Assurance rapport
ISAE 3000d Type II

Uitgebracht aan:	Regionale Belasting Groep
Contactpersoon:	Michel Brouwer, Dick van Oostrom
Uitgebracht door:	Cuccibu B.V.
Onderzoeker(s):	Roel Harmsen, Timo Waars
Aftekende Auditor:	Patriek Nouwen
Datum:	02-02-2024
Rapportnummer:	202401PN007
Versie:	1.0
Status:	Definitief
Pagina's:	21

Assurance rapportage van de onafhankelijke auditor

Aan: de directie van Regionale Belasting Groep

Wij hebben onderzocht of de applicaties Key2Belastingen, Ortax gedurende het jaar 2023, de verslagperiode, aan het normenkader van de Regionale Belasting Groep voldaan hebben.

Ons oordeel

Naar ons oordeel, in alle van materieel belang zijnde aspecten:

1. Zijn de interne beheersingsmaatregelen die verband houden met de beheersingsdoelstelling in de verslagperiode op afdoende wijze opgezet om de beheersingsdoelstelling te bereiken;
2. Bestaan de interne beheersingsmaatregelen binnen de organisatie zoals beschreven in het toetsingskader gedurende de verslagperiode; en
3. Hebben met uitzondering van de hieronder genoemde normen/processen de getoetste interne beheersingsmaatregelen effectief gewerkt om de beheersingsdoelstelling te bereiken gedurende de verslagperiode.

De volgende normen/processen hebben niet effectief gewerkt gedurende de verslagperiode:

- Het uitdiensttredingsproces: Accounts zijn in meerdere gevallen te laat afgesloten. De controle doelstelling *“Toegang tot ICT-diensten en -middelen is adequaat afgeschermd. Pogingen tot ongeautoriseerde toegang tot ICT-middelen dienen tijdig te worden gedetecteerd.”* wordt daardoor niet behaald.
- De periodieke controle op autorisaties: Heeft één keer plaatsgevonden, terwijl de BIO één keer per half jaar voorschrijft. De doelstelling *“Toegang tot ICT-diensten en -middelen dient te worden beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers en beheerders.”* wordt daardoor niet behaald.
- Logging op wijzigingen in autorisaties en accounts is niet mogelijk. Dit is echter wel vereist als een van de onderdelen vanuit de norm. De doelstelling *“Acties en uitgevoerde activiteiten zijn in de applicatie herleidbaar.”* wordt daardoor niet geheel behaald.

De basis voor ons oordeel

Wij hebben onze opdracht uitgevoerd overeenkomstig Richtlijn 3000. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie ‘Verantwoordelijkheden van de auditor’.

Wij zijn onafhankelijk van en hebben de vereisten nageleefd van het NOREA Reglement gedragscode met betrekking tot integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

Het onderzoek omvat het uitvoeren van onderstaande:

1. Het verkrijgen van inzicht in de interne beheersing die relevant is voor het onderzoek, met als doel assurance werkzaamheden te selecteren die passend zijn in de omstandigheden;
2. Beoordeling van de interne beheersing die relevant is voor de applicaties Key2Belastingen en Ortax voor het jaar 2023.

Beperkingen van interne beheersingsmaatregelen

Interne beheersingsmaatregelen bij een organisatie kunnen, vanwege hun aard, niet alle fouten of omissies bij het verwerken van persoonsgegevens voorkomen of ontdekken, waaronder de mogelijkheid van menselijke fouten en het omzeilen van interne beheersingsmaatregelen.

Ons onderzoek heeft geen betrekking op toekomstige perioden. Derhalve kunnen wij niet uitsluiten dat zich in de toekomst gebeurtenissen voordoen die kunnen leiden tot een afwijking van het stelsel van maatregelen en procedures of kunnen leiden dat de beheersingsmaatregelen ontoereikend worden als gevolg van veranderingen in de omstandigheden.

Doeleinden assurance rapport en beoogde gebruikers

Onze schriftelijke rapportage is alleen bestemd voor Regionale Belasting Groep, haar auditor(s), en gemeenten Delft, Schiedam en Vlaardingen, aangezien anderen, die niet op de hoogte zijn van de precieze reikwijdte, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

De rapportage, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming.

Voor zover het Regionale Belasting Groep is toegestaan het rapport aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld.

Indien de producten van onze werkzaamheden aan derden ter beschikking worden gesteld, dient erop te worden gewezen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan het product kunnen worden ontleend. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

Verantwoordelijkheden van het bestuur van Regionale Belasting Groep

Het bestuur van Regionale Belasting Groep is verantwoordelijk voor:

1. Regionale Belasting Groep is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de verslagperiode;
2. Het identificeren van de risico's die een bedreiging vormen voor het bereiken van de beheersingsdoelstelling;
3. Het opstellen van interne beheersingsmaatregelen om de beheersingsdoelstelling te bereiken;
4. Het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om de beheersingsdoelstelling uit het normenkader te bereiken.

5. Het monitoren van interne beheersingsmaatregelen teneinde hun effectiviteit vast te stellen, tekortkomingen te identificeren en corrigerende acties te nemen.

Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel over de opzet en werking van interne beheersingsmaatregelen die verband houden met de beheersingsdoelstelling in overeenstemming met het toetsingskader.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële fouten, misbruik of fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing van NOREA toe en bijgevolg onderhouden een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

Ons onderzoek van de opzet en effectieve werking van interne beheersingsmaatregelen bestond onder andere uit:

- Het identificeren en inschatten van de risico's dat interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of effectief werken om de beheersingsdoelstelling te bereiken gedurende de verslagperiode als gevolg van fouten, misbruik of fraude;
- Risico's bepalen van assurance werkzaamheden voor het verkrijgen van assurance informatie die voldoende en geschikt is als basis voor ons oordeel;
- Het evalueren van de geschiktheid van de beheersingsdoelstelling en de geschiktheid van toetsingskader;
- Het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet van interne beheersingsmaatregelen om de beheersingsdoelstelling te bereiken;
- Het toetsen van het bestaan en de werking van de interne beheersingsmaatregelen die noodzakelijk zijn voor het verschaffen van een redelijke mate van zekerheid dat de beheersingsdoelstelling werd bereikt.

Eindhoven, 02-02-2024
Cuccibu B.V.

Namens deze,

Patriek Nouwen

Bijlage 1 Oordeel per norm

1. Algemene IT-beheersmaatregelen

1.1 Informatiebeveiliging

Beheersdoelstelling: De ICT-middelen zijn adequaat beveiligd. Het gewenste beveiligingsniveau is vastgelegd en is goedgekeurd door het management.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.1.1	Een actueel, gedocumenteerd en door het management geaccordeerd beveiligingsbeleid voor de ICT-middelen en diensten is aanwezig.	Interview met de CISO, functioneel applicatiebeheerder en de ICT-adviseur, inspectie van het beveiligingsbeleid en de vaststelling ervan. **Resultaat** Geen afwijkingen geconstateerd.

Beheersdoelstelling: Toegang tot ICT-diensten en -middelen is adequaat afgeschermd. Pogingen tot ongeautoriseerde toegang tot ICT-middelen dienen tijdig te worden gedetecteerd.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.1.2	Toegang tot applicaties kan alleen worden verkregen door de invoer van een unieke gebruikersnaam en wachtwoord.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van het wachtwoordbeleid en inspectie van de wachtwoordinstellingen in het systeem. **Resultaat** Het wachtwoordbeleid is conform de BIO. Er wordt ingelogd via SSO, waarbij de wachtwoordeisen niet aan het wachtwoordbeleid voldoen. Echter voldoen de wachtwoordeisen wel aan de BIO en de industriestandaarden, daarom is er geen risico voor de controledoelstelling.
1.1.3	Een procedure voor aanpassing van autorisaties dient te zijn vastgelegd en bestaat uit werkwijzen voor goedkeuring en implementatie van de autorisatie aanvraag met betrekking tot 1) bij indiensttreding, 2) bij	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, controle van een steekproef op in dienst en wijzigingen in functies en de integrale controle van alle uitdiensttreders van 2023.

	wijziging van functie en 3) bij uitdiensttreding.	**Resultaat** Er is een vastgestelde procedure voor in dienst, uitdienst en doorstroom voor HR, echter is ICT hier niet in opgenomen. Voor de processen voor indiensttreding en wijziging van functie zijn geen afwijkingen geconstateerd. Voor het uitdiensttredingsproces zijn meerdere afwijkingen (6 van de 23) geconstateerd, waarbij accounts te laat afgesloten zijn. Van deze accounts zijn er 2 ook niet tijdig in de IAM-tool afgesloten, doordat er te laat een melding vanuit HR gekomen is. De norm voldoet derhalve niet en de controledoelstelling wordt hierdoor niet behaald.

Beheersdoelstelling: Toegang tot ICT-diensten en -middelen dient te worden beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers en beheerders.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.1.4a	De inrichting van de autorisaties in Key2GH is inzichtelijk. Een opzet van de autorisatiematrix is aanwezig waarbij de rol gekoppeld is aan de persoon.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur en controle van de autorisaties in het systeem aan de hand van de autorisatiematrix. **Resultaat** Geen afwijkingen geconstateerd.
1.1.4b	Autorisaties worden periodiek beoordeeld en gecontroleerd.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de rapportages van de interne auditor en het door de externe auditor uitvoeren van een controle op autorisaties aan de hand van de autorisatiematrix. **Resultaat** De autorisaties zijn in 2023 1 keer gecontroleerd door de interne auditafdeling. De BIO schrijft echter eens per half jaar voor bij BBN2 applicaties. Derhalve voldoet de norm niet en is er een risico voor de beheersdoelstelling.

1.1.5	Het aantal gebruikers met "hoge bevoegdheden" (oftewel de superusers/administrators; met rechten aanpassen autorisaties, workflow en overwerking) is beperkt en wordt periodiek gevalideerd.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de autorisaties en autorisatiematrix en inspectie van de logging op wijzigingen uitgevoerd door beheeraccounts. **Resultaat** Geen afwijkingen geconstateerd.
1.1.6	Logging op belangrijke objecten is geactiveerd in Key2GH. Op basis van een risicoanalyse is bepaald welke objecten worden gelogd.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van het loggingbeleid en inspectie van het systeem. **Resultaat** Er is geen risicoanalyse beschikbaar gesteld, wel zijn de risico's benoemd van het niet loggen van bepaalde tabellen. Logging is wel zeer breed geactiveerd en wordt periodiek gecontroleerd. Daarom geen risico voor de controledoelstelling.
1.1.7	Logging op objecten wordt periodiek gecontroleerd.	

1.2 Wijzigingsbeheer

Beheersdoelstelling: Wijzigingen aan de automatiseringsomgeving en de applicaties worden op een gecontroleerde wijze geïmplementeerd.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.2.1	Een procedure wordt gevolgd voor het doorvoeren van wijzigingen (query's, applicatie patches/updates, database updates) in de applicatie, database en besturingssysteem.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de procedure, inspectie van het systeem, inspectie van een steekproef op de wijzigingen en patches, inspectie van tickets uit Service Now, inspectie van de testscripts en draaiboeken van grote releases en inspectie van de Service Level Agreement met de leveranciers. **Resultaat** Geen afwijkingen geconstateerd.

1.2.2	De mogelijkheid om wijzigingen in productie aan te brengen is beperkt tot daartoe geautoriseerde personen.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de procedure, inspectie van het systeem, inspectie van een steekproef op de wijzigingen en patches, inspectie van tickets uit Service Now, inspectie van de testscripts en draaiboeken van grote releases en inspectie van de Service Level Agreement met de leveranciers. **Resultaat** Geen afwijkingen geconstateerd.

1.3 Operations

Beheersdoelstelling: De gegevensverwerking tussen Key2GH en andere applicaties verloopt juist en volledig.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.3.1	Geautomatiseerde scheduling tools zijn geïmplementeerd ten behoeve van de volledigheid van de stroom van verwerking. Na verwerking genereert de batch job een uitzonderingslijst waaruit kan worden vastgesteld dat alle gegevens zijn overgezet. Ingelezen basisgegevens uit andere registraties kunnen niet dubbel worden verwerkt.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van het systeem, inspectie van de gebruikte scripts, inspectie van de logging van de jobs, inspectie van de rapportages over de vergelijking tussen Ortax en Key2Belastingen en inspectie van het rapport van de waarderingskamer. **Resultaat** Er is geen opzet document beschikbaar met een overzicht van de gewenste jobs. Voor bestaan en werking zijn geen afwijkingen geconstateerd, er is geen risico voor de doelstelling geconstateerd.

Beheersdoelstelling: De ICT-omgeving dient in het geval van een calamiteit tijdig herstelbaar te zijn.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.3.2	De uitvoering van back-up processen wordt beoordeeld. Eventuele geconstateerde uitzonderingen worden zichtbaar opgevolgd.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de contracten en de Service Level Agreements met de leveranciers.

		Resultaat Geen afwijkingen geconstateerd.

1.4 Supplier Management

Beheersdoelstelling: Het kwaliteitsniveau van geleverde ICT-diensten is gewaarborgd.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
1.4.1	De ICT-diensten van leveranciers en de daarbij horende voorwaarden (beleidspunten, dienstenniveaus, beheers doelstellingen en geautoriseerde ontvangers van ICT-diensten) worden formeel overeengekomen.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de contracten en de Service Level Agreements met de leveranciers. **Resultaat** Geen afwijkingen geconstateerd.
1.4.2	Prestaties van ontvangen ICT-diensten worden gemeten en geregistreerd en beoordeeld.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de opgeleverde Service Level Reports en inspectie van de gespreksverslagen van de periodieke overleggen met de leveranciers. **Resultaat** Geen afwijkingen geconstateerd.

2. Beoordeling controle query's

2.1 Query's

Beheersdoelstelling: Juist, volledig en geautoriseerd onderhouden van queries.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
2.1.1	De organisatie beschikt over vastgelegde beschrijvingen / toelichting op de werking en functie van de gehanteerde query's.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, interview van de query applicatie, inspectie van het wijzigingsbeheerproces. **Resultaat** Geen afwijkingen geconstateerd.

3. Geautomatiseerde controlemaatregelen

3.1 Algemeen

Beheersdoelstelling: Acties en uitgevoerde activiteiten zijn in de applicatie herleidbaar.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
3.1.1	Logging op objecten (audit trail) is geactiveerd voor de volgende onderdelen: - wijzigingen van bankrekeningnummers - wijzigingen van gebruikersaccounts - wijzigingen van autorisaties - wijzigingen van parameters - verwijderen van mutatievastlegging (logging) - wijzigingen buiten de applicatie om (wijzigingen direct aangebracht in de database)	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van het logging en monitoring beleid, inspectie van de systemen en de logging. **Resultaat** Het loggen van wijzigingen van gebruikersaccounts en autorisaties is niet mogelijk in het systeem. Verder geen afwijkingen geconstateerd. De norm voldoet daarom gedeeltelijk en de controledoelstelling wordt niet geheel gehaald.

3.2 Basisregistratie

Beheersdoelstelling: De invoer en het onderhoud van basisgegevens vindt juist en volledig plaats.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
3.2.1	Nieuwe objecten worden uniek (doorlopend) geïdentificeerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.2.2	De applicatie dwingt af dat velden (status, ingangsdatum, hoofdcode, heffingsmodel, WOZ-objectnummer) verplicht dienen worden ingevuld bij het aanmaken en muteren van objecten.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.2.3	Het ingevoerde BSN-nummer dient te voldoen aan de eis van 9 karakters en kan niet dubbel worden ingevoerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric.

	Een maximale veldlengte wordt toegepast.	**Resultaat** Geen afwijkingen geconstateerd.
3.2.4	De ingevoerde ingangsdatum mag niet recenter zijn dan de datum waarop het object is ingevoerd. Een maximale veldlengte wordt toegepast.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

3.3 Waarderen

Beheersdoelstelling: De waardering van belastingen vindt juist en volledig plaats.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
3.3.1	De waardering van de hoogte van de belastingen wordt aan de hand van vastgelegde rekenregels/tarieven uitgevoerd en vindt juist en volledig plaats.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van het rapport van de waarderingskamer, inspectie van de autorisatiematrix en inspectie van het systeem. **Resultaat** De juistheid en volledigheid van de rekenregels is buiten scope geplaatst van deze audit. De RBG beraadt zich of deze norm onderdeel moet uitmaken van dit normenkader. Op de andere normen geen afwijkingen geconstateerd. Echter kan over de beheersdoelstelling geen zekerheid gegeven worden.
3.3.2	De hoogte van belastingen (belastingtarieven) kan niet door de eindgebruikers worden aangepast. De hoogte wordt bepaald aan de hand van rekenregels binnen de applicatie.	
3.3.3	Ingevoerde rekenregels/tarieven zijn alleen aan te passen door daartoe bevoegde personen.	
3.3.4	De applicatie voorziet in een rapportage waarbij objecten die niet zijn gekoppeld aan een taxatiewaarde worden getoond. Deze rapportage wordt periodiek gecontroleerd.	

3.4 Heffen

Beheersdoelstelling: De heffing van belastingen vindt juist en volledig plaats.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**

3.4.1	Een heffingsopdracht (aanslag) kan slechts eenmaal worden verwerkt en ingevoerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.4.2	Bij het invoeren van een heffingsopdracht dienen belastingsoorten, heffingswijzecodes en btw-tarief geselecteerd te worden op basis van een tabel. Voor deze gegevens kunnen geen eigen waardes ingevoerd worden.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.4.3	De applicatie voorziet in een rapportage waarbij heffingsopdrachten die nog niet zijn verwerkt worden getoond.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

3.5 Innen

Beheersdoelstelling: Het innen van belastingen vindt juist en volledig plaats.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
3.5.1	Heffingen kunnen niet worden verwijderd of gemuteerd als deze nog niet zijn geïnd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.2	De ontvangstwijze (internet betaling, automatische incasso) van betalingen op vorderingen dient verplicht te worden ingevoerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.3	Het bankrekeningnummer dient te voldoen aan de eisen die gesteld worden ten opzichte van IBAN	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric.

	weergave. Een maximale veldlengte wordt toegepast.	**Resultaat** Geen afwijkingen geconstateerd.
3.5.4	De applicatie dwingt af dat velden (aantal termijnen, betaalwijze) verplicht dienen worden ingevuld bij het aanmaken of muteren van een betalingsregeling.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.5	De applicatie dwingt af dat velden (bedrag van restitutie, rekeningnummer begunstiger) verplicht dienen worden ingevuld bij het opvoeren van restituties.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.6	De applicatie dwingt af dat bij een aanmaningstop door middel van uitstel een einddatum wordt ingevoerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.7	Betalingen kunnen alleen worden gekoppeld aan bestaande vorderingen.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.8	Het gekoppelde bedrag van een betaling mag niet groter zijn dan het totaal van de openstaande vorderingen bij een debiteur.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.9	De hoogte van de restitutie mag niet groter zijn dan het ontvangen bedrag.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

3.5.10	Het betaalbestand van de bankapplicatie wordt juist en volledig geïmporteerd in de applicatie.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.11	De applicatie dwingt af dat betalingen uit betalingenbestanden slechts eenmaal kunnen worden verwerkt.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.12	Het betaalbestand dat wordt ingevoerd in de applicatie is niet te wijzigen.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.13	Uitval van de bankapplicatie (te veel betaalde heffingen, te weinig betaalde heffingen) wordt tijdig verwerkt.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.14	De applicatie dwingt af dat het niet mogelijk is om het betaalde bedrag handmatig aan te passen.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.15	De applicatie dwingt af dat het totaalbedrag aan betalingen gelijk is aan de geaccepteerde betalingen.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

3.5.16	Ontvangsten en betalingen worden juist en volledig in de belastinghistorie van de debiteur verwerkt.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

Beheersdoelstelling: Toegang tot kritische gegevens dient te worden beperkt tot geautoriseerd gebruik door geautoriseerde gebruikers en beheerders.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
3.5.17	De applicatie dwingt af dat openstaande posten (kwijtschelding, ontheffing, vernietiging, vermindering, oninbaar, opschorting) slechts kunnen worden gewijzigd door geautoriseerde medewerkers.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.18	De applicatie dwingt af dat betalingsprocessen bij restitutie slechts kunnen worden opgestart door geautoriseerde medewerkers.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.19	Het wijzigen van een betaalstatus (bewind voering) bij een subject is voorbehouden aan geautoriseerde medewerkers.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.20	Het wijzigen van een status voor bezwaar/beroep is voorbehouden aan geautoriseerde medewerkers	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
3.5.21	De applicatie dwingt af dat het importeren van betalingsbestanden slechts kunnen worden opgestart door geautoriseerde medewerkers.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric.

		Resultaat Geen afwijkingen geconstateerd.
3.5.22	De applicatie dwingt af dat aanpassingen in workflows alleen door daardoor geautoriseerde personen uitgevoerd kunnen worden.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de autorisatiematrix en inspectie van het systeem. **Resultaat** Geen afwijkingen geconstateerd.

4. Autorisatie-inrichting op functiescheidingsaspecten

4.1 Functiescheiding

Beheersdoelstelling: Organisatorische functiescheiding is adequaat doorgevoerd in de applicatie.		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
4.1.1	De organisatie beschikt over een overzicht waaruit blijkt hoe het met controle-technische functiescheidingen binnen de verschillende processen omgaat.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de autorisatiematrix en beoordeling van het wijzigingsbeheerproces. **Resultaat** Geen afwijkingen geconstateerd.
4.1.2	Autorisaties met betrekking tot het (functionele en technische) beheer van de applicatie zijn gescheiden van de autorisaties met betrekking tot operationele werkzaamheden.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de autorisatiematrix en beoordeling van het wijzigingsbeheerproces. **Resultaat** Geen afwijkingen geconstateerd.
4.1.3	Autorisaties met betrekking tot het onderhoud van de basisregistratie zijn gescheiden van de autorisaties met betrekking tot het heffen en innen van belastingen.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de autorisatiematrix en beoordeling van het wijzigingsbeheerproces. **Resultaat** Geen afwijkingen geconstateerd.

4.1.4	De applicatie dwingt af dat aanpassingen in belastingtarieven worden gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.5	De applicatie dwingt af dat aanpassingen bij het invoeren van kwijtscheldingen worden gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.6	De applicatie dwingt af dat aanpassingen in status bezwaar/beroep worden gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.7	Autorisaties met betrekking tot het heffen van belastingen zijn gescheiden van de autorisaties met betrekking tot het innen van belastingen.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur, inspectie van de auditrapportage van KPMG over Key2Belastingen en inspectie van de autorisatiematrix. **Resultaat** Geen afwijkingen geconstateerd.

Beheersdoelstelling: Systeeminstellingen		
Nr.	**Norm**	**Testwerkzaamheden en conclusie**
4.1.8	De applicatie dwingt af dat de betalingsregeling wordt gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

4.1.9	De applicatie dwingt af dat de restitutie wordt gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.10	De applicatie dwingt af dat oninbaar leiden wordt gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.11	De applicatie dwingt af dat onvermogen afzonderlijk wordt gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.12	De applicatie dwingt af dat invoeren van een bankrekeningnummer afzonderlijk wordt gefiatteerd.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur en inspectie van het systeem en het wijzigingsproces. **Resultaat** Geen afwijkingen geconstateerd.
4.1.13	De applicatie dwingt af dat bezwaarschriften afzonderlijk worden gefiatteerd.	Interview met de functioneel applicatiebeheerder en de ICT-adviseur en inspectie van het systeem en het wijzigingsproces. **Resultaat** Geen afwijkingen geconstateerd.
4.1.14	Autorisaties tot het ontwerpen/uitvoeren van queries zijn gescheiden van de autorisaties met betrekking tot operationele werkzaamheden.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

4.1.15	Een nieuwe of gewijzigde heffingsopdracht dient afzonderlijk te worden gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.
4.1.16	De applicatie dwingt af dat aanpassingen in taxaties / nieuwe taxaties van objecten afzonderlijk wordt gefiatteerd.	Inspectie van de auditrapportage van KPMG over Key2Belastingen en de ISAE 3402 Type II verklaring van Centric. **Resultaat** Geen afwijkingen geconstateerd.

Bijlage 2 Aanbevelingen

Nr.	Norm	Aanbeveling
Algemeen	Normenkader	Update het normenkader, zodat deze overeenkomt met de gewenste situatie. Benoem hierbij geen applicatienamen in de normen.
1.1.2	Toegang tot applicaties kan alleen worden verkregen door de invoer van een unieke gebruikersnaam en wachtwoord.	Pas de wachtwoordinstellingen aan conform het beleid, welke aan de BIO voldoet.
1.1.3	Een procedure voor aanpassing van autorisaties dient te zijn vastgelegd en bestaat uit werkwijzen voor goedkeuring en implementatie van de autorisatie aanvraag met betrekking tot 1) bij indiensttreding, 2) bij wijziging van functie en 3) bij uitdiensttreding.	Momenteel is er alleen HR-procedure. Stel een overkoepelende procedure vast voor in dienst, uitdienst en doorstroom waarin zowel de HR als de ICT-werkzaamheden beschreven staan.
1.1.4b	Autorisaties worden periodiek beoordeeld en gecontroleerd.	Voer de periodieke controle minimaal elk half jaar uit, conform de eisen uit de BIO.
1.1.6	Logging op belangrijke objecten is geactiveerd in Key2GH. Op basis van een risicoanalyse is bepaald welke objecten worden gelogd.	Leg een aparte risicoanalyse vast, waarin bepaald wordt wat er gelogd dient te worden. Werk vanuit die analyse naar de tabellen toe.
1.3.1	Geautomatiseerde scheduling tools zijn geïmplementeerd ten behoeve van de volledigheid van de stroom van verwerking. Na verwerking genereert de batch job een uitzonderingslijst waaruit kan worden vastgesteld dat alle gegevens zijn overgezet. Ingelezen basisgegevens uit andere registraties kunnen niet dubbel worden verwerkt.	Documenteer welke jobs er bestaan en wat deze inhouden.
3.1.1	Logging op objecten (audittrail) is geactiveerd voor de volgende onderdelen: - wijzigingen van gebruikersaccounts - wijzigingen van autorisaties	Leg bij de nieuwe aanbesteding voldoende druk op de leverancier om dit mogelijk te maken.

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security en audit/compliance. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!

www.cuccibu.nl | Cuccibu B.V. | Boutenslaan 195c | Eindhoven | KvK 61072923 | info@cuccibu.nl | +31 (0) 85 303 2984