en het bestaan van maatregelen, in lijn met de uitkomsten van onze werkzaamheden die hebben geleid tot de managementletter 2021. Anderzijds doen wij een uitspraak over de effectieve werking van maatregelen dan wel over de uitkomsten van door ons aanvullend uitgevoerde gegevensgerichte werkzaamheden met betrekking tot het gehele jaar. Voorgaande leidt tot een eindoordeel in hoeverre de beheersdoelstellingen zijn gerealiseerd.

Over de door ons uitgevoerde vervolgwerkzaamheden na het uitbrengen van de managementletter 2021, hebben wij u en de controllers en accountants van de deelnemende klantorganisaties geïnformeerd tijdens de bespreking van de managementletter op 21 oktober 2021.

1.3 Belangrijkste bevindingen processen

In de managementletter 2021 hebben wij per proces onze bevindingen gerapporteerd en hebben wij diverse aanbevelingen geformuleerd.

Door middel van de figuur op de volgende pagina hebben wij inzichtelijk gemaakt wat ons (overall) eindoordeel per proces is en wat de aard is geweest van de controleaanpak die we hebben gevolgd om tot dit oordeel te komen. Hieruit blijkt dat - ondanks het aantal en de aard van de bevindingen in de managementletter 2021 - ons eindoordeel positief is, op basis van een voornamelijk gemengde (systeem- en gegevensgericht) controleaanpak. Tegelijkertijd geeft dit aan dat er nog ruimte is voor verbetering ten aanzien van de interne beheersing.

Proces	Controleaanpak			Overall eindoordeel
Rekeningschema Decade				✓
Crediteurenbeheer				✓
Betalingsverkeer				✓
Purchase 2 Pay				✓
Personele lasten				✓
	←	Systeemgericht	Gegevensgericht	→

Interne beheersing op niveau voor Betalingsverkeer en Personeelslasten

In de managementletter 2021 hebben wij gerapporteerd dat de kwaliteit van de interne beheersing van de processen Betalingsverkeer en Personele lasten een constant en toereikend niveau heeft bereikt. Onze werkzaamheden met betrekking tot het tweede halfjaar 2021 bevestigen dit beeld voor heel 2021.

Voor beide processen hebben wij een vrijwel volledige systeemgerichte aanpak kunnen volgen.

Aandacht voor Rekeningschema Decade en Crediteurenbeheer

De bevindingen ten aanzien van Rekeningschema Decade en Crediteurenbeheer zoals gerapporteerd in de managementletter 2021 zijn niet nieuw, in de zin dat deze ook in 2020 (en eventueel in 2019) zijn gerapporteerd. De door ons gesignaleerde verbeterpunten die van belang zijn om het niveau van interne beheersing in beide processen te versterken en daarmee een systeemgerichte controle mogelijk te maken, zijn vrijwel gelijk aan de verbeterpunten die wij in 2020 hebben gerapporteerd.

Servicepunt71 heeft besloten om onze aanbevelingen op dit vlak niet op te volgen, omdat zij het restrisico verwaarloosbaar acht. Net als in 2020 heeft de uitvoering van de controlewerkzaamheden 2021 daarom hoofdzakelijk een gegevensgericht karakter.

Eindoordeel Purchase 2 Pay uitsluitend op basis van data-analyse

Als gevolg van ontoereikende algemene IT-beheersmaatregelen die ten grondslag liggen aan geautomatiseerde beheersmaatregelen in de applicatie Proquro, hebben wij ook in 2021 ons eindoordeel voor het proces P2P gebaseerd op de uitkomsten van de door ons verrichte data-analyse. Wij merken expliciet op dat in dit eindoordeel géén uitspraak is verweven over de prestatielevering van inkopen, daar wij conform afspraak met Servicepunt71 over 2021 geen test- en / of gegevensgerichte werkzaamheden hebben verricht met betrekking tot dit aspect.

1.4 Belangrijkste bevindingen general IT controls en rapportages

Gedurende 2021 heeft Servicepunt71 een eigen normenkader geïmplementeerd. Ten aanzien van de IT General Controls hebben wij vastgesteld dat de organisatie de verwachte beheersing nog niet voor alle applicaties in scope van de IT audit heeft geïmplementeerd. Voor een deel van de normen gerelateerd aan de IT General Controls resulteert dit in de conclusie 'Verbetering(en) gewenst'.

Verder hebben wij door middel van data analyse vastgesteld in hoeverre facturen binnen de workflow in Proquro volgens het 4-ogen principe afgehandeld worden. Hierin zijn twee uitzonderingsstromen noemenswaardig. Enerzijds is er een "papieren" factuurafhandeling die vervolgens alleen administratief verwerkt wordt in Proquro, waardoor wij niet kunnen vaststellen of voor deze facturen het 4-ogen principe gehanteerd is. Ten aanzien van deze stroom geven wij daarom geen oordeel. Anderzijds is er een groeiende stroom facturen die gekoppeld is aan een order, het 4-ogen principe op deze facturen wordt mede geborgd door de goedkeuring van de order.

Ten aanzien van de betrouwbaarheid van de Cognos rapportages geldt dat wij hebben vastgesteld dat er een aansluiting is tussen de geselecteerde rapportages en de onderliggende brondata per einde boekjaar. Uitzonderingen zijn opgenomen in de betreffende sectie van deze rapportage.

1.5 Vooruitblik boekjaar 2022

Dit assurance-rapport vormt het sluitstuk van de controle in het kader van de assurance-opdracht met betrekking tot boekjaar 2021. In het voorjaar van 2022 zullen de eerste stappen worden gezet richting de controle over boekjaar 2022.

In dit licht willen wij graag benadrukken dat Servicepunt71 in 2021 wederom stappen heeft gezet om tot een beheerste bedrijfsvoering ten behoeve van de deelnemende klantorganisaties te komen. De inspanningen die tot op heden door Servicepunt71 zijn verricht om de (beheersing van de) bedrijfsvoering naar een hoger niveau te tillen worden bevestigd door de uitkomsten van onze werkzaamheden. Dit komt met name tot uitdrukking in de uitkomsten ten aanzien van Betalingsverkeer en Personele lasten en de stappen die zijn gezet om tot een eigen normenkader voor IT General Controls te komen.

Dat neemt niet weg dat er nog ruimte voor verbetering is ten einde tot een situatie te komen waarin de interne beheersing in de basis betrouwbaar is voor alle processen in scope van de assurance-opdracht. Tegelijkertijd zijn we ons ervan bewust dat Servicepunt71 hierbij de balans moet bewaken tussen enerzijds doorontwikkeling en vernieuwing van processen en anderzijds 'de basis op orde' houden. De bevindingen en aanbevelingen uit onze managementletter 2021 alsook de uitkomsten van dit assurance-rapport, vormen een goed uitgangspunt voor het doorvoeren van verbeteringen in de bedrijfsvoering. Met het oog op de beoogde introductie van een nieuwe financiële applicatie, zijn wij van mening dat de focus van Servicepunt71 in eerste instantie uit dient te gaan naar een betrouwbare (IT-)beheersing in en rondom deze nieuwe financiële applicatie.

Ervan uitgaande dat het gerealiseerde niveau van interne beheersing bij de processen Betalingsverkeer en Personele lasten in 2022 gehandhaafd blijft, zal vanuit controleperspectief de belangrijkste vraag zijn in hoeverre met betrekking tot boekjaar 2022 de systeemgerichte werkzaamheden met betrekking tot de processen Rekeningschema Decade en Crediteurenbeheer geïntensiveerd kunnen worden..

Onze verwachting is dat de controleaanpak voor deze processen in 2022 nagenoeg gelijk zal zijn aan die van 2021, aangezien Servicepunt71 reeds heeft aangegeven onze aanbevelingen op dit vlak niet op te volgen, omdat zij het restrisico verwaarloosbaar acht

1.6 Resumé

De controle over boekjaar 2021 is met een positief eindoordeel afgerond. Hiertoe hebben wij van een voornamelijk gemengde (systeem- en gegevensgericht) controleaanpak gebruik gemaakt. Aandachtspunten die wij vanuit onze werkzaamheden signaleren zijn met name gelegen in de processen Rekeningschema Decade en Crediteurenbeheer.

Gelet op de controle over boekjaar 2021, is ons streven om hierbij een zo veel mogelijk systeemgerichte aanpak te volgen. Dat vraagt van Servicepunt71 de nodige inspanningen om haar interne beheersing naar een hoger niveau te tillen. Wij vertrouwen erop dat wij u met onze managementletter 2021 en met voorliggend assurance-rapport hiervoor van de nodige input hebben voorzien en wij zijn uiteraard bereid om vanuit onze natuurlijke adviesfunctie verder hierover met u in gesprek te gaan.

2. Doel en reikwijdte opdracht

2. Doel en reikwijdte opdracht

2.1 Opdracht

Aan de hand van de opdrachtbrief d.d. 25 juni 2021 heeft u ons opdracht gegeven om een assurance-rapport uit te brengen bij de beheersactiviteiten die Servicepunt71 in 2021 uitvoert ten behoeve van de deelnemende klantorganisaties.

In het kader van deze opdracht toetsen wij de opzet, het bestaan en de werking van de beheersmaatregelen (specifiek: de key controls) in de bedrijfsvoeringsprocessen.

De volgende processen die Servicepunt71 uitvoert ten behoeve van de deelnemende klantorganisaties over het jaar 2021 vallen binnen de scope van onze opdracht:

- | | |
|--------------------------|-----------------------|
| 1. Rekeningschema Decade | 4. Purchase2Pay (P2P) |
| 2. Crediteurenbeheer | 5. Personele lasten |
| 3. Betalingsverkeer | |

De scope van de opdracht 2021 is nagenoeg gelijk aan de opdracht 2020. De enige uitzondering hierop vormt het aspect prestatielevering, binnen het proces P2P. Met Servicepunt71 is afgesproken dat de (gegevensgerichte) werkzaamheden met betrekking tot de prestatielevering dit jaar in z'n geheel worden uitgevoerd door de individuele accountants van de klantorganisaties. De uitkomsten hieruit vallen daardoor niet onder de strekking van de assurance rapportage.

Wij verrichten alleen werkzaamheden met betrekking tot de opzet en het bestaan van de betreffende key control. Bij de inherente beperkingen is dit ook aangegeven.

Voor de processen in scope wordt gebruik gemaakt van de applicaties:

1. Decade: financiële administratie
2. Beaufort: personeelssysteem
3. Youforce: selfservice portaal voor personeelsaangelegenheden
4. TIM: tijdschrijven
5. Proquro: procurement en contractmanagement

Het beoordelen van de effectiviteit van de general IT controls (GITC) voor deze applicaties en de in de applicaties opgenomen application controls die samenhangen met de processen (voor zo ver dit van toepassing is), maakt eveneens onderdeel uit van deze opdracht. Net als vorig jaar, behoort het vaststellen van de betrouwbaarheid van een vooraf afgebakende set van rapporten uit business intelligence (BI) tool Cognos tot de scope van de opdracht.

2.2 Terugblik

Wij zijn in mei 2021 gestart met de opdracht door het voeren van startgesprekken met de proceseigenaren en de begeleiders vanuit team AO/IC. Het doel van deze gesprekken was het verkrijgen van inzicht in de opzet van de processen en eventuele aandachtspunten naar aanleiding van de verbijzonderde interne controle.

Het voorlopige CFW 2021 hebben wij op 16 juni 2021 van Servicepunt71 ontvangen. Op 21 juni 2021 heeft het accountants- en controllersoverleg plaats gevonden. Naar aanleiding van dit overleg zijn geen aanpassingen doorgevoerd in het CFW. Tijdens dit overleg hebben wij de voorlopige controle-aanpak gepresenteerd, waarbij reeds rekening is gehouden met zowel systeem- als gegevensgerichte werkzaamheden.

In juni en juli 2021 hebben wij de van team AO/IC ontvangen lijncontroles beoordeeld en besproken. Voor sommige key controls hebben wij in overleg met de proceseigenaren aanvullende controle-informatie vergaard om het bestaan van de key controls vast te stellen. Begin juli 2021 zijn wij gestart met het maken van selecties, om vervolgens de werking van de maatregelen over het eerste halfjaar 2021 te controleren. In sommige gevallen zijn gegevensgerichte werkzaamheden uitgevoerd, ook deze (en de uitkomsten ervan) hebben betrekking op het eerste halfjaar 2021.

Op basis van voorgaande is de managementletter in het kader van deze assurance-opdracht tot stand gekomen. De definitieve managementletter is op 15 oktober 2021 aangeboden aan Servicepunt71. Op 21 oktober 2021 hebben wij deze toegelicht aan de controllers en accountants van de diverse organisaties. Daarbij is ook in gegaan op de nog te verrichten systeem- en gegevensgerichte werkzaamheden met betrekking tot het tweede halfjaar 2021. Dit assurance-rapport is op basis daarvan tot stand gekomen.

2.3 Normenkader

Servicepunt71 stelt jaarlijks een algemeen controleplan (ACP) op dat als kaderstellend werkdocument geldt voor de uitvoering van de verbijzonderde interne controle (VIC). Het ACP 2021 dateert van 16 februari 2021.

Per proces wordt voorts een interne controleplan (ICP) opgesteld. In de ICP's zijn key controls geformuleerd die moeten borgen dat risico's op het gebied van rechtmatigheid, volledigheid, juistheid en tijdigheid gemitigeerd worden ten einde de beheersdoelstellingen te behalen. De beheersdoelstellingen zijn tevens in de ICP's opgenomen.

De geformuleerde key controls zijn centraal opgenomen in het CFW 2021 en gerelateerd aan de bijbehorende beheersdoelstellingen. Hieruit blijkt derhalve de opzet van de key controls. Bij het vaststellen van het bestaan toetsen wij of de key controls in de praktijk bestaan zoals deze in opzet zijn omschreven in het CFW. Bij het vaststellen van de werking toetsen wij of de key controls gedurende het hele jaar effectief hebben gewerkt.

2.4 Inherente beperkingen onderzoek

Ten aanzien van onze werkzaamheden in het kader van ons onderzoek en de uitkomsten daarvan, geldt een aantal inherente beperkingen. Deze vloeien primair voort uit het feit dat Servicepunt71 afhankelijk is van de deelnemende klantorganisaties voor de processen die zij voor hen uitvoert. Het betreffen de volgende inherente beperkingen:

- Wij verstrekken geen zekerheid over de volledigheid en juistheid van de opbrengsten van de deelnemende klantorganisaties, zoals deze door Servicepunt71 administratief zijn verwerkt;
- Wij verstrekken geen zekerheid over de volledigheid van mutaties die zijn aangeleverd door de deelnemende klantorganisaties (personele mutaties, memoriaalboekingen, begrotings-/kredietwijzigingen, leningen, betaalbatches uit subadministraties etc.);
- Het proces tijdschrijven valt, voor het deel dat bij de deelnemende klantorganisaties plaatsvindt, buiten de scope van de opdracht;
- Wij verschaffen geen zekerheid over de aanbestedingsrechtmatigheid van verrichte inkopen;
- Met betrekking tot de beheersdoelstelling 'Conformiteit aan externe wet- en regelgeving alsook interne regelgeving/beleid' bij het proces P2P verschaffen wij geen zekerheid over de beoordeling van de prestatielevering. Onze werkzaamheden ten aanzien van de betreffende key control zijn uitsluitend gericht op het beoordelen van de opzet en het bestaan van dit deel van het proces;

- De factuurstroom 'factuur compleet' maakt geen onderdeel uit van de uitgevoerde data-analyse bij het proces P2P. Wij verstrekken dus geen zekerheid over de toepassing van het vier-ogenprincipe bij deze stroom;
- Eventuele beheersmaatregelen die betrekking hebben op bedrijfsrisico's worden slechts in formele zin beoordeeld, er wordt geen oordeel in materiële zin gegeven;
- Bij de selectie van proceduretests wordt in acht genomen dat de selectie representatief is voor de gehele controleperiode en dat de massa alle deelnemende klantorganisaties vertegenwoordigt.

2.5 Verantwoordelijkheden Servicepunt71

De verantwoordelijkheid van Servicepunt71 strekt zich uit tot het opzetten, implementeren en effectief laten werken van beheersmaatregelen die verband houden met de beheersdoelstellingen. Deze beheersdoelstellingen zijn beperkt tot de processen binnen de scope van deze opdracht (zie paragraaf 2.1).

2.6 Verantwoordelijkheden van de accountant van Servicepunt71

Onze verantwoordelijkheid als accountant van Servicepunt71 strekt zich uit tot het - op basis van de door ons verrichte werkzaamheden - geven van een oordeel over de opzet, het bestaan en werking van beheersmaatregelen in relatie tot de beheersdoelstellingen van de bedrijfsvoeringsprocessen die Servicepunt71 uitvoert ten behoeve van de deelnemende klantorganisaties.

Wij hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder Standaard 3000D, "Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie (directe opdrachten)". Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of, in alle van

materieel belang zijnde aspecten, de beheersmaatregelen op afdoende wijze zijn opgezet en effectief werken ten einde de daarmee verband houdende beheersdoelstellingen te realiseren.

Een assurance-opdracht om te rapporteren over de opzet, het bestaan en de werking van beheersmaatregelen bij Servicepunt71 omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet, het bestaan en de werking van beheersmaatregelen in de bedrijfsvoeringsprocessen.

Onze werkzaamheden omvatten het toetsen van de werking van die beheersmaatregelen dan wel het verrichten van (aanvullende) gegevensgerichte werkzaamheden, zoals wij noodzakelijk achten bij het verschaffen van een redelijke mate van zekerheid dat de beheersdoelstellingen worden bereikt.

Wij zijn onafhankelijk van Servicepunt71 zoals vereist in de Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten (ViO) en andere voor de opdracht relevante onafhankelijkheidsregels in Nederland. Verder hebben wij voldaan aan de Verordening gedrags- en beroepsregels accountants (VGBA). Wij passen de Nadere voorschriften accountantskantoren ter zake van assurance-opdrachten (RA/AA) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van ethische voorschriften, accountantsstandaarden en andere relevante wet- en regelgeving.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel te bieden.

2.7 Assurance-rapport

Dit assurance-rapport is gebaseerd op de uitkomsten van de verrichte werkzaamheden in het kader van ons onderzoek.

Het doel van onze werkzaamheden is het vaststellen of Servicepunt71 de risico's ten aanzien van de bedrijfsvoeringsprocessen die zij uitvoert voor deelnemende klantorganisaties voldoende beheerst.

Het onderzoek omvat het verkrijgen van inzicht in de wijze waarop processen en daarin verankerde beheersmaatregelen (key controls) zijn opgezet, het beoordelen of dit op afdoende wijze is gedaan om de beheersdoelstellingen per proces te behalen en of de in opzet bepaalde maatregelen in de praktijk ook bestaan. Daarnaast omvat ons onderzoek werkzaamheden gericht op het vaststellen van de effectieve werking van maatregelen.

Uit de managementletter 2021 is gebleken dat niet van elke maatregel opzet, bestaan en/of werking kan worden vastgesteld. Als gevolg hiervan zijn aanvullende gegevensgerichte werkzaamheden geformuleerd om toereikende zekerheid te verkrijgen over het behalen van de beheersdoelstelling(en) per proces. In dit rapport is per beheersdoelstelling opgenomen op welke manier (systeem- of gegevensgericht) zekerheid is verkregen om tot de conclusie over de beheersdoelstelling te komen.

In dit assurance-rapport rapporteren wij onze bevindingen ten aanzien van de hiervoor beschreven werkzaamheden. Dit resulteert in een oordeel of risico's bij processen voldoende worden beheerst ten einde de beheersdoelstellingen te behalen.

Wij rapporteren in dit assurance-rapport tevens over de betrouwbaarheid - op een specifiek moment, ofwel eenmalig - van de rapportages die Servicepunt71 genereert. Servicepunt71 maakt gebruik van de BI applicatie Cognos, zowel voor de interne processen als voor rapportage richting de deelnemers. In overleg met Servicepunt71 is bepaald voor welke rapportages wij een uitspraak doen over de (rapportagetechnische) betrouwbaarheid. Een nadere omschrijving van dit lijstwerk is in hoofdstuk 4 opgenomen.

3. Ons oordeel

3. Ons oordeel

3.1 Onderbouwing van het oordeel

In hoofdstuk 4 beschrijven wij per proces de uitkomsten van onze werkzaamheden met betrekking tot de toetsing van de beheersdoelstellingen.

Hierbij maken wij een onderscheid tussen de opzet / het bestaan en de werking van beheersmaatregelen in relatie tot de beheersdoelstellingen. Voor sommige beheersdoelstellingen hebben wij (aanvullende) gegevensgerichte werkzaamheden verricht. Wij trekken een conclusie over de realisatie van de beheersdoelstellingen.

De beheersmaatregelen zijn geclassificeerd op basis van het onderscheid manual control, IT dependent manual control, application control en authorization control. De GITC's worden apart behandeld. Wij merken expliciet op dat de GITC's randvoorwaardelijk zijn om te kunnen steunen op application controls.

3.2 Ons oordeel

Naar ons oordeel zijn de, in alle van materieel belang zijnde aspecten, beheersdoelstellingen die onderdeel zijn van de in hoofdstuk 2 beschreven bedrijfsvoeringsprocessen van Servicepunt71, gedurende de verslagperiode van 1 januari 2021 tot en met 31 december 2021 op afdoende wijze gerealiseerd.

Dit oordeel is onderworpen aan de inherente beperkingen zoals genoemd in hoofdstuk 2 (paragraaf 2.4).

3.3 Beoogde gebruikers en doel

Deze rapportage is alleen bestemd voor de deelnemende klantorganisaties die gebruik hebben gemaakt van de dienstverlening van Servicepunt71 en hun accountants. De deelnemende klantorganisaties en hun accountants worden geacht voldoende inzicht te hebben in de bedrijfsvoeringsprocessen om de uitkomsten uit dit rapport in aanmerking te nemen bij het inschatten van de risico's op afwijkingen van materieel belang in de financiële overzichten van de deelnemende gemeenten. Dit in samenhang met overige informatie met inbegrip van informatie over interne beheersmaatregelen die door gemeenten zelf worden uitgevoerd. Bij het selecteren van proceduretests en eventuele steekproeven is in acht genomen dat de selectie representatief is voor de gehele controleperiode en dat alle klantorganisaties vertegenwoordigd zijn.

4. Bevindingen per proces

Leeswijzer bij 4. Bevindingen per proces

Voor een goed begrip van de bevindingen per proces die in dit hoofdstuk worden gepresenteerd, verwijzen wij naar onderstaande legenda's:

Legenda “Type”

M = Manual control
handmatig uitgevoerde maatregel

IDM = IT Dependent Manual control
handmatig uitgevoerde maatregel waarbij gebruik wordt gemaakt van vanuit een applicatie verkregen informatie

AP = Application control
geautomatiseerde maatregel in een applicatie

AT = Authorization control
geautomatiseerde maatregel in een applicatie met betrekking tot gebruikersrechten

Legenda “Bevinding”

De bevinding is de eindconclusie over de werking van een key control dan wel over de uitkomsten van aanvullende gegevensgerichte werkzaamheden indien de werking van de key control niet is (of kan worden) vastgesteld.

Bij de werking van een key control is de eindconclusie gericht op een uitspraak over de realisatie van de beheersdoelstelling. Bij aanvullende gegevensgerichte werkzaamheden is de eindconclusie gericht op een uitspraak over het restrisico in relatie tot de beheersdoelstelling.

Legenda “Toetsing werking”

Als de werking van een maatregel is getoetst, wordt in deze kolom de uitkomst daarvan weergegeven.

Van sommige maatregelen is de werking niet getoetst. Enerzijds omdat dit op basis van de opzet / bestaan niet mogelijk bleek, anderzijds omdat via andere aanvullende gegevensgerichte werkzaamheden een uitspraak wordt gedaan over de mitigatie van het risico in relatie tot de beheersdoelstelling.

Legenda “Eindoordeel”

-  Beheersdoelstelling gerealiseerd / Restrisico gemitigeerd
-  Beheersdoelstelling niet gerealiseerd / Restrisico niet gemitigeerd

Legenda “Aanvullende gegevensgerichte werkzaamheden”

Als aanvullende gegevensgerichte werkzaamheden zijn verricht, dan wordt in deze kolom de uitkomst daarvan weergegeven.

1. Rekeningschema Decade

Nr.	Key control	Beheersdoelstelling	Type	Opzet / Bestaan	Toetsing werking	Aanvullende gegevensgerichte werkzaamheden	Bevinding	Eindoordeel
1.	Jaarlijkse controle BTW-labeling	Adequaat en getrouw beheer (aanmaken, muteren) van de stambestanden betreffende de diverse rekeningschema's. incl. betrouwbaarheid van aan het rekeningschema gekoppelde gegevens, zoals de fiscale labeling of de budgethouder	IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	
2.	Periodieke controle mutaties budgethouders	Rechtmatige toekenning van rechten/bevoegdheden, conform mandaatregeling	IDM	Bestaan vastgesteld	Akkoord*	Akkoord	Geen restrisico ten aanzien van beheersdoelstelling	

* De maatregel werkt effectief, maar dekt niet volledig het risico af dat mutaties m.b.t. budgethouders in het rekeningschema volledig worden doorgevoerd. Om die reden hebben wij op dit punt aanvullende gegevensgerichte werkzaamheden verricht, waarmee toereikende zekerheid is verkregen.

1. Rekeningschema Decade

Nr.	Key control	Beheersdoelstelling	Type	Opzet / Bestaan	Toetsing werking	Aanvullende gegevensgerichte werkzaamheden	Bevinding	Eindoordeel
3.	Toets bij aanlevering nieuw aan te maken kostenplaats / wijziging budgethouder	Adequaat en getrouw beheer (aanmaken, muteren) van de stambestanden betreffende de diverse rekeningschema's. incl. betrouwbaarheid van aan het rekeningschema gekoppelde gegevens, zoals de fiscale labeling of de budgethouder Rechtmatige toekenning van rechten/bevoegdheden, conform mandaatregeling	IDM	Bestaan niet vastgesteld	N.v.t.	Akkoord	Geen restrisico ten aanzien van beheersdoelstelling	
4.	Geen verwijdering dimensie	Adequaat en getrouw beheer (aanmaken, muteren) van de stambestanden betreffende de diverse rekeningschema's. incl. betrouwbaarheid van aan het rekeningschema gekoppelde gegevens, zoals de fiscale labeling of de budgethouder	AP	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	

2. Crediteurenbeheer

Nr.	Key control	Beheersdoelstelling	Type	Opzet / Bestaan	Toetsing werking	Aanvullende gegevensgerichte werkzaamheden	Bevinding	Eindoordeel
1A.	Vier-ogenprincipe Decade	Adequaats en getrouw beheer (integer en consistent) van relatiestamgegevens van crediteuren (NAW, KVK, BRP en bankgegevens)	AP	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
1B.	Controle bij wijziging stamgegevens		IDM	Bestaan vastgesteld	Niet uitgevoerd *	Zie KC2.2	Risico wordt ondervangen door KC2.2	●
2.	Steekproef gewijzigde crediteuren		M	Bestaan vastgesteld	Niet uitgevoerd *	Akkoord	Geen restrisico ten aanzien van beheersdoelstelling	●

* Daar tijdens het uitbrengen van de managementletter reeds was geconstateerd dat brondocumentatie voor het doorvoeren van mutaties (KC1B) dan wel het controleren van mutaties vanuit de derde lijn (KC2) in sommige gevallen ontoereikend was, zijn geen systeemgerichte werkzaamheden verricht.

3. Betalingsverkeer

Nr.	Key control	Beheersdoelstelling	Type	Opzet / Bestaan	Toetsing werking	Aanvullende gegevensgerichte werkzaamheden	Bevinding	Eindoordeel
3.	Funcatiescheiding betaalproces	Het juist, tijdig, volledig (getrouw) en rechtmatig verrichten van betalingen	AT	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
4.	Betaalbestand met goedgekeurde facturen		AP	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
5.	Controle betaalbatch door tweede handtekeningzetter		IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
6.	Periodieke controle op niet toewijsbare betalingen	Het juist, tijdig en volledig (getrouw) registreren van betalingen in de administratie	IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
7.	Controle op bevoegdheid bij handmatige betalingen / betalingen uit subadministraties	Het juist, tijdig, volledig (getrouw) en rechtmatig verrichten van betalingen	M	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
8.	Periodieke controle op dubbele facturen	Het juist, tijdig en volledig (getrouw) registreren van betalingen in de administratie	IDM	Bestaan vastgesteld	Akkoord*	Akkoord	Geen restrisico ten aanzien van beheersdoelstelling	●

* In de managementletter is aangegeven dat op facturen < EUR 1.000 geen nadere analyse wordt uitgevoerd. Om die reden hebben wij op dit punt aanvullende gegevensgerichte werkzaamheden verricht.

4. Purchase 2 Pay

Nr.	Key control	Beheersdoelstelling	Type	Opzet / Bestaan	Toetsing werking	Aanvullende gegevensgerichte werkzaamheden	Bevinding	Eindoordeel
1.	Autorisatie order / factuur	Conformiteit aan externe wet- en regelgeving alsook interne regelgeving/beleid	AT	Bestaan vastgesteld	Niet uitgevoerd *	Uitvoering data analyse op 4-ogen principe***	Geen restrisico ten aanzien van beheersdoelstelling	●
2.	Prestatiebeoordeling		IDM	Bestaan vastgesteld	Niet uitgevoerd **	Niet uitgevoerd **	Geen uitspraak **	Geen uitspraak**
3.	Vier-ogenprincipe orders	Conformiteit aan externe wet- en regelgeving alsook interne regelgeving/beleid	AT	Bestaan vastgesteld	Niet uitgevoerd *	Uitvoering data analyse op 4-ogen principe***	Geen restrisico ten aanzien van beheersdoelstelling	●
4.	Vier-ogenprincipe facturen	Juiste en tijdige verantwoording lasten (juistheid inclusief rubricering, tijdigheid/afgrenzing)	AT	Bestaan vastgesteld	Niet uitgevoerd *	Uitvoering data analyse op 4-ogen principe***	Geen restrisico ten aanzien van beheersdoelstelling	●

* Er is een onvoldoende basis in de GITC van Proquro om de werking van deze maatregelen vast te stellen. Ten aanzien van deze maatregelen zijn daarom aanvullende gegevensgerichte werkzaamheden verricht in de vorm van data-analyse.

** Alleen het bestaan van deze key control wordt vastgesteld. De (gegevensgerichte) controle op prestatielevering van inkoopfacturen is geen onderdeel van de controlewerkzaamheden.

*** Ten aanzien van de uitgevoerde data analyse geldt dat er niet voor alle facturen vast te stellen is of het vier-ogenprincipe gehanteerd is. Dit wordt veroorzaakt door de workflow factuur compleet, waarbij de autorisatie op papier plaatsvindt en waardoor deze niet te achterhalen is op basis van data analyse. Dit is ook vermeld in de inherente beperkingen van dit rapport.

5. Personele lasten

Nr.	Key control	Beheersdoelstelling	Type	Opzet / Bestaan	Toetsing werking	Aanvullende gegevensgerichte werkzaamheden	Bevinding	Eindoordeel
1.	Jaarlijkse controle op parameters RAET	Juiste en tijdige verantwoording (incl. rubricering) van personeelslasten	M	Bestaan vastgesteld	Akkoord	Akkoord	Geen restrisico ten aanzien van beheersdoelstelling	●
2.	Goedkeuring mutaties in YouForce	Rechtmatige uitvoering proces conform wet- en regelgeving (extern en intern normenkader/toetsingskader)	AT	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
3.	2 ^e -lijns steekproef indiensttredingen		IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
4.	2 ^e -lijns steekproef uitdiensttredingen		IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
5.	2 ^e -lijns steekproef declaraties		IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
6.	Controle op handmatig ingevoerde mutaties		IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
7.	2 ^e -lijns steekproef handmatig ingevoerde mutaties		IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
8.	Maandelijks rondrekening	Juiste en tijdige verantwoording (incl. rubricering) van personeelslasten Volledigheid schulden (netto lonen, declaraties, afdrachten loonheffingen, pensioenpremies etc.)	IDM	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●
9.	Jaarlijkse beoordeling ISAE-3402-rapportage RAET	<i>Draagt in principe bij aan alle beheersdoelstellingen van dit proces</i>	M	Bestaan vastgesteld	Akkoord	N.v.t.	Effectief	●

6. General IT Controls Decade

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
1.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de toegekende accounts en rechten actueel zijn. Dit wordt gedaan op basis van rollen welke gekoppeld zijn aan rechten met inachtneming van de gewenste functiescheiding. Hierin worden de rechten en rollen van de functioneel beheerders betrokken. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Voorts hebben wij vernomen dat deze maatregel pas zal worden uitgevoerd na implementatie van de nieuwe financiële applicatie. Op basis van een deelwaarneming op tickets voor aanvragen in rechten van accounts hebben wij vastgesteld in hoeverre er sprake is geweest van functiescheiding tussen aanvrager / account waar rechten aan toegekend dienden te worden en de goedkeurder van het betreffende verzoek. Hierbij zijn geen uitzonderingen geconstateerd.
2.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de mutaties m.b.t. accounts en rechten zijn doorgevoerd op basis van de daarvoor geldende procedure (autorisatie en vastlegging). De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Voorts hebben wij vernomen dat deze maatregel pas zal worden uitgevoerd na implementatie van de nieuwe financiële applicatie. Op basis van een deelwaarneming op tickets voor wijzigingen in rechten van accounts hebben wij vastgesteld in hoeverre er sprake is geweest van functiescheiding tussen aanvrager / account waar rechten aan toegekend dienden te worden en de goedkeurder van het betreffende verzoek. Hierbij zijn geen uitzonderingen geconstateerd.

-  Geen bevinding(en)
-  Verbetering(en) benodigd
-  Verbetering(en) gewenst
-  Tekortkoming(en)

6. General IT Controls Decade

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
3.	Om het risico op fraude door ongeoorloofde toegang te voorkomen dient het wachtwoord te voldoen aan het vigerende Regionaal Wachtwoordbeleid. Dit wordt afgedwongen door het systeem. Minimaal 1 keer per halfjaar wordt een controle uitgevoerd of de instellingen binnen de applicatie conform het wachtwoordbeleid zijn ingericht. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Op basis van beoordeling van wachtwoordinstellingen hebben wij vastgesteld dat deze toereikend zijn.
4.	Om het risico op informatieverlies, hoge boetes en reparatiekosten bij calamiteiten te voorkomen (doordat back-ups en geteste uitwijk- en herstelprocedures ontbreken) wordt minimaal 1 keer per jaar door OpenLine en/of SAAS-leverancier i.s.m. SP71 (functioneel beheerders) de uitwijk- en herstelprocedure uitgevoerd. De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk	Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure.		-

6. General IT Controls Decade

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
5.	Om het risico op storingen, fouten, fraude en extra kosten te mitigeren (doordat wijzigingen aan applicaties niet conform de procedure voor wijzigingsbeheer worden ingepland en voorbereid) voert de functioneel beheerder de nodige applicatiewijzigingen conform een vaste procedure door. Wijzigingen worden pas in productie genomen nadat deze getest zijn in de testomgeving. Vooraf wordt het testplan doorlopen en na het testen wordt een testverslag opgesteld. Deze wordt voorgelegd aan de proces-/applicatie-eigenaar. Na akkoord van de proces-/applicatie-eigenaar wordt de wijziging in productie genomen. Dit wordt vastgelegd in TopDesk.	Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.	●	-
6.	Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.	Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier	●	-

6. General IT Controls Proquero

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
1.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de toegekende accounts en rechten actueel zijn. Dit wordt gedaan op basis van rollen welke gekoppeld zijn aan rechten met inachtneming van de gewenste functiescheiding. Hierin worden de rechten en rollen van de functioneel beheerders betrokken. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Voorts hebben wij vernomen dat deze maatregel pas zal worden uitgevoerd na implementatie van de nieuwe financiële applicatie. Op basis van een deelwaarneming op tickets voor aanvragen in rechten van accounts hebben wij vastgesteld in hoeverre er sprake is geweest van functiescheiding tussen aanvrager / account waar rechten aan toegekend dienden te worden en de goedkeurder van het betreffende verzoek. Hierbij zijn geen uitzonderingen geconstateerd.
2.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de mutaties m.b.t. accounts en rechten zijn doorgevoerd op basis van de daarvoor geldende procedure (autorisatie en vastlegging). De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Voorts hebben wij vernomen dat deze maatregel pas zal worden uitgevoerd na implementatie van de nieuwe financiële applicatie. Op basis van een deelwaarneming op tickets voor wijzigingen in rechten van accounts hebben wij vastgesteld in hoeverre er sprake is geweest van functiescheiding tussen aanvrager / account waar rechten aan toegekend dienden te worden en de goedkeurder van het betreffende verzoek. Hierbij zijn geen uitzonderingen geconstateerd.

6. General IT Controls Proquero

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
3.	Om het risico op fraude door ongeoorloofde toegang te voorkomen dient het wachtwoord te voldoen aan het vigerende Regionaal Wachtwoordbeleid. Dit wordt afgedwongen door het systeem. Minimaal 1 keer per halfjaar wordt een controle uitgevoerd of de instellingen binnen de applicatie conform het wachtwoordbeleid zijn ingericht. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Op basis van beoordeling van wachtwoordinstellingen hebben wij vastgesteld dat deze toereikend zijn.
4.	Om het risico op informatieverlies, hoge boetes en reparatiekosten bij calamiteiten te voorkomen (doordat back-ups en geteste uitwijk- en herstelprocedures ontbreken) wordt minimaal 1 keer per jaar door OpenLine en/of SAAS-leverancier i.s.m. SP71 (functioneel beheerders) de uitwijk- en herstelprocedure uitgevoerd. De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk	Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure.		-

6. General IT Controls Proquero

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
5.	Om het risico op storingen, fouten, fraude en extra kosten te mitigeren (doordat wijzigingen aan applicaties niet conform de procedure voor wijzigingsbeheer worden ingepland en voorbereid) voert de functioneel beheerder de nodige applicatiewijzigingen conform een vaste procedure door. Wijzigingen worden pas in productie genomen nadat deze getest zijn in de testomgeving. Vooraf wordt het testplan doorlopen en na het testen wordt een testverslag opgesteld. Deze wordt voorgelegd aan de proces-/applicatie-eigenaar. Na akkoord van de proces-/applicatie-eigenaar wordt de wijziging in productie genomen. Dit wordt vastgelegd in TopDesk.	Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.	●	-
6.	Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.	Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier	●	-

6. General IT Controls YouForce

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
1.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de toegekende accounts en rechten actueel zijn. Dit wordt gedaan op basis van rollen welke gekoppeld zijn aan rechten met inachtneming van de gewenste functiescheiding. Hierin worden de rechten en rollen van de functioneel beheerders betrokken. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		-
2.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de mutaties m.b.t. accounts en rechten zijn doorgevoerd op basis van de daarvoor geldende procedure (autorisatie en vastlegging). De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		-

6. General IT Controls YouForce

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
3.	Om het risico op fraude door ongeoorloofde toegang te voorkomen dient het wachtwoord te voldoen aan het vigerende Regionaal Wachtwoordbeleid. Dit wordt afgedwongen door het systeem. Minimaal 1 keer per halfjaar wordt een controle uitgevoerd of de instellingen binnen de applicatie conform het wachtwoordbeleid zijn ingericht. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Op basis van beoordeling van wachtwoordinstellingen hebben wij vastgesteld dat deze toereikend zijn.
4.	Om het risico op informatieverlies, hoge boetes en reparatiekosten bij calamiteiten te voorkomen (doordat back-ups en geteste uitwijk- en herstelprocedures ontbreken) wordt minimaal 1 keer per jaar door OpenLine en/of SAAS-leverancier i.s.m. SP71 (functioneel beheerders) de uitwijk- en herstelprocedure uitgevoerd. De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk	Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure.		-

6. General IT Controls YouForce

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
5.	Om het risico op storingen, fouten, fraude en extra kosten te mitigeren (doordat wijzigingen aan applicaties niet conform de procedure voor wijzigingsbeheer worden ingepland en voorbereid) voert de functioneel beheerder de nodige applicatiewijzigingen conform een vaste procedure door. Wijzigingen worden pas in productie genomen nadat deze getest zijn in de testomgeving. Vooraf wordt het testplan doorlopen en na het testen wordt een testverslag opgesteld. Deze wordt voorgelegd aan de proces-/applicatie-eigenaar. Na akkoord van de proces-/applicatie-eigenaar wordt de wijziging in productie genomen. Dit wordt vastgelegd in TopDesk.	Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.		-
6.	Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.	Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier		-

6. General IT Controls Beaufort

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
1.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de toegekende accounts en rechten actueel zijn. Dit wordt gedaan op basis van rollen welke gekoppeld zijn aan rechten met inachtneming van de gewenste functiescheiding. Hierin worden de rechten en rollen van de functioneel beheerders betrokken. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		-
2.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de mutaties m.b.t. accounts en rechten zijn doorgevoerd op basis van de daarvoor geldende procedure (autorisatie en vastlegging). De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		-

6. General IT Controls Beaufort

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
3.	Om het risico op fraude door ongeoorloofde toegang te voorkomen dient het wachtwoord te voldoen aan het vigerende Regionaal Wachtwoordbeleid. Dit wordt afgedwongen door het systeem. Minimaal 1 keer per halfjaar wordt een controle uitgevoerd of de instellingen binnen de applicatie conform het wachtwoordbeleid zijn ingericht. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Op basis van beoordeling van wachtwoordinstellingen hebben wij vastgesteld dat deze toereikend zijn.
4.	Om het risico op informatieverlies, hoge boetes en reparatiekosten bij calamiteiten te voorkomen (doordat back-ups en geteste uitwijk- en herstelprocedures ontbreken) wordt minimaal 1 keer per jaar door OpenLine en/of SAAS-leverancier i.s.m. SP71 (functioneel beheerders) de uitwijk- en herstelprocedure uitgevoerd. De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk	Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure.		-

6. General IT Controls Beaufort

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
5.	Om het risico op storingen, fouten, fraude en extra kosten te mitigeren (doordat wijzigingen aan applicaties niet conform de procedure voor wijzigingsbeheer worden ingepland en voorbereid) voert de functioneel beheerder de nodige applicatiewijzigingen conform een vaste procedure door. Wijzigingen worden pas in productie genomen nadat deze getest zijn in de testomgeving. Vooraf wordt het testplan doorlopen en na het testen wordt een testverslag opgesteld. Deze wordt voorgelegd aan de proces-/applicatie-eigenaar. Na akkoord van de proces-/applicatie-eigenaar wordt de wijziging in productie genomen. Dit wordt vastgelegd in TopDesk.	Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.	●	-
6.	Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.	Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier	●	-

6. General IT Controls TIM

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
1.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de toegekende accounts en rechten actueel zijn. Dit wordt gedaan op basis van rollen welke gekoppeld zijn aan rechten met inachtneming van de gewenste functiescheiding. Hierin worden de rechten en rollen van de functioneel beheerders betrokken. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		-
2.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de mutaties m.b.t. accounts en rechten zijn doorgevoerd op basis van de daarvoor geldende procedure (autorisatie en vastlegging). De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders.		-

6. General IT Controls TIM

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
3.	Om het risico op fraude door ongeoorloofde toegang te voorkomen dient het wachtwoord te voldoen aan het vigerende Regionaal Wachtwoordbeleid. Dit wordt afgedwongen door het systeem. Minimaal 1 keer per halfjaar wordt een controle uitgevoerd of de instellingen binnen de applicatie conform het wachtwoordbeleid zijn ingericht. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.	Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders.		Op basis van interview hebben wij vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. Op basis van beoordeling van wachtwoordinstellingen hebben wij vastgesteld dat deze toereikend zijn.
4.	Om het risico op informatieverlies, hoge boetes en reparatiekosten bij calamiteiten te voorkomen (doordat back-ups en geteste uitwijk- en herstelprocedures ontbreken) wordt minimaal 1 keer per jaar door OpenLine en/of SAAS-leverancier i.s.m. SP71 (functioneel beheerders) de uitwijk- en herstelprocedure uitgevoerd. De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk	Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure.		-

6. General IT Controls TIM

Nr.	Key control	Beheersdoelstelling	Eindoordeel	Bevindingen 2021
5.	Om het risico op storingen, fouten, fraude en extra kosten te mitigeren (doordat wijzigingen aan applicaties niet conform de procedure voor wijzigingsbeheer worden ingepland en voorbereid) voert de functioneel beheerder de nodige applicatiewijzigingen conform een vaste procedure door. Wijzigingen worden pas in productie genomen nadat deze getest zijn in de testomgeving. Vooraf wordt het testplan doorlopen en na het testen wordt een testverslag opgesteld. Deze wordt voorgelegd aan de proces-/applicatie-eigenaar. Na akkoord van de proces-/applicatie-eigenaar wordt de wijziging in productie genomen. Dit wordt vastgelegd in TopDesk.	Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.	●	-
6.	Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.	Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier	●	-

Betrouwbaarheid Cognos rapporten

Cognos is een rapportagetool die door middel van query's informatie haalt uit Decade Financials. In het kader van de assurance-rapportage zijn de vermelde rapporten geselecteerd. Uitgangspunt voor de werkzaamheden is dat de betrouwbaarheid van de rapportages éénmalig wordt vastgesteld op rapportagemoment na afsluiten van administraties. De betrouwbaarheid van de rapportages is vastgesteld per 04-03-2022. Het daarbij gehanteerde aggregatieniveau is in de tabel vermeld.

Nr.	Cognos rapportage	Applicatie bronadministratie	Aggregatieniveau	Bevinding
1.	Balans	Decade	Grootboek	 Leiden Voor Leiden is een verschil van EUR 2,1 mln. geconstateerd (Cognos hoger t.o.v. Decade): - EUR 815.500 heeft betrekking op kapitaalverstrekking aan deelneming. Dit heeft betrekking op grootboekrekening 05002 Voorziening Innovationquarter. Deze loopt niet over de activamodule en wordt daarom niet getoond in het overzicht activarekening. - EUR 1,3 mln. heeft betrekking op langlopende geldleningen. Servicepunt 71 heeft aangegeven dat dit te maken heeft met twee correctieposten op deze balanspost (voorzieningen). Zoeterwoude Voor Zoeterwoude is een verschil geconstateerd in de voorziening dubieuze debiteuren (EUR 92.700). De voorziening staat in de saldibalans geclassificeerd als FVA, deze wordt per jaareinde gereclassificeerd naar de debiteuren en komt derhalve niet voor op de activa-rekening.
2.	Activa-rekening	Decade	Activasoort, per administratie	
3.	Kolommenbalans	Decade	N.v.t.	
4.	Saldo afstemming balans crediteuren	Decade	Zonder controleur	
5.	Budgetbewaking Programma	Decade	Programma	

Betrouwbaarheid Cognos rapporten

Cognos is een rapportagetool die door middel van query's informatie haalt uit Decade Financials. In het kader van de assurance-rapportage zijn de vermelde rapporten geselecteerd. Uitgangspunt voor de werkzaamheden is dat de betrouwbaarheid van de rapportages éénmalig wordt vastgesteld op rapportagemoment na afsluiten van administraties. De betrouwbaarheid van de rapportages is vastgesteld per 04-03-2022. Het daarbij gehanteerde aggregatieniveau is in de tabel vermeld.

Nr.	Cognos rapportage	Applicatie bronadministratie	Aggregatieniveau	Bevinding
6.	Boeking per grootboek	Decade	Grootboek	●
7.	Boeking per kostenplaats	Decade	Kostenplaats	●
8.	Inkoopfacturen met boekingen en verplichtingen (versie 2019)	Decade	Excel specificatie	Op het totaalniveau van inkoopfacturen is een verschil van EUR 201.000 geconstateerd. Dit verschil heeft uitsluitend betrekking op de BTW-weergave. Voor een deel van de inkoopfacturen is wel BTW in Cognos opgenomen en niet in Decade; andersom is voor een deel van de inkoopfacturen wel BTW in Decade opgenomen en niet in Cognos.

Bijlagen

Bijlage 1: Uitgebreide omschrijving key controls

1. Rekeningschema Decade

Nr.	Key control <i>verkorte omschrijving</i>	Key control <i>uitgebreide omschrijving</i>
1.	Jaarlijkse controle BTW-labeling	Jaarlijks wordt door de fiscalist een controle uitgevoerd op de juistheid van de BTW-labeling bij de in het boekjaar nieuw aangemaakte kostenplaatsen / kostensoorten. Hierover rapporteert hij aan de controllers van de gemeenten. Jaarlijks vindt eveneens door de fiscalist - halverwege het jaar - een integrale controle over jaar t-1 plaats op kostenplaatsniveau op de BTW-boeking. Wijzigingen in de BTW-labeling van reeds in het boekjaar bestaande kostenplaatsen vallen hier onder. Ook hierover rapporteert hij aan de controllers van de gemeenten.
2.	Periodieke controle mutaties budgethouders	Om het risico op onrechtmatig geautoriseerde mutaties in het rekeningschema te ondervangen, stellen de senior financieel adviseurs vast, 2x per jaar achteraf, dat alle doorgevoerde mutaties conform mandaatregisters resp. budgethoudersregelingen van de betreffende partnerorganisaties zijn. De senior financieel adviseurs leggen de controle zichtbaar vast middels een rapport. Betreft een detectieve key control welke per halfjaar plaatsvindt.
3.	Toets bij aanlevering nieuw aan te maken kostenplaats / wijziging budgethouder	Een financieel specialist voert een controle uit op de aangeleverde mutatie voor een nieuw aan te maken kostenplaats. De financieel specialist toetst of de juiste persoon, conform de budgethoudersregeling de wijziging / aanmaak heeft geautoriseerd en dat deze dan ook budgethoudersrechten heeft verkregen. Daarnaast stelt de financieel specialist vast dat de koppeling met taakveld en programma logisch is. Bij akkoord wordt de wijziging opgenomen in de uploadsheet, waarmee de wijziging wordt doorgevoerd in de financiële administratie. Bij een wijziging van de budgethouder op een kostenplaats in het systeem voert een financieel specialist een controle uit waarbij wordt vastgesteld dat de nieuwe budgethouder, budgethoudersrechten heeft conform de budgethoudersregeling / mandaatregeling van de partnerorganisatie en dat voor wijziging de gemandateerde medewerkers hebben getekend voor akkoord. NB: het controleren of de aan Decade aangeboden mutaties ook daadwerkelijk zijn doorgevoerd in Decade maakt geen onderdeel uit van de controle door de financieel specialist.
4.	Geen verwijdering dimensie	Een dimensie in Decade kan niet worden verwijderd als er al op geboekt is

2. Crediteurenbeheer

Nr.	Key control <i>verkorte omschrijving</i>	Key control <i>uitgebreide omschrijving</i>
1A.	Vier-ogenprincipe Decade	Binnen Decade wordt afgedwongen dat een financieel medewerker die een wijziging in de crediteuren stamgegevens accordeert een ander dient te zijn dan de medewerker die de wijziging heeft aangemaakt.
1B.	Controle bij wijziging stamgegevens	Een tweede financieel medewerker controleert of de wijziging in de stamgegevens van een crediteur is doorgevoerd op basis van achterliggende brondocumentatie, welke voldoende betrouwbaar is. Zichtbaar door de accordering in het systeem.
2.	Steekproef gewijzigde crediteuren	Door medewerker Financieel advies van team AO/IC wordt jaarlijks middels een deelwaarneming vastgesteld dat autorisatie van crediteuren stamgegevens heeft plaatsgevonden op deugdelijke en betrouwbare brondocumentatie. Deze selectie wordt gemaakt op basis van een aselechte steekproef van de gewijzigde crediteuren in het boekjaar.

3. Betalingsverkeer

Nr.	Key control verkorte omschrijving	Key control uitgebreide omschrijving
3.	Functiescheiding betaalproces	Functiescheiding in het betaalproces (eerste en tweede handtekening). Zichtbaar middels de autorisatie-inrichting in de BNG-module.
4.	Betaalbestand met goedgekeurde facturen	Bij het maken van een betaalbestand in Decade is het alleen mogelijk om facturen te selecteren die een goedkeuringsworkflow hebben doorlopen.
5.	Controle betaalbatch door tweede handtekeningzetter	De tweede handtekeningzetter in het betaalproces controleren per betaling of het bedrag van de betaling overeenstemt met de achterliggende betaalbatch, dat het aantal posten gelijk is, dat het SHA controlegetal overeenstemt en dat het te betalen bedrag juist wordt overgenomen. Bij akkoord zetten zij hun handtekening in de betaalapplicatie van de BNG waaruit de controle blijkt.
6.	Periodieke controle op niet toewijsbare betalingen	Periodiek wordt door een financieel medewerker, op basis van een cognoslijst, een controle uitgevoerd op de niet toewijsbare betalingen/ontvangsten uit een betaalbatch. Dit wordt vastgelegd in Eqili waarbij wordt vastgelegd welke acties zijn verricht per niet toewijsbare betaling/ontvangst en welke opvolging hieraan is gegeven.
7.	Controle op bevoegdheid bij handmatige betalingen / betalingen uit subadministraties	Bij handmatige betalingen/ betalingen uit subadministraties wordt door de medewerker betaalverkeer vastgesteld dat de aanlevering heeft plaatsgevonden conform een daartoe bevoegde medewerker van de klantorganisatie.
8.	Periodieke controle op dubbele betalingen	Periodiek wordt door een financieel medewerker een controle uitgevoerd op inkoopfacturen met dezelfde bedragen op basis van een standaard export uit cognos. De opvolging van bevindingen wordt per item vastgelegd en gedocumenteerd. Deze werkzaamheden worden vastgelegd in Eqili en door een tweede onafhankelijke medewerker Kwaliteit gereviewed.

4. Purchase2Pay (P2P)

Nr.	Key control verkorte omschrijving	Key control uitgebreide omschrijving
1.	Autorisatie order / factuur	Facturen met order > €300,-: De budgethouder autoriseert de order (> €300,-) in Proquro. Facturen zonder order: De budgethouder autoriseert de factuur.
2.	Prestatiebeoordeling	De prestatieverklaarder (of budgethouder bij facturen zonder order) stelt zichtbaar vast of de goederen en diensten zijn geleverd conform contract, opdrachtbevestiging o.i.d., voordat de factuur betaalbaar wordt gesteld. De prestatiebeoordelaar neemt het bedrag op of uren bij inhuur en een toelichting waarin verklaard wordt dat de prestatie is geleverd. NB: Het is niet verplicht om ook onderliggende documentatie van de prestatiebeoordeling op te nemen in Proquro.
3.	Vier-ogenprincipe orders	Bij orders > €300,- is er sprake van functiescheiding (4-ogen) tussen budgethouder en besteller.
4.	Vier-ogenprincipe facturen	Bij facturen zonder order is er sprake van functiescheiding (4-ogen) tussen codeur en budgethouder.

5. Personele lasten

Nr.	Key control <i>verkorte omschrijving</i>	Key control <i>uitgebreide omschrijving</i>
1.	Jaarlijkse controle op parameters RAET	Om het risico op onjuiste en onvolledige verantwoording van personele lasten en schulden te ondervangen, stelt de senior salarisadministrateur jaarlijks integraal vast, dat alle werkgeverspremies, percentages, franchisebedragen en overige regelgeving per klantorganisatie die in het systeem zijn opgenomen, overeenkomstig de betreffende normen zijn.
2.	Goedkeuring mutatie in YouForce	Om het risico op onrechtmatige mutaties in aanspraken op beloningscomponenten m.b.t. dienstverband (IN DIENST / UIT DIENST) en in aanspraken op beloningscomponenten m.b.t. niet uren-componenten (KOSTENDECLARATIES) te ondervangen, wordt in de workflow in YouForce afgedwongen dat de verantwoordelijke manager de mutatie goedkeurt.
3.	2 ^e -lijns steekproef indiensttredingen	Om het risico op onrechtmatige mutaties in aanspraken op beloningscomponenten m.b.t. dienstverband (IN DIENST) te ondervangen, stelt de 2e-lijns-kwaliteitsmedewerker steekproefsgewijs vast, nadat de mutatie in Beaufort is verwerkt, dat noodzakelijke documentatie aanwezig is en voldoet aan de relevante kaders (formele en materiële toets aan de hand van regelgeving) en dat de invoer in Beaufort overeenkomt met deze documentatie en de aanvraag in YouForce. Indien afwijkingen worden geconstateerd, worden deze opgevolgd.
4.	2 ^e -lijns steekproef uitdiensttredingen	Om het risico op onrechtmatige mutaties in aanspraken op beloningscomponenten m.b.t. dienstverband (UIT DIENST) te ondervangen, stelt de 2e-lijns-kwaliteitsmedewerker steekproefsgewijs vast, nadat de mutatie in Beaufort is verwerkt, dat noodzakelijke documentatie aanwezig is en voldoet aan de relevante kaders (formele en materiële toets aan de hand van regelgeving) en dat de invoer in Beaufort overeenkomt met deze documentatie en de aanvraag in YouForce. Indien afwijkingen worden geconstateerd, worden deze opgevolgd.
5.	2 ^e -lijns steekproef declaraties	Om het risico op onrechtmatige mutaties in aanspraken op beloningscomponenten m.b.t. niet-uren componenten (KOSTENDECLARATIES) te ondervangen, stelt de 2e-lijns-kwaliteitsmedewerker steekproefsgewijs vast, nadat de mutatie in Beaufort is verwerkt, dat noodzakelijke documentatie aanwezig is en voldoet aan de relevante kaders (formele en materiële toets aan de hand van regelgeving) en dat de invoer in Beaufort overeenkomt met deze documentatie en de aanvraag in YouForce. Indien afwijkingen worden geconstateerd, worden deze opgevolgd.
6.	Controle op handmatig ingevoerde mutaties	Om het risico op onrechtmatige mutaties in aanspraken op beloningscomponenten te ondervangen, verricht een tweede medewerker van de SA invoercontrole op handmatig ingevoerde mutaties, waarbij hij vaststelt dat de mutatie juist is ingevoerd in Beaufort. Hij legt dit vast door het betreffende mutatieverslag te paraferen.

5. Personele lasten

Nr.	Key control verkorte omschrijving	Key control uitgebreide omschrijving
7.	2 ^e -lijns steekproef handmatig ingevoerde mutaties	Om het risico op onrechtmatige mutaties in aanspraken op beloningscomponenten te ondervangen, verricht de 2e-lijns-kwaliteitsmedewerker steekproefsgewijs een controle op handmatig ingevoerde mutaties in Beaufort, waarbij hij vaststelt dat het oorspronkelijke mutatieverslag uit KC6 is gecontroleerd door een tweede medewerker SA en dat de mutatie juist is ingevoerd in Beaufort. Indien afwijkingen worden geconstateerd, worden deze opgevolgd.
8.	Maandelijkse rondrekening	Om het risico op een onjuiste of onvolledige verantwoording van personele lasten en schulden te ondervangen, voert de medewerker SA maandelijks een rondrekening uit. Hierbij voert de medewerker SA een drietal controles uit: • Of betaalstaten, betaalopdrachten en de loonaangifte met elkaar aansluiten. • Of de saldi tussenrekeningen m.b.t. salarissen aflopen. • Of de SA aansluit op de FA.
9.	Jaarlijkse beoordeling ISAE-3402-rapportage RAET	Om het risico op een onbetrouwbare werking van de extern verzorgde salarisadministratie en de extern ondersteunde webomgeving YouForce te ondervangen, beoordelen de applicatiebeheerder en de teammanager jaarlijks de van RAET ontvangen ISAE-3402-rapportage en stellen de impact daarvan op de AO/IB en op eventueel resterende procesrisico's daarbij in gezamenlijkheid vast.

6. General IT Controls

Nr.	Key control
1.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de toegekende accounts en rechten actueel zijn. Dit wordt gedaan op basis van rollen welke gekoppeld zijn aan rechten met inachtneming van de gewenste functiescheiding. Hierin worden de rechten en rollen van de functioneel beheerders betrokken. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.
2.	Om het risico op toegang tot applicaties of specifieke functies binnen applicaties voor niet bevoegden te voorkomen wordt minimaal 1 keer per halfjaar gecontroleerd of de mutaties m.b.t. accounts en rechten zijn doorgevoerd op basis van de daarvoor geldende procedure (autorisatie en vastlegging). De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.
3.	Om het risico op fraude door ongeoorloofde toegang te voorkomen dient het wachtwoord te voldoen aan het vigerende Regionaal Wachtwoordbeleid. Dit wordt afgedwongen door het systeem. Minimaal 1 keer per halfjaar wordt een controle uitgevoerd of de instellingen binnen de applicatie conform het wachtwoordbeleid zijn ingericht. De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.
4.	Om het risico op informatieverlies, hoge boetes en reparatiekosten bij calamiteiten te voorkomen (doordat back-ups en geteste uitwijk- en herstelprocedures ontbreken) wordt minimaal 1 keer per jaar door OpenLine en/of SAAS-leverancier i.s.m. SP71 (functioneel beheerders) de uitwijk- en herstelprocedure uitgevoerd. De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk
5.	Om het risico op storingen, fouten, fraude en extra kosten te mitigeren (doordat wijzigingen aan applicaties niet conform de procedure voor wijzigingsbeheer worden ingepland en voorbereid) voert de functioneel beheerder de nodige applicatiewijzigingen conform een vaste procedure door. Wijzigingen worden pas in productie genomen nadat deze getest zijn in de testomgeving. Vooraf wordt het testplan doorlopen en na het testen wordt een testverslag opgesteld. Deze wordt voorgelegd aan de proces-/applicatie-eigenaar. Na akkoord van de proces-/applicatie-eigenaar wordt de wijziging in productie genomen. Dit wordt vastgelegd in TopDesk.
6.	Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.

Contactgegevens

drs. S. (Stefan) Turenhout RA

Director Audit

06 – 52 75 98 79

s.turenhout@bakertilly.nl

R. (Roy) Zwartjes MSc RE

Senior manager IT Advisory

06 – 52 76 53 78

r.zwartjes@bakertilly.nl

Kantoorgegevens:

Baker Tilly (Netherlands) N.V.

Scheveningseweg 80 - 82

2517 KZ DEN HAAG

Postbus 85745

2508 CK DEN HAAG

T: 070 358 90 00

