

# Managementletter

Servicepunt71

Boekjaar 2021

*15 oktober 2021*

# Aanbiedingsbrief

Servicepunt71  
t.a.v. de directie  
Postbus 171  
2300 AD LEIDEN

**Referentie:** 202131/DZ/ST/FMD/1013935

**Betreft:** Aanbieding managementletter 2021

Geachte directie,

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 ons tussentijds onderzoek.

In onze managementletter rapporteren wij over de uitkomsten van ons onderzoek naar de opzet en het bestaan van de administratieve organisatie en interne beheersing (AO/IB) van de bedrijfsvoerings-processen inzake de dienstverlening van Servicepunt71 ten behoeve van de deelnemende klantorganisaties. Eveneens rapporteren wij in deze managementletter ook - zo veel mogelijk - over de werking van maatregelen in het eerste halfjaar 2021 dan wel over de uitkomsten van gegevensgerichte werkzaamheden.

Onze bevindingen vloeien voort uit ons onderzoek naar de opzet van de AO/IB in relatie tot de beheersdoelstellingen die in de interne controleplannen 2021 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.

Daarnaast doen wij vanuit onze natuurlijke adviesfunctie een aantal aanbevelingen die een bijdrage leveren aan het zelfcontrolerende vermogen van uw organisatie.

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

Wij verzoeken u vriendelijk onze rapportage niet onder anderen dan de genoemde gebruikersgroep te verspreiden zonder onze voorafgaande schriftelijke toestemming. Eveneens verzoeken wij u vriendelijk om onze rapportage niet publiek te maken.

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

# Inhouds- opgave

|                                      |    |
|--------------------------------------|----|
| 1. Management samenvatting           | 4  |
| 2. Doel en reikwijdte opdracht       | 8  |
| 3. Bevindingen tussentijds onderzoek | 13 |

## **Bijlagen:**

|                                                               |    |
|---------------------------------------------------------------|----|
| Bijlage 1: Detailbevindingen tussentijds onderzoek            | 21 |
| Bijlage 2: Detailbevindingen bij GITC in het CFW              | 32 |
| Bijlage 3: Opvolging aanbevelingen management-<br>letter 2020 | 48 |
| Bijlage 4: Uitgebreide omschrijving key controls              | 53 |

# 1. Management samenvatting

# 1. Management samenvatting

## 1.1 Onze opdracht

Wij hebben tijdens het tussentijds onderzoek, conform de overeengekomen opdracht, werkzaamheden verricht ter beoordeling van de opzet en het bestaan van de key controls in de bedrijfsvoeringsprocessen die Servicepunt71 uitvoert ten behoeve van de eigen organisatie en de deelnemende klantorganisaties. Hierbij is ook de werking van maatregelen over het eerste halfjaar 2021 getest en/of zijn aanvullende gegevensgerichte werkzaamheden uitgevoerd. Dit tussentijds onderzoek is gericht op het vaststellen of Servicepunt71 de risico's ten aanzien van deze processen voldoende beheerst ten einde de beheersdoelstellingen per proces te behalen.

## 1.2 Belangrijkste bevindingen

### *Scope van de opdracht nagenoeg gelijk aan 2020*

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.

Ten aanzien van het proces Purchase2Pay (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.

### *Verbetering in de beschrijving van de opzet van GITC*

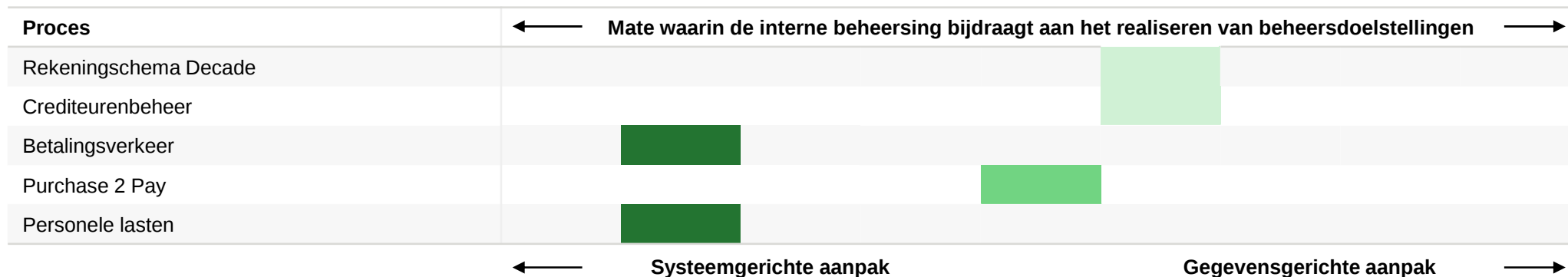
Servicepunt71 heeft voor dit controlejaar haar beschrijving van de interne beheersing op het gebied van de algemene IT beheersing herzien. Dit heeft geleid tot een, in opzet, dekkend stelsel van algemene IT beheersingsmaatregelen als fundament onder het control framework. Hiermee is een belangrijke stap gezet op het gebied van interne beheersing waardoor de organisatie beter in staat is toetsingen uit te voeren op de IT beheersing.

### *Op weg naar het gewenste kwaliteitsniveau van de interne beheersing*

Wij zien met name ten aanzien van de processen Betalingsverkeer en Personele lasten dat het kwaliteitsniveau van de interne beheersing een constant en toereikend niveau bereikt. Dit maakt het mogelijk om voor deze processen een vrijwel volledige systeemgerichte aanpak te volgen.

### *Aandacht voor processen Rekeningschema Decade en Crediteurenbeheer*

Met name bij de processen Rekeningschema Decade en Crediteurenbeheer zien wij nog belangrijke verbeterpunten in de interne beheersing. Dit leidt ertoe dat ook dit jaar een groot deel van de controlewerkzaamheden bij deze processen gegevensgericht van aard is om voldoende zekerheid te verkrijgen over de realisatie van de beheersdoelstellingen. De gesignaleerde verbeterpunten 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. Om die reden hebben wij in de managementletter 2021 dan ook een onderscheid aangebracht tussen enerzijds bevindingen die nieuw zijn in 2021 en anderzijds bevindingen die ook in 2020 (en eventueel 2019) zijn gerapporteerd, maar eveneens van toepassing zijn op 2021.



### 1.3 De interne beheersing per proces

In bovenstaande tabel is in één oogopslag te zien in welke mate (per proces) de interne beheersing bijdraagt aan het realiseren van de beheersdoelstellingen. Dit is gebaseerd op de bevindingen uit ons tussentijds onderzoek. Per proces volgt een beknopte toelichting in relatie tot de tabel uit de managementletter 2020. Uit het overzicht blijkt dat er een gecombineerde systeem- en gegevensgerichte aanpak mogelijk is om een oordeel te geven over de beheersdoelstellingen van Servicepunt71. Ten opzichte van het controlejaar 2020 constateren wij dat de controle-aanpak in 2021 voor Rekeningschema Decade en Crediteurenbeheer vergelijkbaar is. Voor Betalingsverkeer en Personele lasten verwachten wij minder aanvullende gegevensgerichte werkzaamheden te hoeven uitvoeren ten opzichte van 2020.

**Rekeningschema Decade:** Het vaststellen van de juistheid en volledigheid van doorgevoerde mutaties blijft net als in 2020 een aandachtspunt. De gegevensgerichte aanpak voor dit proces wordt daarom gecontinueerd.

**Crediteurenbeheer:** Sinds vorig jaar is een derdelijnscontrole ingevoerd om het risico te mitigeren dat mutaties worden doorgevoerd op basis van ontoereikende brondocumentatie. Deze controle dekt echter, in overeenstemming met de bevindingen van vorig jaar, het risico nog niet volledig af doordat niet in alle gevallen onderbouwingen worden vergaard die vanuit een assurance-perspectief

voldoende zijn. De gegevensgerichte aanpak wordt daarom voor dit proces dit jaar gecontinueerd.

**Betalingsverkeer:** Conform verwachting is voor dit proces een systeemgerichte aanpak mogelijk. Ten opzichte van voorgaand jaar nemen wij ook een verbetering waar in de analyse op dubbele betalingen, waardoor wij verwachten ook op dit aspect een systeemgerichte aanpak te kunnen hanteren.

**Purchase 2 Pay:** Net als voorgaand jaar hanteren wij een gegevensgerichte aanpak voor dit proces, waarbij wij gebruik maken van de inzet van data-analyse. Dit vloeit voort uit ontoereikende algemene IT-beheersmaatregelen die ten grondslag liggen aan geautomatiseerde beheersmaatregelen in de applicatie Proquro. Met betrekking tot de prestatielevering van inkopen worden door ons geen test- en / of gegevensgerichte werkzaamheden verricht, conform afspraak met Servicepunt71.

**Personele lasten:** Conform verwachting is voor het proces van personele lasten een systeemgerichte aanpak mogelijk. Ten opzichte van voorgaand jaar nemen wij ook een verbetering waar in de borging van de volledigheid van het (Beaufort-) lijstwerk dat wordt gebruikt bij de tweedelijns steekproeven.

#### 1.4 Belangrijkste bevindingen general IT controls

Servicepunt71 heeft de general IT controls, die dienen als fundament onder het control framework, dit jaar herzien. Dit heeft geleid tot een set aan beheersingsmaatregelen die duidelijk binnen de organisatie belegd zijn enerzijds en een duidelijk doel kennen binnen het bredere control framework anderzijds. Tijdens onze interviews is naar voren gekomen dat hoewel deze general IT controls in opzet beschreven zijn, de concrete invulling van deze controls in veel gevallen nog niet is vormgegeven. Dit leidt er in veel gevallen toe dat wij de werking van de (nieuwe) general IT controls voor dit controlejaar nog niet vast kunnen stellen. Wij hebben daarom aanvullende controlewerkzaamheden uitgevoerd om te beoordelen in hoeverre de risico's voor het eerste halfjaar voldoende gemitigeerd zijn.

Daarnaast dient opgemerkt te worden dat wij voor een aantal maatregelen, met name gericht op de aspecten back-up en recovery en wijzigingsbeheer, tijdens de interim audit nog geen controlewerkzaamheden hebben kunnen uitvoeren omdat de maatregel nog niet uitgevoerd was.

Tot slot is er in het bijzonder aandacht nodig voor de overgang naar Beaufort SaaS. Hoewel Servicepunt71 controles heeft uitgevoerd om vast te stellen dat deze overgang goed verlopen is, ontbreekt het aan een officiële decharge of akkoord voor in gebruik nemen van de applicatie. Dit terwijl wij begrepen hebben dat de applicatie in maart 2021 in gebruik genomen is.

#### 1.5 Vooruitblik nog uit te voeren werkzaamheden

De bevindingen in deze managementletter zijn gebaseerd op de tot op heden uitgevoerde systeem- en gegevensgerichte werkzaamheden over de periode tot en met juni. Hieruit blijken nog geen bevindingen die van invloed zijn op het niet realiseren van beheersdoelstellingen.

De nog uit te voeren werkzaamheden bestaan uit systeem- en gegevensgerichte werkzaamheden die nodig zijn om een uitspraak te doen over het gehele jaar.

Bij hoofdzakelijk Crediteurenbeheer en Rekeningschema Decade zijn aanvullende gegevensgerichte werkzaamheden nodig om toereikende zekerheid te verkrijgen over de realisatie van de beheersdoelstellingen.

#### 1.6 Resumé

Ons onderzoek heeft als referentiepunt de doelstelling van Servicepunt71 om de bedrijfsvoeringsprocessen voor haar deelnemers zo betrouwbaar, tijdig en accuraat mogelijk uit te voeren.

Wij constateren dat de interne beheersing van de processen Betalingsverkeer en Personele lasten verder versterkt is ten opzichte van voorgaand jaar. Tegelijkertijd zien wij nog ruimte voor verbetering in de interne beheersing van de processen Crediteurenbeheer en Rekeningschema Decade. In voorliggende en eerdere rapportages (2019 en 2020) doen wij u daarvoor diverse aanbevelingen om te komen tot een situatie waarin in opzet de doelstelling van de organisatie gestand wordt gedaan. Indien Servicepunt71 ervoor kiest om geen invulling te geven aan deze aanbevelingen vanuit een eigen risicoafweging, dan blijft op deze processen een gecombineerde systeem- en gegevensgerichte aanpak noodzakelijk.

***Op basis van de werkzaamheden die zijn uitgevoerd is het realiseren van toereikende controlezekerheid over de realisatie van de beheersdoelstellingen in het CFW haalbaar. De realisatie van de beheersdoelstellingen is daarmee afhankelijk van de nog uit te voeren werkzaamheden in het tweede halfjaar.***

## 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. 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 verschillende 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 (beperkte) 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 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 eerste halfjaar 2021 effectief hebben gewerkt.

### **2.4 Inherente beperkingen tussentijds onderzoek**

Ten aanzien van onze werkzaamheden in het kader van het tussentijds 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;
- 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;
- Na het uitbrengen van deze managementletter kan het mogelijk zijn dat nieuwe inherente beperkingen worden geïdentificeerd. Hiervan zullen wij in het assurance-rapport melding maken.

## 2.5 Managementletter

Deze managementletter is gebaseerd op de uitkomsten van de tot nu toe verrichte werkzaamheden voor het assurance-rapport 2021.

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 tussentijds onderzoek omvat het verkrijgen van inzicht in:

- De wijze waarop processen en daarin verankerde beheersmaatregelen (key controls) zijn opgezet en beoordelen of dit op afdoende wijze is gedaan om de beheersdoelstellingen per proces te behalen;
- Het uitvoeren van werkzaamheden om vast te stellen of de in opzet bepaalde maatregelen in de praktijk ook bestaan;
- Het toetsen van de werking van die maatregelen over het eerste halfjaar 2021 dan wel het verrichten van gegevensgerichte werkzaamheden in relatie tot de beheersdoelstelling(en) indien testwerkzaamheden op basis van de uitkomsten met betrekking tot de opzet en/of het bestaan van maatregelen niet mogelijk blijken.

De testwerkzaamheden en eventuele gegevensgerichte werkzaamheden met betrekking tot het tweede halfjaar 2021 worden op een later moment uitgevoerd.

De uitkomsten van deze werkzaamheden worden eveneens op een later moment gerapporteerd en gecommuniceerd.

In deze managementletter rapporteren wij enerzijds onze bevindingen ten aanzien van de opzet en het bestaan van de key controls, waaronder inbegrepen de application controls en de GITC. Anderzijds rapporteren wij ook op basis van de uitkomsten met betrekking tot de opzet en het bestaan van de key controls de vervolgwerkzaamheden die ons inziens nodig zijn om uiteindelijk te kunnen oordelen of risico's bij processen voldoende worden beheerst ten einde de beheersdoelstellingen te behalen. Per key control wordt expliciet inzichtelijk gemaakt of dit systeemgerichte- dan wel gegevensgerichte werkzaamheden betreffen en wat de uitkomsten van deze uitgevoerde werkzaamheden met betrekking tot het eerste halfjaar 2021 zijn.

Daar waar aanvullende gegevensgerichte werkzaamheden nodig blijken – dat wil zeggen dat het werkzaamheden betreffen waarmee in de voorlopige controle-aanpak, die tijdens het accountants- en controllersoverleg is gepresenteerd, geen rekening is gehouden – maken wij dit expliciet inzichtelijk.

Wij benadrukken dat bij het bepalen (en uitvoeren over het eerste halfjaar 2021) van deze werkzaamheden rekening is gehouden met het feit dat de general IT controls randvoorwaardelijk zijn om te kunnen steunen op de application controls. De effectieve werking van de application controls is met andere woorden afhankelijk van de effectieve werking van de general IT controls.

Wij rapporteren in deze managementletter niet over de betrouwbaarheid 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. Omdat het tussentijds onderzoek gericht is op het verkrijgen van inzicht in de beheersmaatregelen en er geen formele beheersing rond Cognos is ingericht, hebben wij in het kader van het tussentijds onderzoek geen werkzaamheden uitgevoerd ten aanzien van deze rapportages.

Servicepunt71 heeft de volgende rapporten, op basis van gebruik door de deelnemers en nadere afstemming met de klantorganisaties, geïdentificeerd:

| Nr. | Cognos rapportage                                            | Applicatie bronadministratie | Aggregatieniveau               |
|-----|--------------------------------------------------------------|------------------------------|--------------------------------|
| 1.  | Balans                                                       | Decade                       | Grootboek                      |
| 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                      |
| 6.  | Boeking per grootboek                                        | Decade                       | Grootboek                      |
| 7.  | Boeking per kostenplaats                                     | Decade                       | Kostenplaats                   |
| 8.  | Inkoopfacturen met boekingen en verplichtingen (versie 2019) | Decade                       | Excel specificatie             |

Wij zullen per jaareinde de aansluiting van deze rapportages op de bronsystemen éénmalig vaststellen (op het rapportagemoment en na afsluiten van de administraties). Over de uitkomsten van deze werkzaamheden zullen wij in het assurance-rapport door middel van een aparte bijlage verslag doen.

Tot slot wijzen wij u erop dat een managementletter van nature kritisch van aard is, omdat deze zich richt op te verbeteren aspecten binnen uw organisatie en het bieden van handvaten daarbij.

### 3. Bevindingen tussentijds onderzoek

# 3. Bevindingen tussentijds onderzoek

## 3.1 Key controls benaderd vanuit het COSO-model

Voordat wij in gaan op het CFW 2021 en de bevindingen per proces op hoofdlijnen, lichten wij beknopt toe wat wij onder een key control verstaan. Hierbij baseren wij ons op het COSO-model, dat binnen de auditpraktijk een veel gebruikt raamwerk op het gebied van risicomanagement is.

Elke organisatie heeft doelstellingen. Deze kunnen grofweg in vier categorieën ingedeeld worden: behalen van strategische doelstellingen, effectieve en efficiënte bedrijfsprocessen, betrouwbare (financiële) informatievoorziening en naleving van wet- en regelgeving.

Externe en interne risico's kunnen het behalen van deze doelstellingen in gevaar brengen. Om die reden is een adequate beheersing van die risico's nodig. Daarvoor moeten in de processen van de organisatie beheersmaatregelen worden opgezet en uitgevoerd die de geïdentificeerde risico's mitigeren. *Alleen de beheersmaatregelen die écht noodzakelijk zijn om een beheerste procesgang te garanderen, zijn key controls.*

Deze key controls borgen dat risico's die het behalen van de geformuleerde beheersdoelstellingen per proces in gevaar brengen, voldoende worden gemitigeerd. De beheersdoelstellingen bij Servicepunt71 hebben hoofdzakelijk betrekking op een betrouwbare informatievoorziening en naleving van wet- en regelgeving met betrekking tot de financiële verantwoordingen van de deelnemende klantorganisaties.

## 3.2 Het CFW 20201

Wij maken ten behoeve van onze werkzaamheden rondom de opzet en het bestaan van de key controls gebruik van het bestaande CFW. Voor het actuele CFW verwijzen wij naar Bijlage 4.

Het CFW 2021 (d.d. 16 juni 2021) is, op enkele beperkte tekstuele wijzigingen na, nagenoeg gelijk gebleven aan dat van 2020.

Een belangrijke verbetering die wij in het CFW 2021 hebben geconstateerd heeft betrekking op de formulering van GITC. Wel vragen wij nog uw aandacht voor de invulling van deze “nieuwe” general IT controls, deze was tijdens ons tussentijds onderzoek nog niet in alle gevallen afgerond waardoor de betreffende controls voor ons niet toetsbaar waren.

## 3.3 Belangrijkste risico's

Bij onze beoordeling van de opzet van de key controls zijn wij primair uitgegaan van vier risico's (met betrekking tot de financiële verantwoordingen) die het behalen van de beheersdoelstellingen in gevaar kunnen brengen:

1. *Rechtmatigheid*: Risico dat externe wet- en regelgeving en intern beleid niet worden nageleefd.
2. *Volledigheid*: Risico dat passiva en opbrengsten niet volledig zijn verantwoord.
3. *Nauwkeurigheid*: Risico dat activa en kosten niet juist zijn verantwoord.
4. *Tijdigheid*: Risico dat mutaties in de financiële administratie niet tijdig worden doorgevoerd.

Indien wij bevindingen bij de opzet en/of het bestaan van de key controls hebben, worden deze hierna per proces op hoofdlijnen weergegeven. Voor de detailbevindingen per proces (per key control) verwijzen wij naar Bijlage 1.

### **3.4 Bevindingen per proces op hoofdlijnen**

In deze paragraaf rapporteren wij op hoofdlijnen de belangrijkste bevindingen per proces, specifiek gericht op het eerste halfjaar 2021. Wij sluiten de paragraaf af met een overzicht van de restrisico's per proces.

Het doel van deze opzet is om in de managementletter een onderscheid te maken tussen enerzijds bevindingen die nieuw zijn in 2021 en anderzijds bevindingen die ook in 2020 (en eventueel 2019) zijn gerapporteerd, maar eveneens van toepassing zijn op 2021.

Voor een overzicht van de detailbevindingen verwijzen wij naar Bijlage 1. Voor de bevindingen bij de GITC in het CFW, wordt naar Bijlage 2 verwezen.

Tot slot maken wij in Bijlage 3 inzichtelijk of en in hoeverre gedane aanbevelingen in de managementletter 2020 zijn opgevolgd, voor zo ver deze relevant zijn gelet op de scope van de assurance-opdracht 2021.

#### **3.4.1 Rekeningschema Decade**

Wij verwijzen naar de tabel aan het einde van deze paragraaf.

#### **3.4.2 Crediteurenbeheer**

Wij verwijzen naar de tabel aan het einde van deze paragraaf.

#### **3.4.3 Betalingsverkeer**

##### *Analyse niet toewijsbare betalingen (KC6)*

Wij hebben vastgesteld dat de maandelijkse controles uit het eerste kwartaal 2021 niet in Eqili zijn vastgelegd in verband met de drukte rondom de opstelling van de diverse jaarrekeningen. Pas vanaf de analyse van april 2021 vindt vastlegging in Eqili plaats. Dit heeft tot gevolg dat er geen vier-ogenprincipe (uitvoering versus review) wordt toegepast op de maandelijkse controles uit het eerste kwartaal 2021. Aangezien de uitvoerende medewerker niet geheel zelfstandig bankbetalingen kan verrichten én geen rechten heeft om mutaties in crediteurenstamgegevens te verwerken, achten wij het restrisico nihil. Immers, door de van toepassing zijnde functiescheidingen en vier-ogenprincipes in het betalingsproces, is er bij de analyse geen sprake van zelfcontrole.

##### *Analyse dubbele betalingen (KC8)*

De analyse op dubbele betalingen wordt in beginsel adequaat uitgevoerd. Wij hebben kunnen vaststellen dat bij de uitvoering van de analyse het vier-ogenprincipe is toegepast. Echter kan niet worden vastgesteld welke werkzaamheden de reviewer exact heeft uitgevoerd en op basis van welke motivatie deze functionaris de uitgevoerde analyse heeft goedgekeurd. Wij bevelen u aan om in het vervolg expliciet door de reviewer vast te laten leggen welke werkzaamheden bij de review op de uitgevoerde analyse worden uitgevoerd en wat de conclusie hieromtrent is.

Tot slot zijn in de analyse op dubbele betalingen – in overeenstemming met het interne beleid – facturen < EUR 1.000 niet betrokken. Wij adviseren om deze stroom periodiek te monitoren op basis van omvang en op basis daarvan te beoordelen of aanvullende beheersingsmaatregelen nodig zijn.

Tot slot verwijzen wij eveneens naar de tabel aan het einde van deze paragraaf.

#### **3.4.4 Purchase 2 Pay (P2P)**

Wij verwijzen naar de tabel aan het einde van deze paragraaf.

#### **3.4.5 Personele lasten**

##### *Volledigheid rubriekcodes bij steekproef op handmatige mutaties (KC7)*

Handelingen die in YouForce plaatsvinden, kunnen worden overschreden in Beaufort. De rechten voor de salarisadministratie kunnen namelijk onvoldoende worden afgeschermd. Servicepunt71 voert daarom maandelijks een steekproef uit op handmatige mutaties in Beaufort.

In het eerste halfjaar 2021 heeft Servicepunt71 een aanpassing doorgevoerd in haar eigen controleproces om te waarborgen dat alle rubriekcodes (code met betrekking tot het type handmatige mutatie) worden betrokken in de steekproef op handmatige mutaties in Beaufort. Tijdens onze controle hebben wij namelijk geconstateerd dat in eerste instantie niet alle rubriekcodes zijn meegenomen in de steekproef. Servicepunt71 heeft dit opgelost door een aanvullende steekproef uit te voeren over het eerste halfjaar 2021 waarin de ontbrekende codes wel zijn meegenomen. Deze aanvullende steekproef hebben wij betrokken in onze testwerkzaamheden. Servicepunt71 heeft aangegeven dat de volledigheid van de rubriekcodes structureel geborgd is in de maandelijkse steekproeven van het tweede halfjaar 2021.

##### *Volledigheid lijstwerk ten behoeve van tweedelijns steekproeven*

Met ingang van 2021 kunnen kwaliteitsmedewerkers zelfstandig de relevante rapportages uit Beaufort exporteren ten behoeve van de tweedelijns steekproeven. Verder is een proces ingericht waarbij wijzigingen in de

rapportages uitsluitend op voordracht van kwaliteitsmedewerkers door functioneel beheer worden doorgevoerd. Hiermee wordt voorkomen dat tussentijds ongewenste wijzigingen in de rapportages worden doorgevoerd, wat bijdraagt aan het borgen van de volledigheid van het lijstwerk.

Tot slot verwijzen wij eveneens naar de tabel aan het einde van deze paragraaf.

#### **3.4.6 GITC**

In het nieuwe control framework zijn periodieke controles ingericht om na te gaan in hoeverre de toegewezen rechten aan gebruikers nog actueel zijn. Voor Decade en Proquiro geldt echter dat deze controle gedurende het afgelopen halfjaar niet consequent is uitgevoerd.

Daarnaast is een controle toegevoegd om vast te stellen in hoeverre de wachtwoordinstellingen van de diverse applicaties voldoen aan de eisen die beleidsmatig gesteld worden aan authenticatiemechanismen. Deze controle is voor geen van de applicaties in scope nog uitgevoerd gedurende het afgelopen half jaar.

Verder hebben wij vernomen dat er geen wijziging is geweest in de toekenning van rechten van financieel applicatiespecialisten om rechtstreekse mutaties uit te voeren op de Decade database. Wij achten dit een onwenselijke toekenning van deze rechten doordat het ervoor zorgt dat diverse controls, die specifiek zijn gericht op de beheersing op (hoge) rechten, omzeild kunnen worden.

Tot slot geldt voor een aantal beheersingsmaatregelen, met name op het gebied van back-up en recovery en wijzigingsbeheer, dat wij nog niet hebben kunnen vaststellen dat deze ingericht zijn geweest in dit controlejaar omdat de uitvoering zich nog niet heeft voorgedaan. Wij zullen over de werkzaamheid van deze maatregelen daarom pas na afloop van het controlejaar rapporteren.

Tot slot is er in het bijzonder aandacht nodig voor de overgang naar Beaufort SaaS. Hoewel Servicepunt71 controles heeft uitgevoerd om vast te stellen dat deze overgang goed verlopen is, ontbreekt het aan een officiële decharge of akkoord voor in gebruik nemen van de applicatie. Dit terwijl wij begrepen hebben dat de applicatie in maart 2021 in gebruik genomen is.

#### ***3.4.7 Overzicht van restrisico's per proces***

In de tabel op de volgende pagina hebben wij per proces inzichtelijk gemaakt welke restrisico's wij identificeren en welke eventuele (aanvullende) werkzaamheden hieruit voortvloeien.

| Proces                   | Bevinding en restrisico                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | (Aanvullende) werkzaamheden                                                                                                                                                                                        |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Rekeningschema Decade | <p><b>KC2</b> Twee keer per jaar wordt achteraf en integraal vastgesteld dat mutaties die van invloed zijn op een budgethouder in het rekeningschema, conform mandaatregisters / budgethoudersregelingen van de betreffende klantorganisaties zijn. Met deze key control wordt echter niet het risico ondervangen dat mutaties volledig worden doorgevoerd, omdat het een analyse op totaalniveau is en niet op kostenplaatsniveau.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>Per jaareinde zullen wij vaststellen dat er geen kostenplaatsen aanwezig zijn waaraan geen budgethouder gekoppeld is, maar waar wel op is geboekt.</p>                                                          |
|                          | <p><b>KC3</b> Binnen dit proces wordt (in opzet) een nieuw aan te maken of te wijzigen kostenplaats door de financieel specialist vooraf gecontroleerd op een aantal aspecten. Wij hebben echter vastgesteld dat deze preventieve controles niet structureel zichtbaar worden gemaakt door de financieel specialist.</p> <p>Verder wordt de mutatie uiteindelijk doorgevoerd door een andere functionaris in Decade (medewerker FIS). Wij benadrukken de noodzaak om achteraf vast te stellen dat een gecontroleerde mutatie daadwerkelijk conform aanlevering / verzoek in het bronsysteem (Decade) is verwerkt. Deze aansluiting wordt op dit moment niet gemaakt. Wij bevelen u aan om dit te doen en gestructureerd inzichtelijk te maken.</p>                                                                                                                            | <p>Wij voeren een gegevensgerichte steekproef uit op nieuw aangemaakte / gewijzigde kostenplaatsen in 2021.</p>                                                                                                    |
| 2. Crediteurenbeheer     | <p><b>KC1b / KC2</b> Mutaties in crediteurenstamgegevens dienen op basis van voldoende betrouwbare documentatie te worden doorgevoerd. Binnen Servicepunt71 wordt hiervoor een mail / brief van de crediteur of een factuur (zonder sticker) als norm gehanteerd; dit onderschrijven wij mits de authenticiteit van deze stukken voldoende kan worden vastgesteld. Gebruikte documentatie ter invoer / controle van mutaties wordt bijgevoegd in de workflow. Voor een aantal mutaties hebben wij geconstateerd dat de gebruikte brondocumentatie vanuit controleperspectief ontoereikend is (bijvoorbeeld interne betalingsopdrachten vanuit klantorganisaties of interne mailwisselingen met bankgegevens zonder nadere onderbouwing). Hierdoor bestaat het risico dat mutaties worden doorgevoerd waarbij de juistheid van de bankrekening onvoldoende is vastgesteld.</p> | <p>Wij voeren gegevensgerichte werkzaamheden uit op posten uit de derdelijns steekproef van team AO/IC die in eerste instantie onderbouwd zijn door vanuit controleperspectief ontoereikende brondocumentatie.</p> |

| Proces              | Bevinding en restrisico                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (Aanvullende) werkzaamheden                                                                                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Betalingsverkeer | <p><b>KC7</b> Periodiek worden betaalopdrachten voor handmatige betalingen of betalingen uit subadministraties (bijvoorbeeld uitkeringen of salarissen) aangeleverd bij SP71. Hierbij wordt gecontroleerd of de juiste autorisatie – in de meeste gevallen van een budgethouder – is afgegeven voor het verrichten van de betaling. Er zijn lijsten beschikbaar die voor de controle op deze autorisatie (kunnen) worden gebruikt. Wij hebben echter vastgesteld dat deze niet in alle gevallen volledig / actueel zijn. Hierdoor bestaat het risico dat de autorisatie niet (meer) op het juiste niveau wordt afgegeven. Wij bevelen u aan om deze bij te werken en bij te houden.</p>                                                                                                                                                                             | N.v.t.                                                                                                                                                                                                                                                |
|                     | <p>Ten aanzien van het risico op onrechtmatige betalingen als gevolg van automatische incasso's zijn, conform de bevinding uit eerdere jaren, geen specifieke maatregelen getroffen. De analyses op niet toewijsbare betalingen en dubbele betalingen mitigeren dit risico deels. In combinatie met de gegevensgerichte steekproef op inkoopfacturen die de individuele accountants van de klantorganisaties uitvoeren, wordt het restrisico voldoende gemitigeerd. Wij bevelen u aan om periodiek zichtbaar vast te stellen dat automatische incasso's zijn afgegeven door daartoe bevoegde functionarissen volgens mandaatregelingen of vergelijkbare besluiten.</p>                                                                                                                                                                                              | N.v.t.                                                                                                                                                                                                                                                |
| 4. Purchase2Pay     | <p><b>KC2</b> De prestatiebeoordeling wordt in Proquro afgegeven. De prestatiebeoordelaar van de klantorganisatie is verantwoordelijk voor het afgeven van de prestatieverklaring (bij facturen zonder order valt deze stap samen met het akkoord van de budgethouder) en het onderbouwen daarvan. Het is niet verplicht om de prestatiebeoordeling met documentatie te onderbouwen. Dit wordt ook niet door het systeem afgedwongen. Omdat wij niet kunnen vaststellen dat ten tijde van factuurautorisatie een (zichtbare) onderbouwing van de prestatielevering heeft plaatsgevonden, is het niet mogelijk om een systeemgerichte controle uit te voeren. Op den duur wordt overigens wel een (beleidsmatige) ondergrens ingesteld voor de onderbouwing van de prestatielevering met documentatie; deze zal echter niet systeemtechnisch worden afgedwongen.</p> | <p>N.v.t.</p> <p>Conform afspraak met Servicepunt71 zijn onze werkzaamheden met betrekking tot de beoordeling van de prestatielevering in 2021 uitsluitend beperkt tot het beoordelen van de opzet en het bestaan van de betreffende key control.</p> |

| Proces              | Bevinding en restrisico                                                                                                                                                                                                                                                                                                                                                  | (Aanvullende) werkzaamheden                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 5. Personele lasten | <b>KC1</b> Jaarlijks vindt een controle plaats op de belangrijkste parameters die door RAET worden ingevoerd. Deze percentages zijn muteerbaar / te overschrijven door medewerkers salarisadministratie (SA). Hierdoor bestaat het risico dat percentages gedurende het jaar ten onrechte worden gewijzigd, wat kan leiden tot onrechtmatigheden in de personeelslasten. | Per jaareinde stellen wij vast of percentages zijn gewijzigd en of hiervoor adequate onderbouwing aanwezig is. |

## **Bijlagen**

### **Bijlage 1: Detailbevindingen tussentijds onderzoek**

# Leeswijzer bij Bijlage 1

Voor een goed begrip van de detailbevindingen per proces die in deze bijlage 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 "Vervolgwerkzaamheden"

Vervolgwerkzaamheden zijn de werkzaamheden die plaatsvinden nadat opzet en bestaan zijn vastgesteld. Dit kunnen systeemgerichte- of gegevensgerichte werkzaamheden zijn, afhankelijk van de uitkomsten met betrekking tot opzet en bestaan. In sommige gevallen blijkt dat aanvullende gegevensgerichte werkzaamheden nodig zijn ten opzichte van de voorlopige controle-aanpak. Dit is als volgt aangegeven: (A).

## Legenda "Opzet / Bestaan"

-  Bestaan vastgesteld
-  Bestaan vastgesteld, dekt risico niet af
-  Bestaan niet vastgesteld
-  Bestaan nog niet vast te stellen

## Legenda "Prioriteit"

- L = laag
- M = midden
- H = hoog

## Legenda "Uitkomsten vervolgwerkzaamheden 1<sup>e</sup> halfjaar 2021"

Deze uitkomsten hebben betrekking op de vervolgwerkzaamheden met betrekking tot het 1<sup>e</sup> halfjaar 2021. Deze kunnen zowel systeem- als gegevensgericht van aard zijn.

Als de werking van maatregelen effectief is, dan betekent dit dat de beheersdoelstelling is gerealiseerd. Als er geen bevindingen volgen uit de gegevensgerichte werkzaamheden, dan betekent dit dat het restrisico in relatie tot de beheersdoelstelling gemitigeerd is.

# 1. Rekeningschema Decade

| Nr. | Key control                                | Beheersdoelstelling                                                                                                                                                                                                             | Type | Opzet / Bestaan                                                                      | Bevinding                                                                                                                                                                                                                                                   | Prioriteit | Vervolgwerkzaamheden                                                                                                                                                                                                                                           | Uitkomsten<br>vervolgwerkzaamheden<br>1 <sup>e</sup> halfjaar 2021 |
|-----|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| 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  |    | We hebben het bestaan van deze maatregel nog niet kunnen vaststellen, omdat de rapportage begin 2022 volgt.                                                                                                                                                 | -          | Maatregel begin 2022 toetsen.                                                                                                                                                                                                                                  | -                                                                  |
| 2.  | Periodieke controle mutaties budgethouders | Rechtmatige toekenning van rechten/bevoegdheden, conform mandaatregeling                                                                                                                                                        | IDM  |  | De maatregel dekt in opzet/bestaan het risico af dat onrechtmatige toekenning van budgethoudersrechten bij kostenplaatsen plaatsvindt. Echter blijft het risico bestaan dat mutaties m.b.t. budgethouders in het rekeningschema onvolledig worden verwerkt. | -          | <p>Systeemgericht werking vaststellen (1)</p> <p>(A) Januari 2022: Gegevensgericht op basis van een uitdraai van het rekeningschema vaststellen dat er geen sprake is van kostenplaatsen zonder budgethouder waarop wordt geboekt (volledigheid mutaties).</p> | Werking effectief                                                  |

# 1. Rekeningschema Decade

| Nr. | Key control                                                                    | Beheersdoelstelling                                                                                                                                                                                                                                                                                                    | Type | Opzet / Bestaan                                                                      | Bevinding                                                                                                                                                                                                                                                                                                                                       | Prioriteit | Vervolgwerkzaamheden                                                                      | Uitkomsten vervolgwerkzaamheden 1 <sup>e</sup> halfjaar 2021                    |
|-----|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 3.  | Toets bij aanlevering nieuw aan te maken kostenplaats / wijziging budgethouder | <p>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</p> <p>Rechtmatige toekenning van rechten/bevoegdheden, conform mandaatregeling</p> | IDM  |    | <p>Bestaan van de maatregel is niet vastgesteld, omdat de controle van de financieel specialist niet zichtbaar wordt vastgelegd.</p> <p>Daarnaast is de maatregel in opzet niet toereikend. De mutatie wordt namelijk door de applicatiebeheerder doorgevoerd en de juistheid van de doorgevoerde mutatie in Decade wordt niet vastgesteld.</p> | M          | Gegevensgerichte steekproef op nieuw aangemaakte / gewijzigde kostenplaatsen in 2021 (60) | Geen restrisico t.a.v. beheersdoelstelling*                                     |
| 4.  | Geen verwijdering dimensie                                                     | <p>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</p>                                                                                 | AP   |  | -                                                                                                                                                                                                                                                                                                                                               | -          | Werking vaststellen (afhankelijk van GITC, onderdeel change management)                   | In 1 <sup>e</sup> halfjaar geen uitzonderingen in relevante GITC geconstateerd. |

\* Met betrekking tot de koppeling van de kostenplaats aan het IV3-taakveld en het programma uit de begroting, is door ons een plausibiliteitscontrole uitgevoerd. Dat wil zeggen dat wij hebben gekeken of de koppeling logisch is. Er is nadrukkelijk geen diepgaand onderzoek naar de juistheid van de gekozen koppeling uitgevoerd.

## 2. Crediteurenbeheer

| Nr. | Key control                         | Beheersdoelstelling                                                                                                        | Type | Opzet / Bestaan                                                                      | Bevinding                                                                                                                                                                                                                                                                                                                                                                                                                                    | Prioriteit | Vervolgwerkzaamheden                                                    | Uitkomsten vervolgwerkzaamheden 1 <sup>e</sup> halfjaar 2021                    |
|-----|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 1A. | Vier-ogenprincipe Decade            | Adequaat en getrouw beheer (integer en consistent) van relatiestamgegevens van crediteuren (NAW, KVK, BRP en bankgegevens) | AP   |    | -                                                                                                                                                                                                                                                                                                                                                                                                                                            | -          | Werking vaststellen (afhankelijk van GITC, onderdeel change management) | In 1 <sup>e</sup> halfjaar geen uitzonderingen in relevante GITC geconstateerd. |
| 1B. | Controle bij wijziging stamgegevens |                                                                                                                            | IDM  |    | Bestaan van de maatregel is vastgesteld. Echter hebben wij vastgesteld op basis van de opgenomen documentatie in de workflow dat niet in alle gevallen een wijziging wordt doorgevoerd op basis van documentatie die volgens de richtlijn van SP71 (bron: procesbeschrijving) kwalificeert als 'voldoende betrouwbaar', dat wil zeggen dat er minimaal sprake moet zijn van een mail/brief van de crediteur of een factuur (zonder sticker). | H          | Geen. Het risico wordt ondervangen d.m.v. de werkzaamheden bij KC2.     | -                                                                               |
| 2.  | Steekproef gewijzigde crediteuren   |                                                                                                                            | M    |  | Bestaan van de maatregel is vastgesteld, maar deze dekt het risico onvoldoende*.                                                                                                                                                                                                                                                                                                                                                             | M          | (A) Gegevensgerichte controle op onvoldoende onderbouwde posten         | Geen restrisico t.a.v. beheersdoelstelling                                      |

\* Met betrekking tot de kwaliteit van de informatie constateren wij dat ook op basis van intern mailverkeer / opdrachten van klantorganisaties mutaties worden verwerkt. In de managementletter 2020 hebben wij reeds aangegeven dat interne mailwisselingen en interne betalingsopdrachten met bankgegevens vanuit controleperspectief ontoereikend zijn om de juistheid van nieuwe / gewijzigde bankrekeningen vast te stellen. Net als vorig jaar, verrichten wij om deze reden (aanvullende) gegevensgerichte werkzaamheden met betrekking tot KC2.

### 3. Betalingsverkeer

| Nr. | Key control                                         | Beheersdoelstelling                                                                    | Type | Opzet / Bestaan | Bevinding                                                                                                                                                                                                                                                                                                                                                                             | Prioriteit | Vervolgwerkzaamheden                                                              | Uitkomsten vervolgwerkzaamheden 1 <sup>e</sup> halfjaar 2021                    |
|-----|-----------------------------------------------------|----------------------------------------------------------------------------------------|------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 3.  | Funcitiescheiding betaalproces                      | Het juist, tijdig, volledig (getrouw) en rechtmatig verrichten van betalingen          | AT   | ●               | -                                                                                                                                                                                                                                                                                                                                                                                     | -          | Werking vaststellen (afhankelijk van GITC, onderdeel autorisaties bankapplicatie) | In 1 <sup>e</sup> halfjaar geen uitzonderingen in relevante GITC geconstateerd. |
| 4.  | Betaalbestand met goedgekeurde facturen             |                                                                                        | AP   | ●               | -                                                                                                                                                                                                                                                                                                                                                                                     | -          | Werking vaststellen (afhankelijk van GITC, onderdeel change management)           | In 1 <sup>e</sup> halfjaar geen uitzonderingen in relevante GITC geconstateerd. |
| 5.  | Controle betaalbatch door tweede handtekeningzetter |                                                                                        | IDM  | ●               | -                                                                                                                                                                                                                                                                                                                                                                                     | -          | Systeemgericht werking vaststellen (25)                                           | Werking effectief*                                                              |
| 6.  | Periodieke controle op niet toewijsbare betalingen  | Het juist, tijdig en volledig (getrouw) registreren van betalingen in de administratie | IDM  | ●               | De maandelijkse controles uit het eerste kwartaal 2021, zijn niet vastgelegd in Eqili. Daardoor is ook geen vier-ogenprincipe toegepast (uitvoering versus review). Gelet op het feit dat de uitvoerende medewerker niet geheel zelfstandig bankbetalingen kan verrichten én geen rechten heeft om mutaties in crediteurenstamgegevens te verwerken, achten wij het restrisico nihil. | L          | Systeemgericht werking vaststellen (2)                                            | Werking effectief                                                               |

\* Bij salarisbatches wordt gebruik gemaakt van een SHA-1 controlegetal dat niet overeenstemt met het SHA-1 controlegetal in de BNG. Dit controlegetal wordt namelijk alleen door RAET gebruikt voor overdracht van de batch naar de klant (SP71). Verderop in de keten kan dit getal dus ook niet worden gebruikt. De betaalbatch wordt in de BNG rechtstreeks klaargezet via Equens. Het bestand wordt niet handmatig klaargezet in BNG, waardoor het risico op aanpassing van de batch niet aanwezig is. In de BNG is voorts sprake van de gebruikelijke autorisatie (eerste en tweede handtekening). Er is vastgesteld dat het aantal posten in de betaalbatch en het totaalbedrag van de batch aansluit met de verrichte betaling.

### 3. Betalingsverkeer

| Nr. | Key control                                                                          | Beheersdoelstelling                                                                    | Type | Opzet / Bestaan | Bevinding                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Prioriteit | Vervolg-werkzaamheden                                                                                                                                                 | Uitkomsten vervolg-werkzaamheden 1 <sup>e</sup> halfjaar 2021                                              |
|-----|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| 7.  | Controle op bevoegdheid bij handmatige betalingen / betalingen uit subadministraties | Het juist, tijdig, volledig (getrouw) en rechtmatig verrichten van betalingen          | M    | ●               | De lijsten die worden gebruikt om vast te stellen of functionarissen geautoriseerd zijn tot het geven van de opdracht zijn niet in alle gevallen volledig / actueel. Wij bevelen u aan om deze bij te werken en bij te houden.                                                                                                                                                                                                                                                                                                                                                                           | M          | Systeemgericht werking vaststellen (25)                                                                                                                               | Werking effectief                                                                                          |
| 8.  | Periodieke controle op dubbele facturen                                              | Het juist, tijdig en volledig (getrouw) registreren van betalingen in de administratie | IDM  | ●               | <p>Wij hebben kunnen vaststellen dat bij de uitvoering van de analyse het vier-ogenprincipe is toegepast. Echter kan niet worden vastgesteld welke werkzaamheden de reviewer exact heeft uitgevoerd en op basis van welke motivatie deze functionaris de uitgevoerde analyse heeft goedgekeurd. Wij bevelen u aan om in het vervolg expliciet door de reviewer vast te laten leggen welke werkzaamheden bij de review op de uitgevoerde analyse worden uitgevoerd en wat de conclusie hieromtrent is.</p> <p>Verder is gebleken dat op facturen &lt; EUR 1.000 geen nadere analyse wordt uitgevoerd.</p> | M          | <p>Systeemgericht werking vaststellen (2)</p> <p>(A) Specifiek voor facturen &lt; EUR 1.000: Inzicht verkrijgen in de omvang van deze stroom per klantorganisatie</p> | <p>Werking effectief</p> <p>T.a.v. facturen &lt; EUR 1.000: Geen restrisico t.a.v. beheersdoelstelling</p> |

## 4. Purchase2Pay (P2P)

| Nr. | Key control                 | Beheersdoelstelling                                                            | Type | Opzet / Bestaan | Bevinding                                                                                                                                                                                                                                                                                                                                                       | Prioriteit | Vervolg-werkzaamheden                                                                                                                                                                    | Uitkomsten vervolg-werkzaamheden 1 <sup>e</sup> halfjaar 2021                           |
|-----|-----------------------------|--------------------------------------------------------------------------------|------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1.  | Autorisatie order / factuur | Conformiteit aan externe wet- en regelgeving alsook interne regelgeving/beleid | AT   | ●               | Bestaan van workflows vastgesteld. Er is echter een onvoldoende basis in GITC om de werking vast te kunnen stellen. Daarnaast vastgesteld dat facturen onder de EUR 25 in het geheel niet aan autorisatie onderhevig zijn doordat facturen maximaal EUR 25 mogen afwijken van de order waarde.                                                                  | M          | Uitvoering data-analyse per jaareinde                                                                                                                                                    | De authenticatie van accounts is voldoende geborgd voor het uitvoeren van data analyse. |
| 2.  | Prestatiebeoordeling        |                                                                                | IDM  | ●               | Bestaan van de maatregel is vastgesteld. Echter, net als vorig jaar, wordt door Proquro niet afgedwongen dat documentatie wordt toegevoegd bij het geven van akkoord voor de prestatielevering. Ook is tijdens de interviews aangegeven door betrokken functionarissen dat bij een groot deel van de facturen de prestatielevering niet nader wordt onderbouwd. | H          | Geen. Alleen het bestaan van deze key control wordt vastgesteld. De (gegevensgerichte) controle op inkoopfacturen maakt dit jaar onderdeel uit van de individuele accountants-controles. | N.v.t.                                                                                  |

## 4. Purchase2Pay (P2P)

| Nr. | Key control                | Beheersdoelstelling                                                                              | Type | Opzet / Bestaan | Bevinding                                                                                                           | Prioriteit | Vervolg-werkzaamheden                  | Uitkomsten vervolg-werkzaamheden 1 <sup>e</sup> halfjaar 2021                           |
|-----|----------------------------|--------------------------------------------------------------------------------------------------|------|-----------------|---------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------|-----------------------------------------------------------------------------------------|
| 3.  | Vier-ogenprincipe orders   | Conformiteit aan externe wet- en regelgeving alsook interne regelgeving/beleid                   | AT   | ●               | Bestaan van workflows vastgesteld. Er is echter een onvoldoende basis in GITC om de werking vast te kunnen stellen. | M          | Uitvoering data analyse per einde jaar | De authenticatie van accounts is voldoende geborgd voor het uitvoeren van data analyse. |
| 4.  | Vier-ogenprincipe facturen | Juiste en tijdige verantwoording lasten (juistheid inclusief rubricering, tijdigheid/afgrenzing) | AT   | ●               | Bestaan van workflows vastgesteld. Er is echter een onvoldoende basis in GITC om de werking vast te kunnen stellen. | M          | Uitvoering data analyse per einde jaar | De authenticatie van accounts is voldoende geborgd voor het uitvoeren van data analyse. |

## 5. Personele lasten

| Nr. | Key control                                         | Beheersdoelstelling                                                                                     | Type | Opzet / Bestaan | Bevinding                                                           | Prioriteit | Vervolg-werkzaamheden                                                                                                               | Uitkomsten vervolg-werkzaamheden 1 <sup>e</sup> halfjaar 2021                   |
|-----|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------|------|-----------------|---------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 1.  | Jaarlijkse controle op parameters RAET              | Juiste en tijdige verantwoording (incl. rubricering) van personeelslasten                               | M    | ●               | Percentages zijn muteerbaar / te overschrijven door medewerkers SA. | L          | Systeemgericht werking vaststellen (1)<br><br>Januari 2022: Vaststellen dat tussentijdse wijzigingen conform brondocumentatie zijn. | Werking effectief                                                               |
| 2.  | Goedkeuring mutaties in YouForce                    |                                                                                                         | AT   | ●               | -                                                                   | -          | Werking vaststellen (GITC: autorisatie-beheer en change management)                                                                 | In 1 <sup>e</sup> halfjaar geen uitzonderingen in relevante GITC geconstateerd. |
| 3.  | 2 <sup>e</sup> -lijns steekproef indiensttredingen  | Rechtmatige uitvoering proces conform wet- en regelgeving (extern en intern normenkader/toetsingskader) | IDM  | ●               | -                                                                   | -          | Systeemgericht werking vaststellen (2)*                                                                                             | Werking effectief                                                               |
| 4.  | 2 <sup>e</sup> -lijns steekproef uitdiensttredingen |                                                                                                         | IDM  | ●               | -                                                                   | -          | Systeemgericht werking vaststellen (2)                                                                                              | Werking effectief                                                               |
| 5.  | 2 <sup>e</sup> -lijns steekproef declaraties        |                                                                                                         | IDM  | ●               | -                                                                   | -          | Systeemgericht werking vaststellen (2)                                                                                              | Werking effectief                                                               |

\* Vanaf 2021 wordt er bij uitvoering van de steekproef volledig gesteund op de automatische berekening van het salaris en de verlofdagen in Beaufort. In het kader van onze controlewerkzaamheden zullen wij vaststellen of er gesteund kan worden op deze (configuratie-)berekening.

## 5. Personele lasten

| Nr. | Key control                                                    | Beheersdoelstelling                                                                                                                                                               | Type | Opzet / Bestaan | Bevinding                                                                                                                                                                                                                                                                                                                                                               | Prioriteit | Vervolgwerkzaamheden                                           | Uitkomsten vervolgwerkzaamheden 1 <sup>e</sup> halfjaar 2021 |
|-----|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------|--------------------------------------------------------------|
| 6.  | Controle op handmatig ingevoerde mutaties                      |                                                                                                                                                                                   | IDM  | ●               | -                                                                                                                                                                                                                                                                                                                                                                       | -          | Systeemgericht werking vaststellen (25), in combinatie met KC7 | Werking effectief                                            |
| 7.  | 2 <sup>e</sup> -lijns steekproef handmatig ingevoerde mutaties | Rechtmatige uitvoering proces conform wet- en regelgeving (extern en intern normenkader/toetsingskader)                                                                           | IDM  | ●               | Wij hebben vastgesteld dat de procedure gedurende 2021 is toegepast. Echter zijn in de steekproef eerste halfjaar 2021 in eerste instantie niet alle rubriekcodes (code m.b.t. het type handmatige mutatie) meegenomen. Servicepunt71 heeft daarom een aanvullende steekproef uitgevoerd over het eerste halfjaar 2021 waarin de ontbrekende codes wel zijn meegenomen. | L          | Systeemgericht werking vaststellen (2)                         | Werking effectief                                            |
| 8.  | Maandelijkse rondrekening                                      | Juiste en tijdige verantwoording (incl. rubricering) van personeelslasten<br><br>Volledigheid schulden (netto lonen, declaraties, afdrachten loonheffingen, pensioenpremies etc.) | IDM  | ●               | -                                                                                                                                                                                                                                                                                                                                                                       | -          | Systeemgericht werking vaststellen (2)                         | Werking effectief                                            |
| 9.  | Jaarlijkse beoordeling ISAE-3402-rapportage RAET               | <i>Draagt in principe bij aan alle beheersdoelstellingen van dit proces</i>                                                                                                       | M    | ●               | We hebben het bestaan van deze maatregel nog niet kunnen vaststellen, omdat de rapportage begin 2022 volgt.                                                                                                                                                                                                                                                             | -          | Maatregel begin 2022 toetsen.                                  | -                                                            |

## **Bijlagen**

### **Bijlage 2: Detailbevindingen bij GITC in het CFW**

## 6. General IT Controls Decade

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Beheersdoelstelling                                                                                                                                                        | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                                                                                                                                               |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | <p>Geen risico's geconstateerd op basis van beoordeling van het aanmaken, muteren en verwijderen van accounts in de applicatie.</p> <p>Aandachtspunt blijven de rechten van financieel applicatiespecialisten op de database.</p> |
| 2.  | <p>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).</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                    | Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico's geconstateerd op basis van beoordeling van het aanmaken, muteren en verwijderen van accounts in de applicatie.                                                                                                      |

## 6. General IT Controls Decade

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Beheersdoelstelling                                                                                                              | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 3.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico geconstateerd op basis van een beoordeling van de wachtwoordeisen die gelden voor de applicatie. |
| 4.  | <p>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.</p> <p>De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk</p>                            | Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure. |  | Maatregel is voor dit boekjaar nog niet uitgevoerd.                                                                                | -                                                                                                            |

## 6. General IT Controls Decade

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Beheersdoelstelling                                                                                                                                                                         | Opzet / Bestaan | Bevindingen eerste half jaar 2021                                              | Resultaat aanvullende werkzaamheden |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------------------------------------------------|-------------------------------------|
| 5.  | <p>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.</p> <p>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.</p> | <p>Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.</p> | ●               | Er zijn in het controlejaar nog geen wijzigingen in de applicatie doorgevoerd. | -                                   |
| 6.  | <p>Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier</p>                                   | ●               | Maatregel is voor dit boekjaar nog niet uitgevoerd.                            | -                                   |

## 6. General IT Controls Proquro

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Beheersdoelstelling                                                                                                                                                        | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                                          |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 1.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico's geconstateerd op basis van beoordeling van het aanmaken, muteren en verwijderen van accounts in de applicatie. |
| 2.  | <p>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).</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                    | Accountbeheer (ISMS 3.4) - De wijze waarop autorisaties voor applicaties worden toegekend, gewijzigd en ingetrokken voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico's geconstateerd op basis van beoordeling van het aanmaken, muteren en verwijderen van accounts in de applicatie. |

## 6. General IT Controls Proquro

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Beheersdoelstelling                                                                                                              | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 3.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico geconstateerd op basis van een beoordeling van de wachtwoordeisen die gelden voor de applicatie. |
| 4.  | <p>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.</p> <p>De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk</p>                            | Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure. |  | Maatregel is voor dit boekjaar nog niet uitgevoerd.                                                                                | -                                                                                                            |

## 6. General IT Controls Proquro

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Beheersdoelstelling                                                                                                                                                                         | Opzet / Bestaan | Bevindingen eerste half jaar 2021                   | Resultaat aanvullende werkzaamheden |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------------------------------------------|-------------------------------------|
| 5.  | <p>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.</p> <p>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.</p> | <p>Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.</p> | ●               | -                                                   | -                                   |
| 6.  | <p>Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier</p>                                   | ●               | Maatregel is voor dit boekjaar nog niet uitgevoerd. | -                                   |

## 6. General IT Controls YouForce

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Beheersdoelstelling                                                                                                                                                        | Opzet / Bestaan | Bevindingen eerste half jaar 2021 | Resultaat aanvullende werkzaamheden |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------------------------|-------------------------------------|
| 1.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | 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.  | <p>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).</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                    | 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                                                                                                              | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 3.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico geconstateerd op basis van een beoordeling van de wachtwoordeisen die gelden voor de applicatie. |
| 4.  | <p>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.</p> <p>De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk</p>                            | Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure. |  | Maatregel is voor dit boekjaar nog niet uitgevoerd.                                                                                | -                                                                                                            |

## 6. General IT Controls YouForce

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Beheersdoelstelling                                                                                                                                                                         | Opzet / Bestaan | Bevindingen eerste half jaar 2021                   | Resultaat aanvullende werkzaamheden |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------------------------------------------|-------------------------------------|
| 5.  | <p>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.</p> <p>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.</p> | <p>Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.</p> | ●               | -                                                   | -                                   |
| 6.  | <p>Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier</p>                                   | ●               | Maatregel is voor dit boekjaar nog niet uitgevoerd. | -                                   |

## 6. General IT Controls Beaufort

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Beheersdoelstelling                                                                                                                                                        | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021 | Resultaat aanvullende werkzaamheden |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------|
| 1.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | 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.  | <p>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).</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                    | 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                                                                                                              | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 3.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico geconstateerd op basis van een beoordeling van de wachtwoordeisen die gelden voor de applicatie. |
| 4.  | <p>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.</p> <p>De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk</p>                            | Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure. |  | Maatregel is voor dit boekjaar nog niet uitgevoerd.                                                                                | -                                                                                                            |

## 6. General IT Controls Beaufort

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Beheersdoelstelling                                                                                                                                                                         | Opzet / Bestaan                                                                      | Bevindingen eerste half jaar 2021                                                                                                                                                                                                         | Resultaat aanvullende werkzaamheden |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| 5.  | <p>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.</p> <p>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.</p> | <p>Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.</p> |   | <p>Aandachtspunt is de officiële decharge van het project om over te stappen op de SaaS versie van Beaufort. Deze had ten tijde van de interviews nog niet plaats gevonden, terwijl het systeem al ruim een half jaar in gebruik was.</p> | -                                   |
| 6.  | <p>Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>Leveranciers-managent (ISMS 8.3) - Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier</p>                                   |  | <p>Maatregel is voor dit boekjaar nog niet uitgevoerd.</p>                                                                                                                                                                                | -                                   |

## 6. General IT Controls TIM

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Beheersdoelstelling                                                                                                                                                        | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021 | Resultaat aanvullende werkzaamheden |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------|
| 1.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | 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.  | <p>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).</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                    | 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                                                                                                              | Opzet / Bestaan                                                                     | Bevindingen eerste half jaar 2021                                                                                                  | Resultaat aanvullende werkzaamheden                                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 3.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p> | Wachtwoordbeheer (ISMS 3.6) - Het wachtwoordenbeheer voor deze applicatie voldoet aan de eisen zoals gesteld in de normenkaders. |  | Wij hebben vernomen dat er binnen Servicepunt71 nog geen afspraken zijn gemaakt met betrekking tot het uitvoeren van de maatregel. | Geen risico geconstateerd op basis van een beoordeling van de wachtwoordeisen die gelden voor de applicatie. |
| 4.  | <p>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.</p> <p>De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk</p>                            | Back-up applicaties (ISMS 3.7) - Voor elke applicatie wordt volgens procedure een back-up gemaakt en er is een herstelprocedure. |  | Maatregel is voor dit boekjaar nog niet uitgevoerd.                                                                                | -                                                                                                            |

## 6. General IT Controls TIM

| Nr. | Key control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Beheersdoelstelling                                                                                                                                                                         | Opzet / Bestaan | Bevindingen eerste half jaar 2021                                              | Resultaat aanvullende werkzaamheden |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------------------------------------------------|-------------------------------------|
| 5.  | <p>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.</p> <p>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.</p> | <p>Applicatiewijzigingen testen (ISMS 3.12) - Wijzigingen worden pas in productie genomen na succesvolle test en acceptatie. Hierbij wordt de procedure voor wijzigingenbeheer gevolgd.</p> | ●               | Er zijn in het controlejaar nog geen wijzigingen in de applicatie doorgevoerd. | -                                   |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>Leveranciers-managent (ISMS 8.3)</p> <p>- Er wordt jaarlijks door een onafhankelijke partij zekerheid verschaft over de prestaties van de ICT-leverancier</p>                            | ●               | Maatregel is voor dit boekjaar nog niet uitgevoerd.                            | -                                   |

# **Bijlagen**

## **Bijlage 3: Opvolging aanbevelingen managementletter 2020**

## 1. Rekeningschema Decade

| Nr. | Aanbeveling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Status opvolging | Toelichting (reactie Servicepunt71)                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KC2 | <p>Twee keer per jaar wordt achteraf en integraal vastgesteld dat mutaties die van invloed zijn op een budgethouder in het rekeningschema, conform mandaatregisters / budgethoudersregelingen van de betreffende klantorganisaties zijn. Met deze key control wordt echter niet het risico ondervangen dat mutaties volledig worden doorgevoerd, omdat het een analyse op totaalniveau is en niet op kostenplaatsniveau. Wij bevelen u aan om niet alleen periodiek de rechtmatigheid van mutaties van budgethouders in het rekeningschema vast te stellen, maar ook de volledigheid, tijdigheid en juistheid.</p>                                                                                                                                                                                                                                                                                           | ●                | <p>Er vinden verschillende controles plaats, zowel tijdens het proces als achteraf. Hiermee wordt een groot deel van het risico op een foutieve verwerking afgedekt. Er blijft alleen een restrisico over voor het laatste stuk, de daadwerkelijke verwerking van de mutatie in Decade door FIS. Aangezien het hier gaat om een geautomatiseerde actie, het inlezen van een mutatiebestand, is dit restrisico in onze ogen nihil.</p> |
| KC3 | <p>Binnen dit proces wordt (in opzet) een nieuw aan te maken of te wijzigen kostenplaats door de financieel specialist gecontroleerd op een aantal aspecten. De mutatie wordt uiteindelijk doorgevoerd door een andere functionaris (medewerker FIS). Wij benadrukken de noodzaak om achteraf vast te stellen dat een gecontroleerde mutatie daadwerkelijk conform aanlevering/verzoek in het bronsysteem (Decade) is verwerkt. Deze aansluiting wordt op dit moment niet gemaakt. Wij bevelen u aan om dit te doen en gestructureerd inzichtelijk te maken.</p>                                                                                                                                                                                                                                                                                                                                             | ●                | <p>Er vinden verschillende controles plaats, zowel tijdens het proces als achteraf. Hiermee wordt een groot deel van het risico op een foutieve verwerking afgedekt. Er blijft alleen een restrisico over voor het laatste stuk, de daadwerkelijke verwerking van de mutatie in Decade door FIS. Aangezien het hier gaat om een geautomatiseerde actie, het inlezen van een bestand, is dit restrisico in onze ogen nihil.</p>        |
| KC4 | <p>Tot slot hebben wij vastgesteld dat de controle vooraf door de financieel specialist op de rechtmatige toekenning van budgethoudersrechten aan een nieuwe budgethouder bij een bestaande kostenplaats niet in alle gevallen zichtbaar wordt uitgevoerd. Normaliter wordt hiervoor een speciaal veld in het digitaal formulier gehanteerd waarop de wijziging van budgethouder inclusief de relevante autorisaties inzichtelijk zijn. Deze werkwijze wordt niet consistent gehanteerd, waardoor niet altijd de zichtbare controle door de financieel specialist inzichtelijk is. Daarnaast ontbreekt het hierdoor aan een (zichtbare) preventieve controle op dit soort mutaties binnen het proces. Wij bevelen u aan om deze werkwijze consistent te hanteren, zodat achteraf ook inzichtelijk kan worden gemaakt dat er een preventieve controle door de financieel specialist heeft plaatsgevonden.</p> | ●                | <p>Wij zullen de betreffende medewerkers erop wijzen om de werkwijze consistent te hanteren.</p>                                                                                                                                                                                                                                                                                                                                      |

## 2. Crediteurenbeheer

| Nr.          | Aanbeveling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Status opvolging                                                                    | Toelichting (reactie Servicepunt71)                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KC1<br>b / 2 | <p>Mutaties in crediteurenstamgegevens dienen op basis van voldoende betrouwbare documentatie te worden doorgevoerd. Binnen SP71 wordt hiervoor een mail/brief van de crediteur of een factuur (zonder sticker) als norm gehanteerd; dit onderschrijven wij mits de authenticiteit van deze stukken voldoende kan worden vastgesteld. Gebruikte documentatie ter invoer/controler van mutaties wordt bijgevoegd in de workflow. Voor een aantal mutaties hebben wij geconstateerd dat de gebruikte brondocumentatie ontoereikend is. Hierbij gaat het bijvoorbeeld om interne betalingsopdrachten vanuit klantorganisaties waarbij de opgegeven bankrekening niet nader onderbouwd is of interne mailwisselingen met bankgegevens zonder nadere onderbouwing. Hierdoor bestaat het risico dat mutaties worden doorgevoerd waarbij de juistheid van de bankrekening onvoldoende is vastgesteld. Wij bevelen u aan om te allen tijde mutaties in crediteurenstamgegevens door te voeren op basis van toereikende brondocumentatie. Dit betreft in ieder geval externe documentatie waarvan de authenticiteit voldoende kan worden vastgesteld.</p> |  | <p>Vooralsnog nemen we de aanbeveling niet over. Als naar aanleiding van een betaalopdracht, die goedgekeurd is door de verantwoordelijke budgethouder, een mutatie in het Crediteurenbestand wordt gemaakt, is de betaalopdracht voor ons het brondocument op basis waarvan de mutatie wordt uitgevoerd. Afhankelijk van de bevindingen in de gegevensgerichte steekproef (KC2) over het tweede halfjaar van 2020 zullen we ons standpunt voor 2021 opnieuw bezien.</p> |

## 3. Betalingsverkeer

| Nr. | Aanbeveling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Status opvolging                                                                      | Toelichting (reactie Servicepunt71)   |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------|
| KC7 | <p>Periodiek worden betaalopdrachten voor handmatige betalingen of betalingen uit subadministraties (bijvoorbeeld uitkeringen of salarissen) aangeleverd bij SP71. Hierbij wordt gecontroleerd of de juiste autorisatie – in de meeste gevallen van een budgethouder – is afgegeven voor het verrichten van de betaling. Er zijn lijsten beschikbaar die voor de controle op deze autorisatie (kunnen) worden gebruikt. Wij hebben echter vastgesteld dat deze niet in alle gevallen volledig/actueel zijn. Hierdoor bestaat het risico dat de autorisatie niet (meer) op het juiste niveau wordt afgegeven. Wij bevelen u aan om deze bij te werken en bij te houden.</p> |  | <p>Aanbeveling wordt overgenomen.</p> |

### 3. Betalingsverkeer

| Nr. | Aanbeveling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Status opvolging                                                                     | Toelichting (reactie Servicepunt71)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KC8 | <p>De verrichte analyse op dubbele betalingen is ontoereikend:</p> <ul style="list-style-type: none"> <li>Wij hebben niet kunnen vaststellen dat bij de uitvoering van de analyse het vierogenprincipe is toegepast.</li> <li>Daarnaast is de betrouwbaarheid van het gebruikte (Cognos-)lijstwerk niet aangetoond door dit aan te sluiten op de financiële administratie (Decade).</li> <li>Tot slot is niet expliciet inzichtelijk gemaakt welke criteria worden gebruikt om posten nader te onderzoeken en is ook niet expliciet inzichtelijk gemaakt wat de conclusie per onderzochte post is, welke vervolgacties al dan niet zijn genomen en wat de opvolging hiervan is geweest.</li> </ul> |   | <ol style="list-style-type: none"> <li>Het 4-ogenprincipe wordt nu gehanteerd; 1e medewerker doet zoekwerk naar aanleiding van het Cognosrapport. 2e medewerker controleert en keurt goed. Dit wordt vastgelegd in een excelsheet en in Eqili opgenomen.</li> <li>Decade kan geen rapportage dubbele betalingen draaien. Er is dus geen aansluiting mogelijk met het Cognosrapport. Het Cognosrapport geeft de facturen aan waarvan het bedrag meerdere malen voorkomt.</li> <li>Toetscriteria worden nu bij elke controle toegevoegd. De opvolging wordt per tabblad weergegeven.</li> </ol>                                                                                                 |
| -   | <p>Ten aanzien van het risico op onrechtmatige betalingen als gevolg van automatische incasso's zijn geen specifieke maatregelen getroffen. De analyses op niet toewijsbare betalingen en dubbele betalingen mitigeren dit risico deels. In combinatie met onze gegevensgerichte steekproef op inkoopfacturen wordt het restrisico voldoende gemitigeerd. Wij bevelen u aan om periodiek zichtbaar vast te stellen dat automatische incasso's zijn afgegeven door daartoe bevoegde functionarissen volgens mandaatregelingen of vergelijkbare besluiten.</p>                                                                                                                                       |  | <p>Deze aanbeveling is dezelfde als in 2019 maar nemen wij niet over. Wij proberen te voorkomen dat elders een onbevoegd akkoord wordt gegeven voor automatische incasso. Het opvragen van dergelijke stukken levert alleen een onbekende paraaf of handtekening op zonder dat te achterhalen is welke naam daarbij hoort. De factuur, horende bij deze automatische incasso's, zal daarom altijd de workflow van het inkoopproces doorlopen en akkoord bevonden moeten worden door de budgethouder. Indien louter sprake is van een automatische incasso (dus zónder bijbehorende factuur), dan zal de automatische afschrijving gestorneerd worden door de medewerker betalingsverkeer.</p> |

#### 4. Purchase2Pay

| Nr. | Aanbeveling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Status opvolging                                                                    | Toelichting (reactie Servicepunt71)                                                                                                                                                                                                                                                                                                                                       |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KC2 | De prestatiebeoordeling wordt in Proquro afgegeven. De prestatiebeoordelaar van de klantorganisatie is verantwoordelijk voor het afgeven van de prestatieverklaring (bij facturen zonder order valt deze stap samen met het akkoord van de budgethouder) en het onderbouwen daarvan. Het is niet verplicht om de prestatiebeoordeling met documentatie te onderbouwen. Dit wordt ook niet door het systeem afgedwongen. Omdat wij niet kunnen vaststellen dat ten tijde van factuurautorisatie een (zichtbare) onderbouwing van de prestatielevering heeft plaatsgevonden, is het niet mogelijk om een systeemgerichte controle uit te voeren. |  | Er vinden gesprekken plaats om een ondergrens in te stellen voor het onderbouwen van de prestatielevering met documentatie. Dit zal echter niet systeemtechnisch worden afgedwongen. Het is hierdoor aannemelijk dat de problematiek met betrekking tot het zichtbaar vaststellen van de prestatielevering ten tijde van factuurautorisatie en betaling zal voortbestaan. |

#### 6 t/m 10. General IT Controls (Decade, Beaufort, YouForce, TIM, Proquro)

| Nr. | Aanbeveling                                | Status opvolging                                                                      | Toelichting (reactie Servicepunt71)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----|--------------------------------------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KC2 | Zie Bijlage 2 in de managementletter 2020. |  | Er is een uitgebreid verbeterplan opgesteld om de bevindingen uit de IT-audit van Baker Tilly op te pakken. Dit verbeterplan beschrijft de werkzaamheden en activiteiten die nodig zijn om de benodigde controls te borgen in het CFW en de uitvoering in te richten van generieke, zelfstandige testen en controles binnen Servicepunt71. Hiertoe waren naar aanleiding van gesprekken met Baker Tilly al activiteiten opgestart, andere activiteiten volgen nu op de specifieke bevindingen zoals in de managementletter over het eerste halfjaar van 2020 zijn opgenomen. De activiteiten in het verbeterplan moeten nog geprioriteerd en zullen naar verwachting doorlopen tot en met 2022. |

## **Bijlagen**

### **Bijlage 4: Uitgebreide omschrijving key controls**

## 1. Rekeningschema Decade

| Nr. | Key control<br>verkorte omschrijving                                           | Key control<br>uitgebreide omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>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.<br>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<br><i>verkorte omschrijving</i> | Key control<br><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<br>verkorte omschrijving                                                 | Key control<br>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<br>verkorte omschrijving | Key control<br>uitgebreide omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Autorisatie order / factuur          | Facturen met order > €300,-:<br>De budgethouder autoriseert de order (> €300,-) in Proquro.<br><br>Facturen zonder order:<br>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.<br><br>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<br><i>verkorte omschrijving</i>         | Key control<br><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 <sup>e</sup> -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 <sup>e</sup> -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 <sup>e</sup> -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<br>verkorte omschrijving                           | Key control<br>uitgebreide omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.  | 2 <sup>e</sup> -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: <ul style="list-style-type: none"> <li>• Of betaalstaten, betaalopdrachten en de loonaangifte met elkaar aansluiten.</li> <li>• Of de saldi tussenrekeningen m.b.t. salarissen aflopen.</li> <li>• Of de SA aansluit op de FA.</li> </ul> |
| 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.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                      |
| 2.  | <p>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).</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                                                                                                         |
| 3.  | <p>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.</p> <p>De functioneel beheerder bereidt dit voor en de proces-/applicatie-eigenaar controleert en geeft akkoord. Dit wordt vastgelegd in TopDesk.</p>                                                                                                                                                                             |
| 4.  | <p>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.</p> <p>De functioneel beheerder legt dit vast en rapporteert aan de proces-/applicatie-eigenaar. Dit wordt vastgelegd in TopDesk</p>                                                                                                                                                                                                        |
| 5.  | <p>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.</p> <p>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.</p> |
| 6.  | <p>Elk jaar vraagt SP71 een Assurancerapport op bij de leverancier. SP71 beoordeelt het rapport en legt dit vast. Waar nodig worden aanvullende acties genomen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Contactgegevens

**drs. S. (Stefan) Turenhout RA**

Director

06 – 52 75 98 79

[s.turenhout@bakertilly.nl](mailto:s.turenhout@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