Ministerie van Volksgezondheid,
Welzijn en Sport

ISAE3402 Type 2 rapport

Z-domein PGB2.0

mijnpgb

Rapportage inzake de opzet, het bestaan en de werking van beheersmaatregelen van het Z-domein PGB2.0 over de periode 1 april 2021 tot en met 31 oktober 2021

Datum	18 mei 2022
Status	Definitief

Ministerie van Volksgezondheid,
Welzijn en Sport

Voorwoord

Het Ministerie van VWS biedt u met dit rapport (ISAE3402) inzicht in de genomen interne beheersmaatregelen ten aanzien van het Zorgdomein PGB2.0. Wij versturen dit rapport aan de Vereniging van Nederlandse Gemeenten, Zorgverzekeraars Nederland en de Sociale Verzekeringsbank.

De Auditdienst Rijk is gevraagd een oordeel te geven over de beschrijving van VWS en over de opzet, het bestaan en de werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld in de periode van 1 april 2021 tot en met 31 oktober 2021.

De indeling van dit rapport is als volgt:

- Sectie 1: Vermelding plaatsvervangend secretaris-generaal van het Ministerie van VWS omtrent de beschrijving en de opzet, het bestaan en de werking van de beheersmaatregelen
- Sectie 2: Het Assurance-rapport van de onafhankelijke IT-auditor (Auditdienst Rijk)
- Sectie 3: Beschrijving van het PGB2.0-systeem
- Sectie 4: De specifieke getoetste interne beheersingsmaatregelen en de resultaten daarvan

Programmadirecteur PGB

Ministerie van Volksgezondheid,
Welzijn en Sport

Inhoudsopgave

Ministerie van Volksgezondheid,
Welzijn en Sport

Sectie I: Vermelding VWS

Vermelding VWS betreffende opzet, bestaan en werking van de beheersmaatregelen in het Zorgdomein PGB2.0

Ministerie van Volksgezondheid,
Welzijn en Sport

1. Sectie I: Vermelding VWS

1.1 Inleiding

Het PGB2.0-systeem ondersteunt budgethouders en zorgverleners, gemeenten, zorgkantoren en de SVB bij het uitvoeren van het pgb (persoonsgebonden budget)-proces. Het PGB2.0-systeem bestaat uit twee domeinen, het Zorgdomein en het Financieel domein. Het Zorgdomein voorziet in functionaliteit voor het administreren van budgethouders, zorgverleners, zorgovereenkomsten, budgetten en ziek- en herstelmeldingen, en het indienen van declaraties en aanmaken van betaalopdrachten (OK2PAY).
Het Financieel domein voorziet in de functionaliteiten voor het voeren van een financiële administratie (waaronder het uitvoeren van bovengenoemde betaalopdrachten) en een salarisadministratie voor de budgethouder. Beide domeinen bestaan uit afzonderlijke applicaties welke met een koppelvlak verbonden zijn. Via het koppelvlak worden profielgegevens, zorgovereenkomsten, ziek- en herstelmeldingen en betaalopdrachten van het Zorgdomein naar het Financieel domein gestuurd. Het Financieel domein stuurt bevestiging van de ontvangst en verwerking van deze berichten, berekeningen van werkgeverslasten alsmede de verwerkingsstatus van betaalopdrachten naar het Zorgdomein.

Onder regie van VWS is samen met de VNG, Zorgverzekeraars Nederland en de SVB een Control Framework PGB2.0 opgesteld. In het Control Framework PGB2.0 vl.2 dd. 22-02-2021 zijn de beheersdoelstellingen, geïdentificeerde risico's en beheersmaatregelen verder uitgewerkt voor het Zorgdomein respectievelijk het Financieel domein. De Programmaraad PGB2.0 heeft op 11 maart 2021 het Control Framework PGB2.0 vl.2 vastgesteld.

De "Beschrijving PGB2.0" in sectie 3 heeft als doel inzicht te geven in de interne beheersmaatregelen van VWS-TBO met betrekking tot het ontwikkelen en beheren van het Zorgdomein van het PGB2.0-systeem aan ketenpartners die gebruik maken van het PGB2.0- systeem alsmede hun accountants.

1.2 Vermelding

De bijgaande Beschrijving PGB2.0 is opgesteld voor gemeenten, zorgkantoren en de SVB die gebruik hebben gemaakt van het PGB2.0-systeem en de dienstverlening door VWS-TBO (Tijdelijke Beheerorganisatie) met betrekking tot het gebruik van het PGB2.0-systeem, en voor hun accountants die voldoende inzicht hebben om de beschrijving te beschouwen, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door de ketenpartners zelf worden beheerd, wanneer zij inzicht verwerven in de informatiesystemen van ketenpartners die relevant zijn voor financiële verslaggeving. Onze vermelding heeft uitsluitend betrekking op het

Zorgdomein van het PGB2.0-systeem.

VWS bevestigt dat:
(a) De bijgaande beschrijving in sectie III van het Zorgdomein van het PGB2.0-systeem voor het verwerken van de transacties van de ketenpartners, zorgverleners en budgethouders is beoordeeld onder toepassing van de volgende de criteria die inhielden dat de beschrijving

(i) Weergeeft op welke wijze het Zorgdomein van het PGB2.0-systeem is opgezet en geïmplementeerd, met inbegrip van:

- De soorten diensten die verleend zijn in het Zorgdomein met inbegrip van de verwerkte transactiestromen.
- De procedures binnen informatietechnologie waardoor die transacties werden geïnitieerd, vastgelegd, verwerkt, gecontroleerd voor zover noodzakelijk en overgebracht naar de rapportages die voor de ketenpartners zijn opgesteld.
- De verbonden administratie, die de informatie en specifieke rekeningen waarvan gebruik is gemaakt om transacties te initiëren, verwerken, vast te leggen en rapporteren; dit houdt onder meer het corrigeren van incorrecte informatie in en op welke wijze informatie is overgedragen naar de rapportages die voor de ketenpartners, budgethouders en zorgverlenerszijn opgesteld. Op welke wijze het Zorgdomein van het PGB2.0-systeem de significante gebeurtenissen en omstandigheden, buiten de transacties, heeft behandeld.
- Het proces waarvan gebruik werd gemaakt bij het opstellen van rapportages voor gemeenten, zorgkantoren en de SVB.
- Relevante interne beheersingsdoelstellingen en interne beheersingsmaatregelen die zijn opgezet om die doelstellingen te bereiken. Dit betreft de application controls, IT-dependent controls en genera! IT controls in het Zorgdomein van het PGB2.0-systeem, zoals vastgelegd in het Control Framework PGB2.0. vl.2 Deze maatregelen zijn weergegeven in bijlage 1. Wij benadrukken dat naast de in de bijlage genoemde application controls met betrekking tot de processen Toekenning, Profielgegevens, Zorgovereenkomsten, Declaraties, Betaalopdrachten PGB en Werkgeversondersteuning het noodzakelijk is om ook de handmatige beheersmaatregelen uit bijlage 3 van het Control Framework PGB2.0 toe te passen teneinde de beheersdoelstellingen voor deze zes processen te bereiken.
- Interne beheersingsmaatregelen waarvan wij, bij de opzet van het systeem, aannamen dat zij door gebruikersorganisaties zouden worden geïmplementeerd en die, indien noodzakelijk om de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld te

bereiken, samen met de specifieke interne beheersingsdoelstellingen die niet alleen door onszelf kunnen worden bereikt zijn geïdentificeerd.

- Overige aspecten van de beheersingsomgeving rond het Zorgdomein van het PGB2.0-systeem, het risico-inschattingsproces, het informatiesysteem (met inbegrip van het verbonden bedrijfsproces) en communicatie, beheersingsactiviteiten en interne beheersingsmaatregelen betreffende monitoring die relevant zijn voor het verwerken en het rapporteren van de transacties van de ketenpartners, budgethouders en zorgverleners.

(ii) Geen informatie weglaat of verkeerd voorstelt die relevant is voor de reikwijdte van de application controls, IT-dependent controls en genera! IT controls in het Zorgdomein van het PGB-2.0 systeem, terwijl erkend wordt dat de beschrijving is opgesteld om te voldoen aan de algemene behoeftes van een brede groep gebruikers en hun accountants en daarom niet ieder aspect kan bevatten dat iedere individuele gebruiker in diens eigen bijzondere omgeving belangrijk kan achten.

(b) De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld op afdoende wijze zijn opgezet, bestaan, en hebben gewerkt in de periode 1 april t/m 30 oktober 2021, met uitzondering van de in paragraaf 1.3 genoemde afwijkingen: De criteria waarvan bij het maken van deze vermelding gebruik werd gemaakt hielden in dat:

(i) De risico's die het bereiken van de in de beschrijving opgenomen interne beheersingsdoelstellingen in gevaar brengen, werden geïdentificeerd; en

(ii) De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen

1.3 Afwijkingen

Bij het vaststellen van de opzet, het bestaan en de werking van de interne beheersmaatregelen die in bijgaande beschrijving zijn vermeld, zijn de volgende afwijkingen geconstateerd:

- Het identificeren van risico's die het bereiken van beheersdoelstellingen in gevaar brengen, beperkt zich in het Control Framework tot de functionaliteit van het PGB2.0 in relatie tot de doelstellingen van een juiste (rechtmatige), tijdige en volledige verwerking van gegevens. Ter mitigatie van deze risico's zijn application controls, IT-dependent en handmatige controles gedefinieerd. Een risicoanalyse op de IT-beheerdoelstellingen ontbreekt.
- In de TBO ontbreekt een formele scheiding tussen eerstelijns en tweedelijns

controle. In de praktijk voeren de Quality Assurance Officer en de Information Security Officer controles uit die als tweedelijnscontroles maar soms ook als eerstelijnscontroles beschouwd kunnen worden. Het ontbreken van de formele scheiding heeft het opbouwen en verzamelen van informatie ter onderbouwing van de bewering bemoeilijkt.

- De in het Control Framework genoemde application control D3-Mll betreffende een geautomatiseerde controle waarin declaraties voor bijkomende kosten middels een werktaak voorgelegd worden aan de verstrekker ontbreekt in het systeem.

- Voor de in het eerdere ISAE3402-1 rapport genoemde beheersmaatregel B3-M2 kon niet tijdig aanvullende informatie verzameld en verstrekt worden.
- Met betrekking tot Gebruikersbeheer heeft het ontbroken aan aantoonbare periodieke controle van beheerderaccounts, waardoor tijdige verwerking van uitdiensttreding (L2.4) en evaluatie van toegangsrechten {L2.8) en persoonsgebonden accounts (L2.6) niet geborgd zijn. Verder ontbreken gedetailleerde beschrijvingen van toegangsrechten per beheerdersrol (L2.1) en een mandaatregister (L2.2), waardoor beperktheid (L2.5) en gerechtvaardigde toegang tot onderliggende componenten (L2.7) niet aangetoond kunnen worden. Tegelijkertijd wordt door de eerste lijn gesteld dat iedereen 'elkaar kent', het risico op onjuiste toegang voor/door beheerders wordt door de eerste lijn als laag betiteld.
- Met betrekking tot Beveiliging van componenten is vastgesteld dat de organisatie in staat is (geweest) om ten behoeve van Digid assessments en NEN7510/BIO audits inzichtelijk te maken dat op enig moment (de peildatum in de betreffende onderzoeken) aan de eisen van die audits wordt voldaan. De eisen in het Control Framework gaan echter verder danwel zijn explicieter, voor wat betreft configuratiemanagement (L3.1), patching (L3.3.), standaard wachtwoorden (L3.4), besturingssystemen en services (L3.5), zonering (L3.6) en logging en monitoring (L3.7). Van deze onderdelen is vastgesteld dat er diverse activiteiten plaats vinden, maar deze missen structuur en overzicht om de effectieve werking van deze beheersmaatregelen in de gehele controleperiode te kunnen vaststellen.

In aanvulling op bovenstaande afwijkingen is geconstateerd dat er aanleiding is om de zeer gedetailleerde wijze waarop de application controls in het control framework gedefinieerd zijn, te herzien. TBO ziet deze aanleiding vanwege de volgende ervaringen:

- Het PGB2.0 systeem bevat inmiddels een veelvoud aan functionele controles die bijdragen aan de beheersdoelstellingen, elk daarvan is vastgelegd in een functioneel ontwerp en bedrijfsregels. De huidige application controls komen inmiddels over als een enigszins willekeurige deelverzameling daarvan.
- Conform A34 uit de Norea richtlijn ISAE3402 lijkt het effectiever om; vanwege de inherente consistentie van geautomatiseerde gegevensverwerking, de

zekerheid over het geheel aan functionele controles in PGB2.0 te verkrijgen middels het definiëren van (generieke) it-beheersmaatregelen, in het bijzonder t.a.v. wijzigingsbeheer. Deze aanpak maakt het opnemen van specifieke application controls in het Control Framework overbodig, en richt zich in plaats daarvan op het geheel aan geautomatiseerde gegevensverwerking zoals in het PGB2.0 gerealiseerd via het voortbrengingsproces.

VWS zal de prioriteit voor het adresseren van bovenstaande bevindingen met de ketenpartners in de Programmaraad afstemmen. De bevindingen zijn verzameld op een Control Framework PGB2.0 backlog dat met de ketenpartners besproken zal worden.

Hoogachtend,

de plv. secretaris-generaal,

Sectie II: Assurance rapport van de onafhankelijk iT-auditor

Colofon

Titel	Assurance rapport Norea ISAE 3402 type 2 op Zorgdomein PGB2.0
Uitgebracht aan	Plaatsvervangend Secretaris-Generaal van het Ministerie van Volksgezondheid, Welzijn en Sport, mw. A.I. Norville MSc
Datum	18 mei 2022
Kenmerk	2022-0000147860

Inlichtingen

Auditdienst Rijk

070-342 7700

Inhoud

Assurance rapport van de onafhankelijke IT- auditor

2.1 Oordeel met beperking

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. Bij het vormen van ons oordeel hebben wij gebruik gemaakt van de criteria die in de vermelding van het ministerie van Volksgezondheid Welzijn en Sport (VWS) in sectie I staan beschreven.
Naar ons oordeel, in alle van materieel belang zijnde opzichten, uitgezonderd de aangelegenheden die staan beschreven in de paragraaf '1.2 Onderbouwing van het oordeel met beperking',

- geeft de bijgaande beschrijving in sectie III het zorgdomein van het PGB2.0-systeem getrouw weer zoals deze gedurende de periode van 1 april tot en met 31 oktober 2021 is opgezet en geïmplementeerd;
- zijn de interne beheersmaatregelen, die verband houden met de in de beschrijving vermelde interne beheersdoelstellingen gedurende de periode 1 april tot en met 31 oktober 2021 op afdoende wijze opgezet;
- werkten de getoetste interne beheersingsmaatregelen, die noodzakelijk waren om een redelijke mate van zekerheid te verschaffen dat de in de beschrijving vermelde interne beheersingsdoelstellingen waren bereikt, gedurende de verslagperiode van 1 april tot en met 31 oktober 2021 effectief.

2.2 Onderbouwing van het oordeel met beperking

De omvang en aard van de bevindingen kunnen de indruk wekken dat er in 2021 een verslechtering is opgetreden ten opzichte van vorig jaar. Nadrukkelijk vermelden wij dat deze conclusie uit onderstaande niet kan worden getrokken. De toename van het aantal bevindingen en een veranderde strekking ervan, is voornamelijk gelegen in de toevoeging van het toetsingsaspect 'werking' en de vereiste dat deze over de hele periode op basis van voldoende onderbouwende stukken aantoonbaar gemaakt dient te worden.

Onderstaande bevindingen liggen ten grondslag aan ons oordeel met beperking.

Application controls

- Van de 48 te toetsen application controls, is D3-M11 niet ingericht en van B3-M2 zijn de opzet, bestaan en effectieve werking niet voldoende aantoonbaar gemaakt.

General IT-controls

- Van het gebruikersbeheer is, met uitzondering van L2.3 (Functiescheiding tussen aanvragen autoriseren en wijzigen van accounts en toegangsrechten) in de verslagperiode de opzet en werking van de beheersmaatregelen L2.1 tot en met L2.8 niet voldoende aantoonbaar gemaakt.
- Van de beveiliging van componenten is, met uitzondering van L3.2 (Alertering op nieuwe kwetsbaarheden) in de verslagperiode de opzet en werking van de beheersmaatregelen L3.1 tot en met L3.7 niet voldoende aantoonbaar gemaakt.

2.3 Nadere duiding van de bevindingen

2.3.1 46 van de 48 application en alle IT-dependent controls zijn effectief

- D3-M11 betreffende een geautomatiseerde controle waarin declaraties voor bijkomende kosten middels een werktaak voorgelegd worden aan de verstrekker, ontbreekt in het systeem.
- In relatie tot de beheersingsdoelstelling (B3) dat retourinformatie over het financieel domein verwerkte betaalopdrachten juist en volledig wordt verwerkt door het zorgdomein, is het bestaan van de application control met betrekking tot verwerken van de betaalstatus (B3-M2) niet inzichtelijk gemaakt.
- Van de overige 46 application en 4 IT-dependent controls is de effectieve werking in de verslagperiode vastgesteld.

2.3.2 Gebruikersbeheer niet volledig effectief

- Van gebruikersaccounts kon niet volledig worden vastgesteld of ruimere rechten zijn uitgegeven, dan voor de uitoefening van de desbetreffende functie(s) nodig is. (L2.1). Ook is niet volledig aantoonbaar gemaakt dat toegekende rechten zijn gestoeld op geldige mandaten (L2.2). TBO geeft aan dat dergelijke afwegingen wel aanwezig zijn, grotendeels ingebed in systemen voor uitgifte en intrekken van de autorisaties, maar niet expliciet als basis voor periodieke controle zijn vastgelegd.
- Verwerking van uitdiensttreding (L2.4) en de juistheid van toegekende bevoegdheden (L2.6 en L2.8) werd in de verslagperiode onvoldoende bewaakt. Daardoor ontbrak een doorlopend actueel inzicht in mogelijke kwetsbaarheden door onterecht openstaande bevoegdheden. Dat overzicht is nodig om tijdig en adequaat mogelijk ongeoorloofde toegangsrechten te beperken.
- Het aantal technisch applicatiebeheerders is niet expliciet verklaard en de gehanteerde differentiatie naar junior en senior technisch applicatiebeheerder is niet gemotiveerd. Hierdoor is niet volledig vast te stellen of mogelijk te ruime technisch beheerrechten zijn uitgegeven (L2.5). Wel geeft TBO aan in de praktijk goed zicht te hebben in het aantal technisch beheerders en de aan hen uitgegeven autorisaties.
- Niet aangetoond kon worden dat alleen gerechtvaardigde toegang tot onderliggende componenten (L2.7) gewaarborgd was.

Aanbevelingen

- Stel een autorisatiematrix en mandaatregister op waarin functiescheiding op basis van het need-to-know principe wordt uitgewerkt en waarbij expliciet wordt gemaakt welke bevoegdheden elke rol bevat. Richt vervolgens de rollen die via Topdesk worden uitgegeven in lijn met de autorisatiematrix in en onderhoud beide. (L2.1 en L2.2)
- Controleer maandelijks op de geldigheid van uitgegeven en ingetrokken toegangsrechten en zorg voor adequate en tijdige (bv binnen dag of een week, afhankelijk van de aard van de afwijking) afwikkeling van bevindingen. Stel de betrouwbaarheid van het controleoverzicht vast en neem de rapportages hierover op als evidence voor het aantoonbaar maken van de beheersmaatregelen van het Control Framework. (L2.4, L2.6, L2.7 en L2.8)
- Ga na hoeveel beheeraccounts nodig zijn en breng meer differentiatie aan in beheeraccounts. Maak de onderbouwing van het aantal beheerders expliciet (L2.5).

2.3.3 *Beveiliging van componenten niet effectief*

- Het configuratiemanagement is nog niet op orde (L3.1). Als basisadministratie (configuratiemanagement) voor de IT-infrastructuur gebruikt TBO verschillende afzonderlijke instrumenten. Een overkoepelende centrale administratie waarin ook metagegevens over de componenten zijn geregistreerd, is niet aanwezig. Daardoor ontbreekt een centrale basis die een goede beheersing en onderhoud van de IT-infrastructuur ondersteunt teneinde deze veilig (en continu) te laten functioneren.
- De beschrijving van het patchmanagement beperkt zich tot een zestal middelen/systemen. Deze scope is in verhouding tot de gehele IT-infrastructuur beperkt. Het bestaan is wel aangetoond. Een periodieke controle om de werking aantoonbaar te maken voor de in scope zijnde systemen en componenten is voor de verslagperiode niet ingericht. (L3.3)
- Alleen van instellingen van de Windows accounts is aantoonbaar gemaakt dat geen gebruik gemaakt wordt van standaard wachtwoorden voor toegang door beheerders. Hoewel het bestaan (voor Windows accounts) is aangetoond, is dit ontoereikend voor de beeldvorming over de werking. (L3.4)
- Over het begin van de verslag periode kon geen beschrijving worden aangeleverd aan de hand waarvan is vast te stellen of de juiste en volledige zaken zijn gemonitord. Het IDS/IPS proces is eind oktober beter beschreven; ook het uitgevoerde DigiD assessment leverde een goedkeuring op. Dit valt echter zodanig beperkt binnen de verslagperiode dat wij deze beheersmaatregel over de verslagperiode niet als effectief kunnen aanmerken. (L3.7)
- Ook ten aanzien van besturingssystemen en services (L3.5 en zonering (L3.6) is vastgesteld dat diverse monitoringsactiviteiten plaatsvinden, maar dat het structureel overzicht ontbreekt om de effectieve werking van deze beheersmaatregelen over de verslagperiode vast te kunnen stellen.

Aanbevelingen

- Rond zo snel mogelijk de inrichting van het configuratiemanagement af, zodat een actuele en volledige basisadministratie voor de andere beheerprocessen beschikbaar komt (L3.1).
- Definieer het patchmanagementproces zodanig dat hierin de gehele IT-infrastructuur in scope is. Houd deze actueel en stel definitieve versies formeel vast (L3.3).
- Richt een maandelijkse interne controle in om gedurende een hele verslagperiode vast te stellen dat instellingen zodanig zijn ingericht dat standaard wachtwoorden gewijzigd dienen te worden. Voer dit uit voor alle componenten binnen bereik van de IT-infrastructuur (L3.4, L3.5 en L3.6).
- Stel een procedure en procesbeschrijving vast waarin de manier van actieve monitoring is beschreven en sluit daarbij aan op het IDS/IPS. Richt een proces in van periodieke interne controle op de uitkomsten van de monitoring (L3.7).

2.4 Overige beheersmatige bevindingen interne beheersing

Bovengenoemde bevindingen zijn rechtsreeks gerelateerd aan afwijking van de in het toetskader[1] opgenomen normen. Deze bevindingen raken rechtstreeks het oordeel. In deze paragraaf gaan wij in op bevindingen die gerelateerd zijn aan de interne beheersing, de tweedelijns control en het control framework, zoals ook door VWS vermeld in sectie I, de Vermelding VWS. Wij zien in deze bevindingen belangrijke oorzaken voor bovengenoemde afwijkingen van de norm. Door deze in

[1] Opdrachtbevestiging 3402 type 2 rapport Zorgdomein PGB-systeem 2.0 (2022-0000093007), Bijlage 2A t/m 2D.

dit rapport te adresseren bieden wij TBO en VWS concreet handelingsperspectief om afwijkingen van de normen zo veel mogelijk te beperken.

2.4.1 Beperkte tweedelijnscontrole maakt aantoonbaar maken werking lastig

De interne tweedelijnscontrole binnen de TBO is nog niet voldoende ingericht op het in continuïteit monitoren van de goede werking - en het opvolgen van geconstateerde afwijkingen van beheersmaatregelen. Hierdoor is TBO niet op efficiënte – en voor gebruikersbeheer en beveiliging van componenten effectieve – wijze in staat gebleken om de toereikende werking van alle beheersmaatregelen aantoonbaar te maken. Door het uitvoeren van verdiepende werkzaamheden hebben wij (behoudens voor de hierboven genoemde onderdelen) toereikende assurance informatie verkregen.

Om vast te stellen dat de beheersmaatregelen in opzet, bestaan en werking in de periode van 1 april tot en met 31 oktober 2021 effectief functioneerden, hebben wij derhalve meer werkzaamheden uitgevoerd dan verwacht zou mogen worden bij een NOREA ISAE 3402 type 2 onderzoek. Het uitgangspunt van ISAE 3402 type 2 onderzoeken is dat de IT auditor (hier: ADR) van de serviceorganisatie (hier: TBO) grotendeels kan steunen op periodieke en stelselmatige controlewerkzaamheden (tweedelijnscontrole) van de interne controle- c.q. auditfunctie en de vastleggingen daarvan.

Bij de planning en uitvoering van de werkzaamheden door de interne controlefunctie kon geen gebruik worden gemaakt van een vooraf opgesteld en met de ADR afgestemd controleplan voor een 3402 type 2 (opzet, bestaan en werking) rapportage. De interne controle is grotendeels uitgevoerd conform de uitwerking die bij het eerdere 3402 type 1 onderzoek, naar opzet en het bestaan was gehanteerd. De werkzaamheden en vastleggingen van de interne controlefunctie bleken met name hierdoor niet zodanig dat wij de vereiste assurance-informatie op een efficiënte- en voor gebruikersbeheer en beveiliging van componenten effectieve wijze tot onze beschikking hadden.

Hoewel de interne controle de nodige onderbouwingen heeft aangeleverd op basis waarvan opzet en bestaan van de beheersmaatregelen grotendeels aangetoond zijn, waren deze niet op het niveau dat direct ook een goed beeld over de werking van deze beheersmaatregelen kon worden gevormd. Daarvoor zijn bijvoorbeeld vooraf gedefinieerde aantallen deelwaarnemingen op een vooraf beschreven populatie en met een vooraf geduide periodiciteit nodig. Voorts dienen registraties plaats te vinden van bevindingen uit die deelwaarnemingen en dient opvolging aantoonbaar gemaakt te worden.

Door het gedeeltelijk ontbreken van benodigde informatie hebben wij zelf deelwaarnemingen uitgevoerd, aanvullende assurance informatie opgevraagd en nadere analyses uitgevoerd. Wij zijn van mening dat door het ontbreken van een goed ingerichte interne (tweedelijns) controle, TBO niet voldoende aantoonbaar in control is geweest over de goede werking van de beheersmaatregelen gedurende de verslagperiode. Dit geldt voor het hele stelsel van het control framework en de verantwoording daarover.

Om in de toekomst de werking van de beheersmaatregelen beter aantoonbaar te maken en toereikende en volledige assurance informatie op te leveren, bevelen wij aan om het control framework nader te operationaliseren in een controlewerkprogramma (CWP). Het is daarbij zaak om per beheersmaatregel vooraf nader te definiëren hoe de controles zijn ingericht en dienen te worden uitgevoerd, zodat met name de werking vastgesteld kan worden (wie, in welke frequentie, op welk tijdstip, welke testen (bijvoorbeeld het opvragen van rapportages, het doen van waarnemingen ter plaatse of het uitdraaien van systeeminstellingen) op welke componenten en op basis van welke bescheiden). Ook valt hieronder het beschrijven en inrichten van de manier waarop wordt omgegaan met geconstateerde afwijkingen en de bewaking van de opvolging en afdoening, inclusief vastlegging.

2.4.2 Herziening Control Framework gewenst

Naast het toetsen van de opzet, het bestaan en de werking van de beheersmaatregelen is ook het beoordelen van de criteria onderdeel van deze ISAE 3402 type 2 opdracht. Nagedaan dient te worden of VWS geschikte criteria heeft gedefinieerd en gehanteerd. Wij constateren dat het Control Framework in 2020 met veel zorg en in nauwe samenwerking met de verschillende ketenpartners (SVB, VNG, ZN) is opgesteld en in 2021 geactualiseerd. In deze 1.2 versie ligt het zwaartepunt bij het afleggen van verantwoording over (de opzet en het bestaan van) de application controls in relatie tot de rechtmatigheid. Minder aandacht is besteed aan (het aantoonbaar maken van) de General IT-Controls (GITC), toename van application controls vanuit het voortbrengingsproces en de risicoanalyse die ten grondslag ligt aan de keuze voor de betreffende beheersmaatregelen.

Het PGB2.0 is operationeel in een tijdelijke beheer organisatie, waarbij door het voortbrengingstraject nog wordt gewerkt aan het ontwikkelen en in productie nemen van nieuwe functionaliteit, alsmede het aansluiten van gemeenten, zorgkantoren (2021) en daarmee budgethouders. Het Control Framework plaatst deze factoren zonder argumentatie buiten scope. Een inherent risico is dat bijvoorbeeld vanuit de conversie rechtstreeks op de database gemuteerd zou kunnen worden. Of dat een reëel risico is, hebben wij niet vastgesteld omdat dit expliciet buiten het bereik van de vast te stellen beheersmaatregelen van deze assurance opdracht is gesteld. Omdat het wel volledig binnen de werkingssfeer van het Zorgdomein PGB2.0 valt zijn wij van mening dat het in de risicoanalyse opnemen van de aspecten van voortbrenging en conversie en het pas daarna gemotiveerd buiten scope plaatsen een verbetering zijn van het Control Framework.

Tijdens dit assurance onderzoek is aannemelijk gemaakt dat het voortbrengingsproces en de conversies geen invloed hebben gehad op de werking van de beoordeelde beheersmaatregelen.

Wij bevelen aan om een evaluatie van het control framework uit te voeren en deze te baseren op een risicoanalyse. Laat daarin aspecten zoals (niet limitatief) het voortbrengingsproces, uitbestede dienstverlening, conversie en de gewenste assurance informatie aan de orde komen. Bij bevelen tevens aan om de evaluatie en actualisatie van het control framework te combineren met bovengenoemde operationalisering van het control framework.

2.5 Reikwijdte, verantwoordelijkheden en uitgevoerde werkzaamheden

2.5.1 Beschrijving van getoetste interne beheersingsmaatregelen

De specifieke getoetste interne beheersingsmaatregelen en de resultaten van die toetsingen zijn opgenomen in sectie IV.

2.5.2 Verantwoordelijkheden VWS

VWS is verantwoordelijk voor het

- opstellen van de beschrijving van het PGB2.0-systeem en de bijgaande vermelding in sectie III respectievelijk in sectie I, met inbegrip van de volledigheid, nauwkeurigheid en methode van presentatie van die beschrijving en de vermelding;
- verlenen van de diensten die door de beschrijving worden omvat;
- vermelden van de interne beheersingsdoelstellingen en;
- opzetten en implementeren en effectief laten werken van interne beheersingsmaatregelen om de vermelde interne beheersingsdoelstellingen te bereiken.

2.5.3 Onze onafhankelijkheid en kwaliteitsbeheersing

Wij hebben bij deze opdracht de vereisten van het Reglement Gedragscode (‘Code of Ethics’) nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, vertrouwelijkheid en professionaliteit.
Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden wij 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.

2.5.4 Onze verantwoordelijkheden

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van een oordeel over de beschrijving van VWS en over de opzet, het bestaan en de werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld. Wij hebben onze opdracht uitgevoerd overeenkomstig Richtlijn 3402 “Assurance-rapporten interne beheersing serviceorganisatie”, vastgesteld door Nederlandse Orde van Register
EDP-Auditors (NOREA). Dit vereist dat wij onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de beschrijving getrouw is weergegeven en de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet.

Een assurance-opdracht om te rapporteren over de beschrijving en opzet, bestaan en werking van interne beheersingsmaatregelen bij een serviceorganisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance informatie over de toelichtingen in de beschrijving van de serviceorganisatie van haar systeem en de opzet van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de IT-auditor van de serviceorganisatie toegepaste
oordeelsvorming, met inbegrip van het inschatten van de risico’s dat de beschrijving niet getrouw is weergegeven en dat interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet en niet voldoende effectief werken. Een assurance- opdracht van dit type omvat ook het evalueren van het algehele beeld van de beschrijving, de geschiktheid van de interne beheersingsdoelstellingen die daarin staan vermeld en de geschiktheid van de criteria die door de serviceorganisatie zijn

gespecificeerd. Voor het PGB2.0-systeem zijn deze door VWS aangaande het Zorgdomein beschreven in sectie I.

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

2.5.5 *Uitgevoerde werkzaamheden*

Wij hebben de volgende werkzaamheden uitgevoerd om tot ons oordeel te komen:

- inspectie van de bevestiging door de programmaraad van PGB2.0, waarin een vertegenwoordiging van gemeenten, zorgkantoren, de SVB, gebruikers en belangenorganisaties zitting heeft, over het gebruikte Control Framework waarin de van belang zijnde interne beheersmaatregelen zijn gespecificeerd;
- inspectie van het opgestelde dossier dat betrekking heeft op het PGB2.0-systeem, zoals aangereikt door de interne auditor van VWS;
- aanvullende waarnemingen ter onderbouwing van ons oordeel over de opzet en implementatie van betreffende beheersmaatregelen, bijvoorbeeld interviews met relevante functionarissen en demonstraties van het PGB2.0-systeem;
- een verklaring van het algemene bestuur van VWS opgevraagd waarin wordt bevestigd dat geen informatie wordt weggelaten of verkeerd wordt voorgesteld, die relevant is voor de reikwijdte van het PGB2.0-systeem zoals dat dat is beschreven (Letter of Representation).

2.5.6 *Inherente beperkingen van interne beheersmaatregelen*

De door VWS opgestelde beschrijving is opgezet om aan de algemene behoefte te voldoen van gemeenten, zorgkantoren en de SVB die gebruik hebben gemaakt van het PGB2.0-systeem en, indien van toepassing, hun accountants. Het systeem kan daarom niet ieder aspect bevatten dat iedere individuele betrokkene in diens eigen bijzondere omgeving belangrijk kan achten. Bovendien kunnen met interne beheersingsmaatregelen bij een serviceorganisatie, vanwege hun aard, niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekt worden. Ook is de projectie van een eventuele evaluatie van de effectiviteit naar toekomstige verslagperiodes onderhevig aan het risico dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat kunnen worden of falen.

2.5.7 *Beoogde gebruikers en doel*

Deze rapportage en de beschrijving van toetsingen van interne beheersingsmaatregelen in sectie IV zijn alleen voor gemeenten, zorgkantoren en de SVB en, indien van toepassing, ook voor hun accountants, die gebruik hebben gemaakt van het Zorgdomein van het PGB2.0-systeem van VWS en die voldoende inzicht hebben om deze in aanmerking te nemen bij het inschatten van de risico's op afwijkingen van het materieel belang in hun financiële overzichten, tezamen met overige informatie, waaronder informatie over interne beheersingsmaatregelen die door hen zelf worden uitgevoerd.

2.5.8 *Geadresseerde en reikwijdte*

Wij hebben opdracht gekregen om over de periode 1 april 2021 tot en met 31 oktober 2021 te rapporteren over de beschrijving van VWS in sectie III over het zorgdomein van het PGB2.0-systeem, voor het verwerken van de transacties van gemeenten, zorgkantoren, de SVB, zorgverleners en budgethouders en over de opzet van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld.

Hierbij maken wij gebruik van de carv-out methode (exclusieve methode). De beschrijving omvat de interne beheersingsdoelstellingen en de daarmee verband

houdende interne beheersingsmaatregelen van de subservice-organisatie (ODC- Noord) die in relatie staan tot het zorgdomein van het PGB2.0-systeem.

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de ontwikkelorganisatie en onderdelen van de beschrijving in sectie III, zijnde paragraaf 3.3 Beheerskader en paragraaf 3.5 Verantwoordelijkheden in de Keten en brengen daarover geen oordeel tot uitdrukking.

Deze assurance-rapportage brengen wij uit aan de opdrachtgever van deze opdracht, de pSG VWS, mw. A.I. Norville MSc. De opdrachtgever is eigenaar van deze rapportage.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

Ondertekening

Den Haag, 18 mei 2022

Projectleider
Auditdienst Rijk

Auditdienst
Rijk Postbus
20201 2500 EE
Den Haag
(070) 342 77
00

Ministerie van Volksgezondheid,
Welzijn en Sport

Sectie III Systeembeschrijving

Beschrijving PGB2.0

3. Sectie III: Beschrijving PGB2.0

3.1 Introductie, doelstelling en scope van de beschrijving

3.1.1 Introductie en doelstelling van de beschrijving

Onderstaande beschrijving beschrijft het pgb-proces, het PGB2.0 programma, het PGB2.0 systeem en het PGB2.0 beheer. In de beschrijving van het PGB2.0 systeem is de scope beperkt tot het Zorgdomein gedeelte van het PGB2.0 systeem. De onderverdeling Zorgdomein en Financieel domein in het PGB2.0 systeem wordt toegelicht in H3.4.
Deze beschrijving is opgesteld voor de SVB en gemeenten en zorgkantoren die gebruik hebben gemaakt van het Zorgdomein van het PGB2.0-systeem van VWS en, indien van toepassing, hun accountants, die voldoende inzicht hebben om het in aanmerking te nemen bij het inschatten van de risico's op afwijkingen van het materieel belang in de financiële overzichten van de SVB, gemeenten en zorgkantoren tezamen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door hun zelf worden uitgevoerd.

3.1.2 Scope van deze beschrijving

Deze beschrijving is zo opgesteld dat hij zelfstandig gelezen kan worden. Niet alle onderdelen van deze beschrijving vallen onder de reikwijdte van de assurance-opdracht zoals door de plv. secretaris-generaal van het ministerie van VWS verstrekt aan de Auditdienst Rijk. Hieronder worden de onderdelen van de beschrijving opgesomd.

Buiten de reikwijdte van de assurance-opdracht

- Paragraaf 3.2 Het pgb-proces. Bij het beschrijven van dit proces is per processtap aangegeven welke delen van het proces wel en niet door het PGB2.0 systeem ondersteund worden, waarmee toegelicht wordt op welke delen van het pgb-proces de interne beheersdoelstellingen en –maatregelen betrekking hebben die in het onderzoek beoordeeld zijn.
- Paragraaf 3.3 Programma PGB2.0, waaronder de programmadoelstelling, de programmastructuur, de primaire functies en de primaire rollen. De functies en rollen in de programmastructuur waarop de interne beheersdoelstellingen en -maatregelen betrekking hebben worden toegelicht in H3.5 Beheerskader PGB2.0.

Binnen de reikwijdte van de assurance-opdracht

- Paragraaf 3.4 (De productie omgeving van het) Zorgdomein van het PGB2.0 systeem
- Paragraaf 3.5 Het Beheerskader PGB2.0, met daarin:
    - de diensten Technisch, Functioneel, Applicatie- en Technisch Applicatiebeheer en waar deze belegd zijn
    - de beheerprocessen in deze diensten
    - het voortbrengingsproces (softwareontwikkeling)

- monitoring op deze diensten en processen
- de interne beheersmaatregelen in het Zorgdomein, uitgedrukt in Application Controls, IT-dependent Controls en General IT Controls, zoals vastgelegd in bijlage 3 bij het Control Framework PGB2.0 v1.2 en vastgesteld in de Programmaraad van 11 maart 2021.

3.2 Het PGB Proces

3.2.1 Introductie

Een persoonsgebonden budget (pgb) is een geldbedrag dat toegekend wordt door een gemeente, zorgkantoor of zorgverzekeraar waarmee een persoon (de budgethouder) zelf zorg of hulp in kan kopen. De budgethouder kan daarmee zelf kiezen welke zorg hij/zij krijgt en van wie. Dit in tegenstelling tot 'zorg in natura', waarbij de gemeente, het zorgkantoor of de zorgverzekeraar een zorgaanbieder kiest waar zij (vaak) een contract mee heeft. Als een budgethouder zelf een zorgverlener uitkiest en deze uit het toegekende budget wil laten betalen, dan zal de budgethouder een contract met de zorgverlener moeten sluiten; de zorgovereenkomst.

In Nederland hebben ruim 100.000 mensen een persoonsgebonden budget, met een totale waarde van ruim 3,5 miljard euro[1]. In ruim 223.000 zorgovereenkomsten hebben zij afspraken vastgelegd met ruim 139.000 zorgverleners.
In april 2021 maakten 11773 budgethouders gebruik van het PGB2.0 systeem, in oktober was dat aandeel gestegen tot 23747 door de aansluiting van zorgkantoor ENO, en de aansluiting van 4 extra zorgkantoor regio's van Zilveren Kruis en 1 extra regio van zorgkantoor CZ[2].

De uitvoering van de pgb wetten en regelingen is belegd bij de SVB, gemeenten, zorgkantoren en zorgverzekeraars. De SVB beheert daarbij het budget, en voert betalingen uit in opdracht van de budgethouder. De budgethouder heeft dus zelf niet rechtstreeks de beschikking over het budget. Deze werkwijze is in 2015 ingevoerd en wordt het 'pgb trekkingsrecht' genoemd.

3.2.2 Wetgeving pgb

Het verkrijgen van een persoonsgebonden budget (pgb) is een wettelijk recht dat is vastgelegd in de Wet maatschappelijke ondersteuning 2015 (Wmo), de Jeugdwet (Jw), de Wet langdurige zorg (Wlz), en de Zorgverzekeringswet (Zvw). Op dit moment ondersteunt het PGB2.0-systeem pgb's via de Wmo, Jw en Wlz.

Kenmerken pgb Wmo

- Hiermee kan men hulpmiddelen, zorg, woonvoorziening en ondersteuning inkopen.
- De gemeente waar de cliënt woont is de verstrekker van het budget.
- De gemeente beoordeelt of de cliënt het aangevraagde nodig heeft.

[1] Bron: SVB Kengetallen PGB oktober 2021

[2] Bronnen: Maandrapportage TBO april 2021, Maandrapportage TBO oktober 2021

- De gemeente beoordeelt of de cliënt of vertegenwoordiger bekwaam genoeg is om de verantwoordelijkheden die horen bij het pgb te dragen.

Kenmerken pgb Jw

- In de Jeugdwet is het wettelijk recht op zorg vervangen door zorgplicht. De gemeente is alleen verplicht een voorziening te treffen als het kind en zijn ouders er op eigen kracht niet uitkomen.
- De gemeente beslist of en welke voorziening het kind nodig heeft.
- Met het budget kan men zorg en ondersteuning inkopen.
- De gemeente waar de cliënt woont is de verstrekker van het budget.
- De gemeente beoordeelt of de cliënt het aangevraagde nodig heeft.
- De gemeente beoordeelt of de vertegenwoordiger bekwaam genoeg is om de verantwoordelijkheden die horen bij het pgb te dragen.

Kenmerken pgb Wlz

- Is bedoeld om langdurige, intensieve zorg in te kopen.
- Het Centraal Indicatieorgaan Zorg (CIZ) beslist op welke zorg de cliënt recht heeft.
- Het zorgkantoor van de regio waar de cliënt woont is de verstrekker van het budget.
- Het zorgkantoor beoordeelt of de cliënt of de vertegenwoordiger bekwaam genoeg is om de verantwoordelijkheden die horen bij het pgb te dragen.
- Een pgb onder de Wlz kan worden gecombineerd met andere leveringsvormen van zorg onder de Wlz: zorg in natura (zin) en modulair pakket thuis (mpt).

Kenmerken pgb Zvw

- Is bedoeld om persoonlijke verzorging van volwassenen, verpleging van volwassenen en kinderen en begeleiding & kortdurend verblijf in te kopen.
- Een verpleegkundige beoordeelt welke zorg de cliënt nodig heeft en geeft daarvoor een verwijzing af.
- Gemaakte kosten worden vergoed door de zorgverzekeraar waar de cliënt een basis zorgverzekering heeft afgesloten.
- Alleen als er sprake is van loondienst en de budgethouder kiest voor ondersteuning door de SVB heeft de SVB een taak in het afhandelen van declaraties en de verrekening daarvan.

Een budgethouder kan tegelijkertijd persoonsgebonden budgetten uit meerdere wetten hebben, de combinaties in onderstaande tabel zijn mogelijk.

	Wmo	**Jw**	**Wlz**	**Zvw**
Wmo		Kan	kan	Kan
Jw	Kan		kan niet	Kan
Wlz	Kan	kan niet		kan niet
Zvw	Kan	Kan	kan niet	

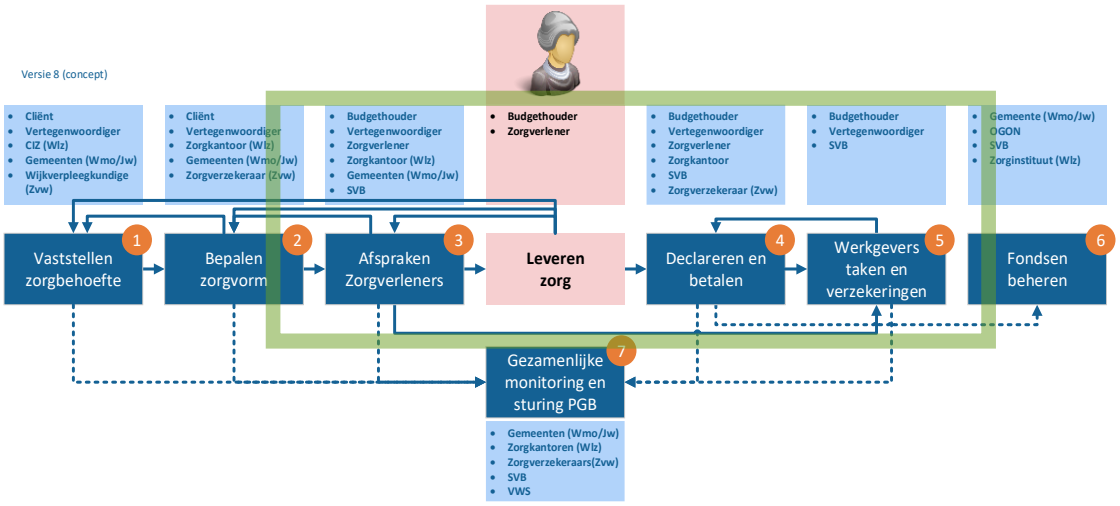
3.2.3 Belangrijke kenmerken budgetten

Het is mogelijk om het Wmo-budget of Jw-budget beschikbaar te stellen als een of meer functiebudgetten. Ieder functiebudget is een deelbudget en kan in principe alleen aan een specifieke vorm van zorg (zorgfunctie) besteed worden en kent zijn eigen uitputting. Of een budgethouder zijn budget als één budget krijgt of als functiebudgetten is een keuze van de verstrekker per budgethouder. Er is geen sprake van schotten tussen functiebudgetten.

In sommige gevallen kan een cliënt budgethouder zijn van meerdere budgetten. Een budget i.h.k.v. de Wlz kan gecombineerd worden met een Wmo- budget. Een budget van de Zvw kan gecombineerd worden met een budget van de Wmo of Jw.
Een overgang van één budget naar een ander budget vraagt aandacht en samenwerking tussen de uitvoerders. Een voorbeeld hiervan is het meerderjarig worden van de cliënt waardoor deze van Jw naar Wlz overgaat. Hierbij is het zaak om de daarvoor benodigde administratie zo te laten verlopen dat de continuïteit van de zorg niet in het geding komt. Omdat budgetten verbonden zijn aan individuele verstrekkers speelt vergelijkbare complexiteit bij verhuizingen van budgethouders naar een andere regio en gemeente.

3.2.4 Het pgb proces

Onderstaande figuur geeft schematisch het pgb proces weer, alsmede groen omkaderd welke delen van het proces door het PGB2.0-systeem (Zorgdomein + Financieel domein) ondersteund worden.



Figuur 1 Overzicht pgb proces

Hieronder worden de onderdelen van het proces toegelicht, daarbij wordt aangeven welke delen van het proces ondersteund worden door het PGB2.0 systeem. Alle onderdelen van het proces worden beschreven voor een goed begrip van het proces. Alleen die delen van het proces die ondersteund worden door het Zorgdomein van het PGB2.0 systeem vallen binnen de scope van de vermelding van VWS in sectie I en de beoordeling daarvan in sectie II. Daar waar papieren stromen benoemd worden maken de beheersmaatregelen voor de verwerking van papieren stukken (inclusief het inscannen door SVB en verstrekkers) geen deel uit van de scope van de vermelding van VWS in sectie I.

Conversie PGB1.0 -> PGB2.0
Hieronder wordt het pgb-proces volgordelijk beschreven_vanaf het moment dat een budgethouder een (nieuw) budget krijgt toegekend. Nagenoeg alle huidige (en toekomstige) budgethouders die met PGB2.0 (gaan) werken hebben echter al een pgb, hebben zorgovereenkomsten afgesloten met zorgverleners, en zijn al bezig het budget te benutten op het moment dat ze PGB2.0 gaan gebruiken. Bij de overstap naar PGB2.0 zorgt TBO er in samenwerking met de betreffende

verstrekkers (zorgkantoren, gemeenten) voor dat de gegevens in het PGB1.0 systeem van de SVB overgezet worden naar PGB2.0 (conversie). Ook leveren de verstrekkers opnieuw gegevens aan PGB2.0 (de toekenningen worden niet geconverteerd uit de systemen van de SVB maar opnieuw aangeleverd door de verstrekkers). Bovendien worden als onderdeel van de conversie gegevens geverifieerd bij externe bronnen als de Basis Registratie Personen en het AGB register. De aansluitingen van verstrekkers en hun budgethouders aan PGB2.0 worden opgeknipt in hanteerbare aantallen van (inmiddels) 5000-10.000 budgethouders per keer. Dit betekent dat er in zijn totaliteit tenminste 10-20 conversies plaatsvinden voordat PGB2.0 geheel is ingevoerd. Elke conversie wordt meerdere keren geoefend in een proefconversie, waarin de daadwerkelijk te converteren gegevens worden getest, en de nieuwe verstrekkers bekend raken met het conversieproces. Voor elke conversie wordt een draaiboek opgesteld en worden mijlpalen in het proces vastgelegd in een dossier.

Bij het daadwerkelijk converteren worden gegevens gecontroleerd en verrijkt, en bij het inlezen van die gegevens worden in PGB2.0 dezelfde application controls doorlopen als die de budgethouders of zorgverleners zouden ervaren (uitgezonderd de interactieve elementen in een control). Hoewel in het conversieproces diverse maatregelen ingebouwd zijn om de kwaliteit van de te converteren gegevens te waarborgen en verbeteren, is uit een met de SVB, ZN en NBA uitgevoerde analyse gebleken dat er geen assurance bereikt kan worden op de geconverteerde gegevens. Ten eerste rust er geen assurance op de oorspronkelijke deelverzamelingen van gegevens die per verstrekker geconverteerd worden, omdat de SVB over pgb1.0 assurance op wetsniveau afgeeft. Ten tweede is het creëren van assurance op verstrekker niveau praktisch onhaalbaar gebleken. De Programmaraad PGB2.0 heeft daarom ingestemd met een adviestraject op het conversieproces door BakerTilly. Het adviesrapport is inmiddels opgeleverd.

Als laatste wordt nog opgemerkt dat bepaalde gegevens in PGB1.0 niet of in een hoger abstractie niveau worden vastgelegd dan interactieve invoer via PGB2.0 bewerkstelligd zou hebben. Het belangrijkste voorbeeld is de beschrijving van de zorg en ondersteuning in de zorgovereenkomst. In PGB1.0 volstaat het vastleggen van het tarief (p) en de hoeveelheid (q), terwijl in PGB2.0 ook de zorginhoud (de zorgfunctie) geduid moet worden. De zorgkantoren hebben met de NZa afgesproken dat zij binnen drie jaar na overstappen op PGB2.0 zorgdragen voor aanvulling van de zorgovereenkomsten door de budgethouder.

3.2.4.1 Vaststellen zorgbehoefte en bepalen zorgvorm

Het proces van vaststellen van de zorgbehoefte en het bepalen van de zorgvorm wordt niet ondersteund door het PGB2.0 systeem, en valt derhalve in zijn geheel buiten de scope van de vermelding van VWS in sectie I. Het proces wordt hier toegelicht ter informatie.

Het proces van het vaststellen van de zorgbehoefte verschilt per wet. In de Wlz neemt het Centraal Indicatieorgaan Zorg (CIZ) een indicatiebesluit. Middels het afgeven van het besluit is de zorgbehoefte erkend, en de omvang van de zorg bepaald. In de WMO en Jeugdzorg stelt de gemeente de zorgbehoefte vast. De vastgestelde zorgbehoefte is de basis van de omvang van de leveren zorg, en daarmee medebepalend voor de hoogte van het pgb als er voor de leveringsvorm pgb gekozen wordt.

De gemeente of het zorgkantoor is wettelijk verplicht een maatwerkvoorziening in de vorm van een pgb aan te bieden, maar is niet zonder meer verplicht een pgb te verstrekken, bijvoorbeeld als een standaard voorziening ook zou voldoen aan de zorg/hulpvraag. Bovendien moet de budgethouder en de aangevraagde zorg/ondersteuning aan een aantal voorwaarden voldoen.

De activiteiten, vereisten, voorwaarden en risico's bij het aanvragen en toekennen van een pgb worden hier verder niet uitgewerkt omdat dit onderdeel van het proces buiten de scope van dit rapport ligt.

3.2.4.2 Toekennen pgb

Buiten de scope van het Zorgdomein van het PGB2.0-systeem
De verstrekker (gemeente, zorgkantoor, op termijn zorgverzekeraar) voert gesprekken met de (aspirant) budgethouder over de voorwaarden voor het toekennen van een persoonsgebonden budget. Als de verstrekker besluit tot het toekennen van een pgb geeft de verstrekker een beschikking af aan de (aspirant) budgethouder. Tevens stuurt de verstrekker een toekenningsbericht naar het PGB2.0-systeem.

Binnen de scope van het Zorgdomein van het PGB2.0-systeem
Het zorgdomein van het PGB2.0-systeem ontvangt het elektronische toekenningsbericht van de verstrekker. Toekenningsberichten van zorgkantoren worden ontvangen via Vecozo[3], toekenningsberichten van gemeenten worden door hen middels een upload functionaliteit ingevoerd in het zorgdomein. Op het moment dat deze vastlegging plaatsvindt worden de budgethouder en de SVB hierover geïnformeerd via het Zorgdomein van het PGB2.0-systeem. Na het verwerken van het toekenningsbericht krijgt de budgethouder toegang tot het PGB2.0-systeem middels Digid. Het toekenningsbericht bevat hiertoe het BSN van de budgethouder. Onjuiste of ongeldige toekenningsberichten worden door het systeem geweigerd, deze controles worden toegelicht in bijlage 3 van het Control Framework PGB2.0. Voor elk aangeboden toekenningsbericht wordt een retourbericht aan de zender gestuurd met de status van de verwerking.

3.2.4.3 Vastleggen profielgegevens

Buiten de scope van het Zorgdomein van het PGB2.0-systeem
De budgetverstrekker legt profielgegevens van de budgethouder vast in het systeem van de verstrekker.

Binnen de scope van het Zorgdomein van het PGB2.0-systeem
Middels het verwerken van het elektronische toekenningsbericht wordt het BSN van de budgethouder automatisch vastgelegd in PGB2.0. Hiermee ontstaat ook de mogelijkheid dat de budgethouder middels Digid kan inloggen in het Zorgdomein van PGB2.0.[4] Vervolgens worden de profielgegevens van de budgethouder aangevuld door het opvragen van gegevens uit de Basis Registratie Personen. De budgethouder kan deze profielgegevens aanpassen, waarbij er invoercontroles zoals genoemd in bijlage 3 van het Control Framework PGB2.0 worden toegepast.

Zorgverleners worden in het systeem gedefinieerd tijdens het aanmaken van een zorgovereenkomst door de budgethouder. De budgethouder kan daarbij kiezen uit reeds in het systeem aanwezige zorgverleners, of een nieuwe zorgverlener specificeren.. De zorgverlener krijgt daardoor toegang tot het systeem, waarna de zorgverlener zijn of haar profielgegevens kan completeren, ook daarop zijn invoercontroles actief.

[3] VECOZO staat voor veilige communicatie in de zorg. Zij zorgen voor veilige en efficiënte uitwisseling van administratieve gegevens in de zorg. Voor meer informatie: https://www.vecozo.nl
[4] In de praktijk 'het PGB Portaal' genoemd, https://www.mijnpgb.nl/

3.2.4.4 Zorgovereenkomsten

Buiten de scope van het Zorgdomein van het PGB2.0-systeem
De budgethouder voert onderhandelingen met de (aspirant) zorgverlener(s) en maakt afspraken over de levering van zorg & ondersteuning en de beloning. Daarbij kan de budgethouder gebruik maken van informatie op de website van de SVB.
In de Wlz is de budgethouder verplicht een budgetplan op te stellen en naar het zorgkantoor te sturen. PGB2.0 biedt geen ondersteuning voor het opstellen van een budgetplan. Vaak hebben budgethouders al een of meerdere zorgovereenkomsten met zorgverleners op het moment dat zij gebruik gaan maken van het PGB2.0-systeem. Deze zijn in een eerder stadium op papier naar de SVB gezonden, en de SVB heeft gegevens uit deze zorgovereenkomsten overgenomen in de PGB 1.0 applicatie van de SVB.

Binnen de scope van het Zorgdomein van het PGB2.0-systeem
Het is verplicht voor de budgethouder om een overeenkomst met een zorgverlener op te stellen conform een van de vier modelovereenkomsten zoals gepubliceerd op de website van de SVB. Het zorgdomein van het PGB2.0-systeem ondersteunt digitale vastlegging en ondertekening van zorgovereenkomsten op een wijze dat gewaarborgd is dat deze digitale zorgovereenkomsten alle gegevens bevatten uit de modelovereenkomsten van de SVB.

De functionaliteit in het zorgdomein van het PGB2.0-systeem t.b.v. het vastleggen van nieuwe zorgovereenkomsten of wijzigingen op bestaande zorgovereenkomsten valt onder te verdelen in twee primaire processen:

<u>Opstellen zorgovereenkomst</u>
Digitale stroom: de budgethouder legt de afspraken elektronisch vast in een (concept) zorgovereenkomst(en) in het Zorgdomein van het PGB2.0-systeem, in afstemming met de (beoogde) zorgverlener(s). Er zijn momenteel vier soorten zorgovereenkomsten, de budgethouder kiest op basis van zijn of haar relatie met de zorgverlener de juiste zorgovereenkomst. De budgethouder stelt de zorgovereenkomst op volgens een van de vier modelovereenkomsten zoals die door de SVB beheerd worden, de schermen van het zorgdomein en de daarop verplichte velden zijn zo ontworpen dat zij in de pas lopen met deze modelovereenkomsten. De noodzakelijk in te voeren gegevens zijn gespecificeerd in bijlage 3 van het Control Framework PGB2.0. Hiermee wordt gewaarborgd dat alle benodigde gegevens vastgelegd worden. Ook vinden op de gegevens invoercontroles plaats. De zorgovereenkomst wordt na het opstellen (inclusief digitale accordering door budgethouder en zorgverlener) op een werklijst voor de verstrekker en SVB geplaatst ter beoordeling[5].

Papieren stroom: de zorgovereenkomst wordt door de budgethouder en zorgverlener op papier opgesteld en ondertekend.
Als de Wlz van toepassing is, wordt de zorgovereenkomst door de budgethouder opgestuurd naar het zorgkantoor. Het zorgkantoor scant de zorgovereenkomst zelf in het PGB2.0-systeem (‘digitale kopie’). Het systeem herkent een aantal gegevens van de digitale kopie, en niet te herkennen gegevens worden aangevuld door de medewerker van het zorgkantoor. Hierbij worden dezelfde invoercontroles toegepast als in de situatie dat de budgethouder de zorgovereenkomst zelf invoert. De medewerker van het zorgkantoor bevestigt vervolgens de invoer van de gegevens uit de zorgovereenkomst en beoordeelt de zorgovereenkomst.

[5] In de Wlz vindt integrale beoordeling plaats door het zorgkantoor, in de WMO en JW is de beoordeling verdeeld over de gemeente en de SVB

In geval de Wmo/Jw van toepassing zijn, stuurt de budgethouder de overeenkomst naar de SVB, de SVB scant de overeenkomst in het PGB2.0-systeem in en neemt de gegevens over, en het systeem plaatst de zorgovereenkomst op een werklijst ter beoordeling door de gemeente.
Bovenstaande werkwijze geldt ook voor wijzigingen op bestaande zorgovereenkomsten.

Beoordelen en goedkeuren zorgovereenkomst
In deze stap wordt de in de voorgaande stap opgestelde en ingevoerde zorgovereenkomst beoordeeld door de SVB en de verstrekker. Deze beoordeling kent een aantal componenten, namelijk

a) een toets of het juiste type zorgovereenkomst is gebruikt;
b) een toets op het recht en het belang van de uitvoerbaarheid van het persoonsgebonden budget en het budgetbeheer (de 'arbeidsrechtelijke' toets) zoals vastgelegd in bijlage 2 bij het Control Framework PGB2.0;
c) een toets op de weergave/omschrijving van de wijze waarop de zorgverlener/ondersteuner voorziet in de behoefte aan zorg/ondersteuning van de budgethouder (buiten de scope van de vermelding van VWS in sectie I);
d) bij langdurige zorg een toets of er sprake is van langdurige zorg zoals gespecificeerd in de regeling langdurige zorg (buiten de scope van de vermelding van VWS in sectie I).

Het zorgdomein van het PGB2.0-systeem ondersteunt de SVB en de verstrekker bij het uitvoeren van punten a) en b) met een mix van invoer- en verband controles. Er zijn echter ook handmatige controles nodig door medewerkers van de SVB en verstrekkers. Een en ander is gespecificeerd in bijlagen 2 en 3 van het Control Framework PGB2.0.

3.2.4.5 Declareren

Buiten de scope van het Zorgdomein van het PGB2.0-systeem
Als de zorgverlener niet met het PGB2.0-systeem werkt, stuurt de zorgverlener papieren facturen of urenstaten naar de budgethouder.

Binnen de scope van het Zorgdomein van het PGB2.0-systeem
In het primaire proces van leveren en declareren van zorg en ondersteuning wordt het volgende onderscheid gemaakt:

Invoeren geleverde zorg: Er worden de volgende situaties onderscheiden:

- Digitale stroom: voor een zorgovereenkomst waarbij een uurtarief is afgesproken voert de zorgverlener zijn/haar uren/factuur elektronisch in. Tijdens de invoer vinden controles plaats zoals gespecificeerd in bijlage 3 van het Control Framework PGB2.0 opdat de gegevens in de latere declaratie passen binnen de afspraken die in de zorgovereenkomst zijn vastgelegd.
- Papieren stroom: er zijn twee scenario's mogelijk:
  - 100% papier: de zorgverlener levert op papier urenbriefjes of een factuur aan bij de budgethouder, de budgethouder voorziet door hem/haar beoordeelde en goedgekeurde facturen of urenbriefjes van een handtekening en stuurt deze door naar de SVB, die deze vastlegt in het PGB2.0-systeem (mits deze voldoet aan de wettelijke vereisten).
  - Hybride papier-digitaal: de zorgverlener levert op papier urenbriefjes of een factuur aan bij de budgethouder, de budgethouder neemt de gegevens van de papieren factuur/urenbriefjes van de zorgverlener over en voert deze in het PGB2.0-systeem in (hiermee dient de budgethouder tevens de declaratie in).
- Voor een arbeidsovereenkomst en voor een Overeenkomst van Opdracht waarbij een periodieke vergoeding is afgesproken, wordt de geleverde zorg niet periodiek ingevoerd of bevestigd (het

systeem genereert automatisch een betaling op basis van de in de overeenkomst vastgelegde periodieke vergoeding).

Declareren van geleverde zorg: Ook hier zijn meerdere situaties aan de orde:

- Digitale stroom: de budgethouder keurt de digitaal ingevoerde uren/factuur van de zorgverlener digitaal goed door het drukken op een knop. Hiermee dient de budgethouder een declaratie in conform de betekenis van de wet- en regelgeving. Daarbij is het uitgangspunt dat als een budgethouder deze uren/facturen goedkeurt hij hiermee verklaart dat de bedoelde zorg ook daadwerkelijk geleverd is[6].
- Papieren stroom:
  - 100% papier: de van de budgethouder ontvangen getekende factuur of urenbriefjes worden door de SVB als een declaratie beschouwd zoals bedoeld in de wet- en regelgeving. De SVB draagt zorg voor een tijdige, juiste en volledige invoer van de ontvangen declaraties in het PGB2.0-systeem. In het geval dat deze papieren declaratie niet voldoet aan de wettelijke eisen wordt de declaratie niet ingevoerd in het systeem[7]. In dit 100% papier-scenario is de budgethouder nog steeds de formele declarant, de SVB doet niet meer dan het vastleggen van de gegevens van de papieren declaratie in het PGB2.0-systeem.
  - Hybride papier-digitaal: de budgethouder declareert digitaal door het invoeren van de geleverde zorg op basis van de papieren urenbriefjes/ factuur van de zorgverlener.
  - Betaling van een overeengekomen periodiek maandbedrag vindt plaats zonder dat de budgethouder daarvoor maandelijks uren/declaraties invoert[8] .

Declareren bijkomende zorgkosten en vervoerskosten: Naast de voornoemde vormen van declaraties kent het PGB-stelsel nog declaraties voor bijkomende zorgkosten en vervoerskosten.

- Digitale stroom: de budgethouder voert specifieke declaraties in het PGB2.0-systeem in om een vergoeding aan de verstrekker te vragen voor kosten die geen verband houden met de gewerkte uren van de zorgverlener. Daarbij kan het gaan om cursus zorgverlener, entreegeld zorgverlener, maaltijden zorgverlener bij overwerk/consumpties, wooninitiatief zorg en wooninitiatief enkel huis, feest- en eindejaarsuitkering, vervoerskosten (aan professionele vervoerders).
- Papieren stroom: de van de budgethouder ontvangen declaraties worden door de SVB als een declaratie beschouwd zoals bedoeld in de wet- en regelgeving. De SVB draagt zorg voor een tijdige, juiste en volledige invoer van de ontvangen declaraties in het PGB2.0-systeem. In het geval dat deze papieren declaratie niet voldoet aan de wettelijke eisen wordt de declaratie niet ingevoerd in het systeem.
- De ingevoerde declaratie wordt ter beoordeling aan de verstrekker aangeboden[9]. De verstrekker controleert of de vergoeding die aangevraagd wordt doelmatig, verantwoord en

---

[6] Het PGB2.0-systeem bevat daarmee gegevens die de verstrekkers in staat stellen data analyses uit te voeren ten behoeve van een risicogerichte controle op feitelijke levering (het PGB2.0-systeem voert zelf geen controles op feitelijk levering uit). De NBA heeft in de SDO-Notitie "Controle interne beheersing Jeugd en Wmo voor gemeenten en accountants een best practice voor de controle op feitelijke levering opgesteld, https://www.nba.nl/globalassets/themas/thema-publieke-sector/sdo/sdo-notitie-controle-interne-beheersing-jeugd-wmo-gemeenten-accountants-januari2019.pdf.
ZN heft voor de zorgkantoren in afstemming met de NZa een leidraad t.b.v. controle op feitelijke levering opgesteld.

[7] Het systeem zal invoer middels invoercontroles verhinderen als de declaratie niet aan de wettelijke eisen voldoet. De SVB bepaalt of een declaratie die niet ingevoerd kan worden, wordt geretourneerd aan de budgethouder, of dat deze terzijde gelegd wordt totdat de budgethouder aanvullende gegevens heeft verstrekt. In het laatste geval zal de SVB maatregelen moeten treffen opdat aanvullend verstrekte gegevens tijdig bij de juiste terzijde gelegde declaratie gevoegd worden.

[8] Met uitzondering van eventuele aanvullende declaraties t.b.v. vervoerskosten, bijzondere zorgkosten, feestdagenuitkering, transitievergoeding, eenmalige uitkering bij overlijden budgethouder.

[9] Niet voor alle categorieën declaraties, op het moment van schrijven geldt dit voor vervoerskosten.

noodzakelijk is. In geval van wooninitiatieven toetst de verstrekker aanvullend of er recht is op deze toeslag en of deze wordt gebruikt waar hij voor bedoeld is. De verstrekker besluit of de betaling rechtmatig kan worden gedaan, en legt de beoordeling van de declaratie vast in het systeem.

Declaratie verantwoordingsvrij bedrag

Bij de toekenning van het budget heeft het zorgkantoor of de gemeente bepaald of de budgethouder recht heeft op een verantwoordingsvrij bedrag. De budgethouder mag dit zonder verantwoording gebruiken voor uitgaven zoals bijvoorbeeld telefoonkosten of het lidmaatschap van een patiëntenvereniging. De budgethouder ziet in het toekenningsbesluit of het budgetoverzicht of de gemeente of zorgkantoor een verantwoordingsvrij bedrag heeft toegekend. De budgethouder kan uitbetaling van het verantwoordingsvrije bedrag opvragen middels het systeem of middels een formulier. Het verantwoordingsvrije bedrag maakt onderdeel uit van het pgb.

Bij het invoeren van declaraties vinden invoercontroles plaats zoals toegelicht in bijlage 3 van het Control Framework PGB2.0.

3.2.4.6 Betaalopdrachten aan het financieel domein

Binnen de scope van het Zorgdomein van het PGB2.0-systeem
Het zorgdomein genereert een 'OK-2-pay' bericht aan het financieel domein als alle voorgaande, in bijlage 3 van het Control Framework PGB2.0 gespecificeerde, controles op toekenningsbericht, zorgovereenkomst en declaratie succesvol doorstaan zijn. Het F-domein geneert op basis van dit bericht een betaalopdracht aan de bank op basis van profielgegevens van de zorgverleners zoals die opgeslagen zijn in het zorgdomein.
Het zorgdomein genereert daarnaast zelfstandig betaalopdrachten (in 'runs') voor geleverde zorg waarvoor periodieke maandelijkse bedragen afgesproken zijn.

3.2.4.7 Ondersteunen van werkgeverstaken

De SVB heeft bij wet de verantwoordelijkheid gekregen om budgethouders te ondersteunen in hun werkgeverstaken. De ondersteuning van de SVB bestaat uit onderstaande taken, waarbij voor de dikgedrukte onderdelen functionaliteit in de Zorgdomein applicatie aanwezig is.

- **Loondoorbetaling aan de zorgverlener bij ziekte van de zorgverlener.**
- **Looncompensatie aan de budgethouder door de SVB.**
- **Maandbetaling nabestaanden bij overlijden zorgverlener en de eenmalige uitkering bij overlijden budgethouder (inclusief het verstrekken van jaaropgaven).**
- **Het voeren van de salarisadministratie bij volledig werkgeverschap (als de budgethouder dat wenst).**
- Het doen van afdrachten loonheffingen en betalen van premies bij werkgeverschap.
- Het faciliteren van Arbo-dienstverlening; dit bestaat uit het beschikbaar stellen van een Arbodienst ten behoeve van de budgethouder in zijn rol als werkgever.
- Het betalen van re-integratietrajecten tijdens het eerste en tweede spoor van zieke zorgverlener, waaronder eventuele bijscholing.
- Ondersteuning van de budgethouder als werkgever bij zieke zorgverlener (Wet verbetering poortwachter). Dit bestaat uit het adviseren van de budgethouder bij ziekte van zijn

zorgverlener ten aanzien van zijn verplichtingen en verantwoordelijkheden als werkgever, zodat een loonsanctie of een bestuurlijke boete wordt voorkomen.
- Ondersteuning van de budgethouder als werkgever bij een zwangere zorgverlener.
- Het ondersteunen van de budgethouder bij loonbeslag en derdenbeslag.
- Het beoordelen van een aanvraag voor een transitievergoeding en het betalen daarvan.

Ad bolletje 1 Loondoorbetaling aan de zorgverlener bij ziekte van de zorgverlener
De budgethouder is als werkgever verplicht een zorgverlener door te betalen indien deze niet in staat is de bedongen arbeid te verrichten (7:629 BW).
Het zorgdomein ondersteunt de medewerker van de SVB in het berekenen en uitvoeren van de loondoorbetaling door middel van een werktaak. De SVB-medewerker bepaalt op basis van de ziekmelding en de gegevens in de zorgovereenkomst in het Zorgdomein de hoogte en duur van de doorbetaling, het Zorgdomein maakt op basis daarvan de (door)betalingsopdrachten aan.

Ad bolletje 2 Looncompensatie aan de budgethouder door de SVB.
De SVB compenseert i.v.m. haar wettelijke taak alsmede afspraken met VWS de budgetgelden die een budgethouder kwijt is aan een zieke zorgverlener teneinde de budgethouder in staat te stellen vervangende zorg in te kopen. Het Zorgdomein van het PGB2.0-systeem verhoogt hiertoe automatisch de budgetruimte met dezelfde bedragen als de berekende loondoorbetalingen.

Ad bolletje 3 Maandbetaling nabestaanden bij overlijden zorgverlener en de eenmalige uitkering bij overlijden budgethouder (inclusief het verstrekken van jaaropgaven).
Als een zorgverlener overlijdt kunnen de nabestaanden van de zorgverlener een overlijdensuitkering van een (gemiddeld) maandloon krijgen. De nabestaanden kunnen deze uitkering krijgen als er een arbeidsovereenkomst was. De SVB bepaalt de hoogte van deze betalingen op basis van de informatie die in het Zorgdomein PGB2.0 is vastgelegd.

Ad bolletje 4 Het voeren van de salarisadministratie bij volledig werkgeverschap (als de budgethouder dat wenst).
De zorgverlener ontvangt loon of vergoeding uit het pgb. De zorgverlener moet hierover belasting en premies betalen. Budgethouder en zorgverlener kunnen er samen voor kiezen de belasting en premies vooraf te betalen aan de Belastingdienst. Dan doet de SVB de salarisadministratie voor de budgethouder. De SVB voert die salarisadministratie in het Financieel domein op basis van de gegevens in de Zorgdomein PGB2.0 applicatie.

In bepaalde gevallen is de budgethouder zelfs verplicht om de salarisadministratie door de SVB te laten doen. Dit hangt af van het soort overeenkomst dat is afgesloten (Arbeidsovereenkomst met >= 4 dagen werk per week). Het Zorgdomein PGB2.0 zorgt er voor dat de budgethouder hiervan op de hoogte wordt gesteld en de budgethouder de SVB machtigt de salarisadministratie uit te voeren.

3.2.4.8 Rapportages over het verwerkingsproces

Dagelijks krijgen de SVB, gemeenten en zorgkantoren via een veilige verbinding een op hun naam afgesplitste database van alle transacties die met bovenstaande processtappen verband houden. De SVB, gemeenten en zorgkantoren kunnen vervolgens naar eigen inzicht tellingen en analyses uitvoeren op deze transacties uit het PGB2.0-systeem.

3.3 Programma PGB2.0

3.3.1. Doelstelling Programma PGB2.0

Het PGB2.0 systeem maakt onderdeel uit van een langlopend programma ter verbetering van de administratieve ondersteuning van de budgethouders, het verbeteren van de mogelijkheid voor de budgethouder eigen regie te voeren, het beter faciliteren van fraudeopsporing, het verlagen van uitvoeringskosten binnen de keten en het vergroten van de rechtmatigheid van de uitvoering van het pgb-trekkingsrecht. Om deze doelstelling te bereiken hebben voorafgaand aan de controleperiode reeds deze activiteiten plaatsgevonden:

- opzetten, inrichten en aansturen van de TBO;
- in samenspraak met de ketenpartijen definiëren en vormgeven van werkprocessen die betrekking hebben op het trekkingsrecht in combinatie met het PGB2.0-systeem, om zo te komen tot vastgestelde ketenprocessen;
- voorbereidingen treffen voor het doorvoeren van de wijzigingen in de taken en verantwoordelijkheden van verstrekkers vóór invoering. Het tijdig realiseren van deze wijzigingen is een verantwoordelijkheid van de verstrekkers;
- vereenvoudiging en standaardisatie van de uitvoering van het pgb-trekkingsrecht; zowel bij de verstrekkers en de SVB als in het PGB2.0-systeem.

De volgende programma activiteiten vinden doorlopend plaats:

- regie voeren op een landelijke verantwoorde, gecontroleerde en succesvolle implementatie van het PGB2.0-systeem;
- coördinatie op alle externe ketenbrede communicatie en opleidingen rond de ontwikkeling van het product en de landelijke uitrol en het bevorderen van het gebruik van het digitale systeem;
- het beheren van het reeds ontwikkelde PGB2.0 systeem;
- het verder ontwikkelen en realiseren van het PGB2.0-systeem op basis van een integrated backlog.;

De scope van de interne beheersmaatregelen welke onderdeel zijn van dit rapport is beperkt tot de laatste twee activiteiten. Om het ontwikkelde PGB2.0 systeem te onderhouden en aan te kunnen blijven bieden aan de gebruikers heeft de programmaorganisatie beheer ingericht zoals toegelicht in 3.5.2.

Doorontwikkeling van het systeem vindt plaats via een roadmap, welke onderverdeeld is in vijf inhoudelijke mijlpalen A t/m E.

- Mijlpaal A: Aansluiting van alle zorgkantoren van CZ. Alle budgethouders van zorgkantoor CZ met enkel Wlz budget.
- Mijlpaal B: Aansluiting van alle zorgkantoren. Alle budgethouders met enkel Wlz budget.
- Mijlpaal C: Aansluiting 1e groep gemeenten. Budgethouders met enkel Wmo en Jw budget
- Mijlpaal D: Aansluiting 2e groep gemeenten. Budgethouders met enkel Wmo en Jw budget.
- Mijlpaal E: Aansluiting zorgverzekeraars. Budgethouders met enkel een Zvw budget én overige budgethouders met een combinatie met Zvw van gemeenten en zorgkantoren

Tijdens de controleperiode is mijlpaal A voltooid. Afronding van mijlpaal B is voorzien aan het einde van 2022. Halverwege 2022 zullen ook de eerste gemeenten aansluiten. De selectie van ontwikkelitems vanaf de integrated backlog wordt afgestemd op deze mijlpalen. De ontwikkeling wordt verder toegelicht in 3.5.3. Het al dan niet behalen van deze mijlpalen heeft géén invloed gehad op de opzet,

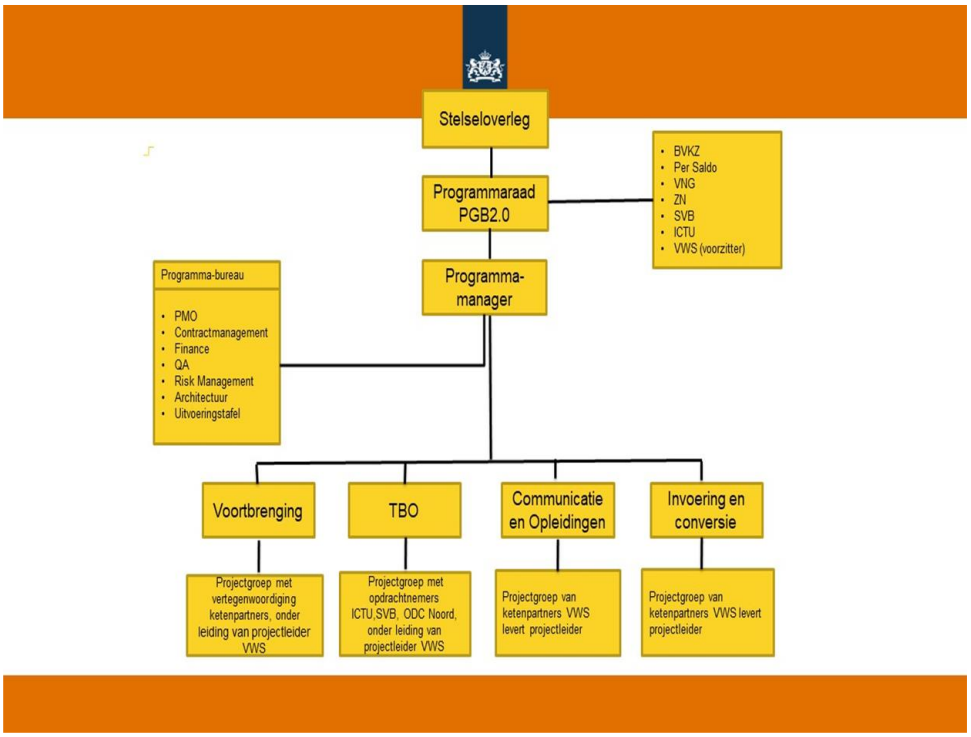
het bestaan en de werking van de interne beheersdoelstellingen en –maatregelen zoals genoemd in het Control Framework PGB2.0 v1.2.

3.3.2 Programmastructuur

Binnen het programma PGB2.0 zijn vier projecten actief. De projecten zijn:

- **Voortbrenging (Ontwikkeling);**
- **Tijdelijke Beheer en Ontwikkelorganisatie;**
- Communicatie en Opleidingen;
- Invoering en Conversie.

Zoals hiervoor genoemd vallen de dikgedrukte projecten binnen de scope van deze beschrijving. Naast bovengenoemde projecten is een programmabureau ingericht met daarin het programma- en projectmanagement, architectuur, project-control, contractmanagement en kwaliteit en risicomanagement. In dit programmabureau worden ook de ketenafspraken pgb bewaakt door op ad hoc basis samen te stellen expertgroepen. Dat laat zich vertalen in de programmastructuur, waarvan een grafische weergave is opgenomen in onderstaande figuur.



Figuur 2 Programmastructuur PGB2.0

3.3.3 Programma PGB2.0 - Primaire functies

De Programmadirecteur PGB is verantwoordelijk voor het voeren van de regie in de pgb-keten.

De Programmamanager PGB2.0 is verantwoordelijk voor het met de ketenpartners maken van de transitie van de huidige werkwijze naar de (meer gedigitaliseerde en geüniformeerde) werkwijze in PGB2.0, waaronder ontwikkeling en implementatie van het PGB2.0-systeem.
De Voortbrenging van het PGB2.0-systeem wordt door de product owners in samenwerking met de ketenpartners via de backlog gestuurd. Hieronder vallen het ontwerpen van functionaliteit en het opstellen van use cases.
Het beheer en de bouw van het PGB2.0-systeem wordt verzorgd door de Tijdelijke Beheer- en Ontwikkelorganisatie (TBO). TBO is een samenwerkingsverband van VWS, ICTU, SVB en ODC-Noord.

3.3.4 Programma PGB2.0 - Primaire rollen

In de ontwikkeling en het beheer van het PGB2.0-systeem zijn de volgende rollen te onderkennen, met de volgende plaats in de TBO-organisatie:

Rol	Uitgevoerd door	Onder aansturing van
Chief Product Owner	VWS	Programmamanager
Product Owner Zorgdomein	VWS	Programmamanager
Product Owner Financieel domein	SVB	Programmamanager
Quality Assurance officer	VWS	Programmamanager
Keten-architect	VWS	Programmamanager
Centraal Functioneel Beheer	SVB	Manager TBO
Applicatiebeheer Zorgdomein	ICTU	Manager TBO
Technisch Applicatiebeheer	SVB	Manager TBO
Housing & Hosting	ODC-N	Manager TBO
Service manager	VWS	Manager TBO
Test- & Releasemanager	VWS	Manager TBO
Security & Privacy Officer	VWS	Manager TBO

3.3.5 Verantwoordelijkheden in de keten

3.3.5.1 Control visie

PGB2.0-systeem
In de wet- en regelgeving zijn voor de uitvoering van het PGB Trekkingsrecht taken en verantwoordelijkheden belegd bij gemeenten, Wlz-uitvoerders (zorgkantoren), Zorgverzekeraars en de SVB. Het PGB2.0-systeem ondersteunt hen daarin[10]. Als ontwerpuitgangspunt geldt dat waar mogelijk wettelijke vereisten in de primaire processen toegepast worden op het moment dat er gegevens door de budgethouder, zorgverlener, verstrekker en SVB ingevoerd worden (invoercontroles). Op onderdelen kan het PGB2.0-systeem ook controles tijdens of na afloop van processen uitoefenen, bijvoorbeeld bij vereisten die zich over een langere periode uitstrekken.

TBO-diensten
De gebruikers van het PGB2.0-systeem mogen verwachten dat gegevens die zij in het PGB2.0-systeem invoeren, juist, tijdig, volledig en veilig worden vastgelegd, integer blijven, en altijd tijdig beschikbaar

[10] Ondersteuning voor zorgverzekeraars wordt op een later moment gerealiseerd

zijn voor (verdere) verwerking. De VNG, Zorgverzekeraars Nederland en de SVB hebben daartoe onder regie van VWS een Control Framework PGB2.0 opgesteld, met daarin beheersdoelstellingen, risico's en maatregelen.
Het realiseren van (geautomatiseerde) controles in het PGB2.0-systeem zoals opgenomen in het Control Framework PGB2.0 is een taak voor TBO als verantwoordelijke voor de ontwikkeling en het beheer van het PGB2.0-systeem. Het PGB2.0-systeem noch de serviceorganisatie TBO nemen echter door het uitvoeren van het beheer en de doorontwikkeling wettelijke taken en verantwoordelijkheden van gemeenten, zorgkantoren en de SVB over.

3.3.5.2 Eisen aan de gebruikersorganisaties

Binnen het PGB2.0-systeem worden persoonsgegevens verwerkt waarvoor de Gemeenten, Zorgkantoren en de SVB een wettelijke grondslag hebben in de Wmo, Jw, Wlz en/of de Zvw. VWS heeft die wettelijke grondslag niet. VWS mag daarom – kort gezegd - alleen persoonsgegevens verwerken indien en voor zover zij dat doet in opdracht van de Gemeenten, Zorgkantoren en de SVB. Deze partijen hebben daarom een verwerkersovereenkomst gesloten met VWS waarin zij afspraken hebben gemaakt over de wijze waarop VWS persoonsgegevens verwerkt binnen het PGB2.0-systeem. De Gemeenten, Zorgkantoren en de SVB hebben gezamenlijk een Onderlinge Regeling PGB Portaal gesloten waarin zij (onder meer) afspraken hebben gemaakt over de wijze waarop zij VWS aan zullen sturen.
Aan gemeenten en zorgkantoren worden voorwaarden voor aansluiting aan het PGB2.0 gesteld. Deze voorwaarden zijn vastgelegd in aansluitvoorwaarden[11] op het PGB2.0-systeem. In de voorwaarden worden de volgende aspecten genoemd:

- Definities
- Het toepassingsbereik van het aansluiten
- Beveiliging
- Inhoud
- Wet- en regelgeving
- Beschikbaarheid
- Financiering
- Intellectueel eigendom
- Wijzigingen in het PGB2.0-systeem
- Wijzigingen in de aansluitvoorwaarden
- Aansprakelijkheid
- Inwerkingtreding, duur en beëindiging overeenkomst
- Toepasselijk recht en bevoegde rechter

Budgethouders, zorgverleners, gemeenten, zorgkantoren en de SVB zijn zelf verantwoordelijk voor de kwaliteit van door hen ingevoerde gegevens. Het zorgdomein bevat diverse invoercontroles om bij te dragen aan een correcte invoer. Het functioneren van invoercontroles valt binnen de scope van de Vermelding van VWS in sectie I, voor zover benoemd in de beheersmaatregelen in bijlage 1. Het vaststellen van de inhoudelijke juistheid van de ingevoerde gegevens valt buiten de scope van deze beschrijving.

[11] 20190430 Aansluitvoorwaarden PGB Portaal 2.0 Def

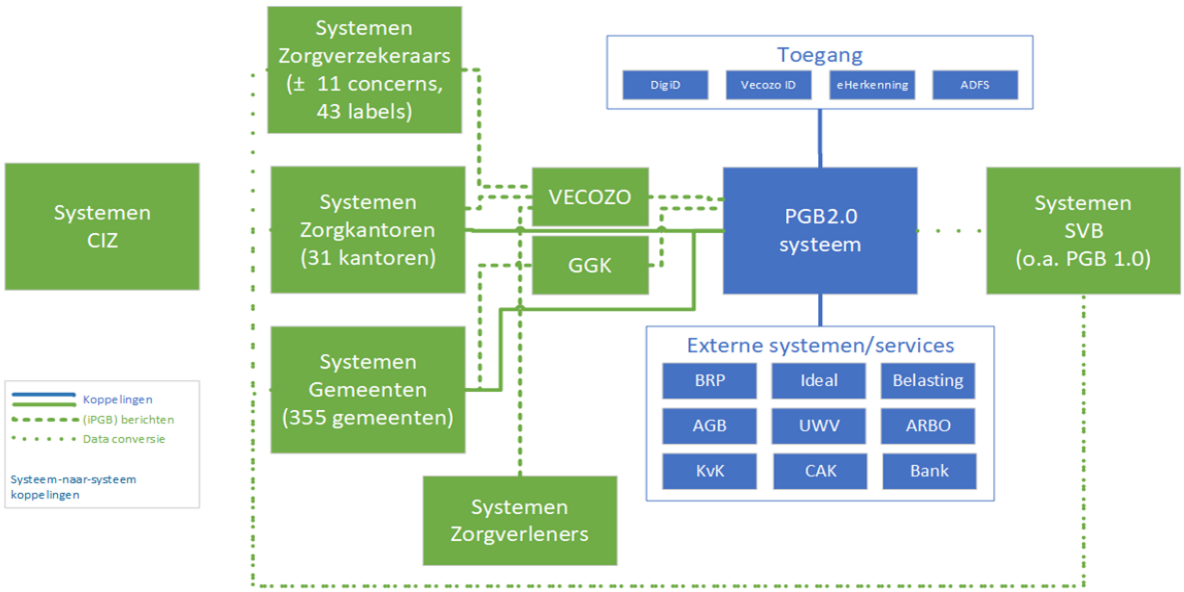
3.3.5.3 Verantwoordelijkheden bij de gebruikersorganisaties

De ketenpartijen zijn ieder voor zich verantwoordelijk voor het borgen van de rechtmatigheid in de PGB-keten, met dien verstande dat die verantwoordelijkheid zich alleen uitstrekt over de wettelijke taken die aan de ketenpartij toebedeeld zijn.
In het ontwikkelproces (in de keten wordt dit het 'voortbrengingsproces' genoemd) betekent dit dat de verantwoordelijkheid voor het specificeren van beheersmaatregelen in de vorm van geautomatiseerde controles en het toezien op de juiste werking volgt uit de taken zoals genoemd in de wet- en regelgeving. Daarbij is het niet per definitie zo dat de beheersmaatregelen (controles) in het Z-domein de verantwoordelijkheid zijn van de verstrekkers, en de beheersmaatregelen in het F-domein de verantwoordelijkheid van de SVB. Om een voorbeeld te noemen: de wet- en regelgeving geeft gedetailleerd aan dat de SVB pas mag betalen als een declaratie een aantal verplichte gegevens bevat. De SVB is derhalve formeel verantwoordelijk voor de declaratiecontroles in het Z-domein, en zal moeten toezien op het juist functioneren van de controles en zich daarover verantwoorden.

3.4 Zorgdomein PGB2.0 systeem

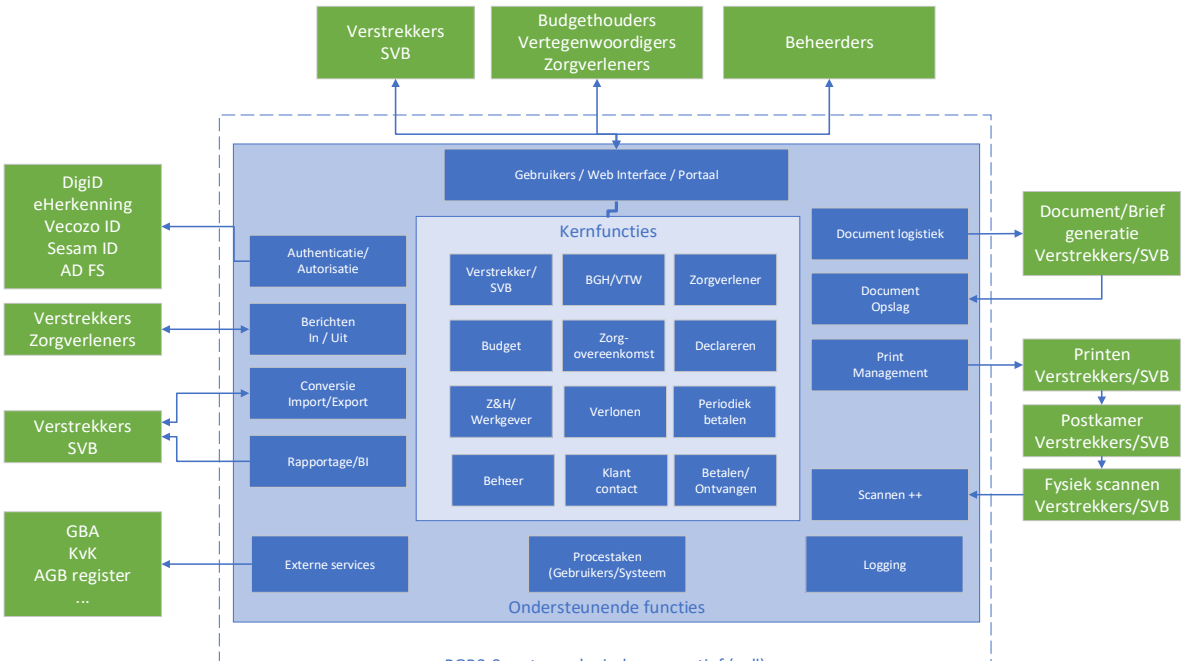
In opdracht van stelselverantwoordelijke Ministerie van VWS wordt door de Tijdelijke Beheer- en Ontwikkelorganisatie (TBO) het PGB2.0-systeem ontwikkeld en geïmplementeerd. Doel van het PGB2.0-systeem is om verbetering aan te brengen in de administratieve ondersteuning van budgethouders, hun zorgverleners, de verstrekkers, en de SVB bij het beheren en besteden van toegekende budgetten in het kader van persoonsgebonden budgetten.

Het PGB2.0-systeem bevat diverse functies en is gekoppeld aan externe systemen. Onderstaande figuur geeft een globaal overzicht van het PGB2.0-systeem en haar omgeving.



Figuur 3 Het PGB2.0-systeem en haar omgeving

Onderstaand figuur geeft een overzicht van de functies in het PGB2.0-systeem.



Figuur 4 Functies van het PGB2.0-systeem

Het PGB2.0-systeem bestaat uit een Zorgdomein en een Financieel domein. Onder het Zorgdomein wordt de algehele functionaliteit voor de (eind)gebruikers verstaan.

Het Zorgdomein bevat functionaliteit voor:

- de budgethouders ter ondersteuning van hun regierol; zij kunnen zorgovereenkomsten opstellen (samen met zorgverleners), declaraties indienen en vrijwillige stortingen doen alsmede overzicht houden op hun gehele PGB;
- de zorgverleners om (samen met budgethouders) zorgovereenkomsten op te kunnen stellen en te kunnen wijzigen, en te factureren aan budgethouders;
- de verstrekkers (gemeenten en zorgkantoren) om zorgovereenkomsten te controleren en goed- of af te keuren, betalingen in te zien en budgetberichten (Toekenningsberichten) aan te kunnen leveren aan het Zorgdomein. Daarnaast kunnen de verstrekkers de informatie uit het Zorgdomein gebruiken voor hun informatievoorziening naar de budgethouders;
- de uitvoerder (SVB) om in staat te zijn via het Zorgdomein de papierenstroom van de budgethouders, zorgverleners en verstrekkers te verwerken. De uitvoerder gebruikt de informatie van het Zorgdomein ook voor de dienst- en informatievoorziening naar de budgethouders en zorgverleners. Op basis van gegevens uit het Zorgdomein verzorgt de SVB betalingen en levert diensten ter ondersteuning van de budgethouders m.b.t. hun werkgeverstaken.

Het Financieel Domein bevat functionaliteit voor:

- het verwerken en betaalbaar stellen van betaalopdrachten uit het zorgdomein;
- het berekenen van werkgeverslasten in situaties waar sprake is van arbeidsverhoudingen;
- het ondersteunen van budgethouders in hun werkgeverstaken (bijv. salarisadministratie en afdrachten werkgeverslasten, berekening ziektegelden).

De vermelding van VWS in sectie I en het assurance rapport in sectie II beperkt zich tot het Zorgdomein van PGB2.0.

Het Ministerie van VWS stuurt het beheer en de ontwikkeling van het PGB2.0-systeem aan via het Programma PGB2.0. Het Programma PGB2.0 is verantwoordelijk voor de ontwikkeling van een PGB2.0-systeem wat aansluit bij de behoeften en (wettelijke) eisen van budgethouders, zorgverleners, gemeenten, zorgkantoren en de SVB. De Product Owners van het Zorgdomein en Financieel domein en de Chief Product Owner voeren in opdracht van VWS hiertoe op gestructureerde wijze overleg met deze partijen, alsmede de ontwikkelpartij ICTU.

TBO is in opdracht van de Programmamanager PGB2.0 verantwoordelijk voor het beheer van de automatiseringsomgevingen waarin de applicaties en systeemservices van het PGB2.0-systeem draaien. De ontwikkeling voor het Zorgdomein is belegd bij ICTU, en voor het Financieel domein bij de SVB. Ictu ontwikkelt het Zorgdomein als maatwerkapplicatie in haar Azure Devops omgeving in de programmeertaal C+. Het F-domein bestaat uit standaard toepassingen van Oracle.
Het technisch applicatiebeheer is voor het Zorgdomein belegd bij VWS en voor het Financieel domein bij de SVB. Het centraal functioneel beheer voor beide domeinen is belegd bij de SVB.

VWS heeft de rekencentradiensten van de automatiseringsomgeving voor het Zorgdomein ondergebracht bij Overheidsdatacenter Noord (ODC-Noord) (voor het Financieel domein zijn deze diensten door de SVB ondergebracht bij Atos). ODC-Noord faciliteert de fysieke ruimte en diensten als noodstroom, klimaatbeheersing van de ruimte, een blusinstallatie en de fysieke bewaking van de servers en het fysieke toegangsbeheer, en redundante verbindingen naar de gebruikers en

beheerders. Ook host ODC-Noord servers en levert het enkele beheerapplicaties zoals Topdesk, Jira en Confluence. De van ODC-Noord afgenomen diensten worden beschreven in het Beheerskader in H3.5. Voor zover relevant voor de beheersdoelstellingen beoordeelt TBO de interne beheersdoelstellingen en -maatregelen van ODC-Noord middels leveranciersmanagement (serviceniveau overeenkomst en serviceniveau rapportages. Tevens vindt wekelijks operationeel overleg plaats tussen TBO en ODC-Noord.Ten aanzien van de rekencentrumdiensten geeft ODC-Noord periodiek een In Control Verklaring af aan VWS, deze wordt beoordeeld door de Servicemanager PGB2.0 en Security Officer PGB2.0.

3.5 Beheerskader van het Programma PGB2.0

3.5.1 Control Framework PGB2.0

Onder regie van VWS is samen met de VNG, Zorgverzekeraars Nederland en de SVB een Control Framework PGB2.0 vastgesteld. In het Control Framework PGB2.0 v1.2 van 22-02-2021 zijn de beheersdoelstellingen, geïdentificeerde risico's en beheersmaatregelen uitgewerkt voor het Zorgdomein (bijlage 3 bij het Control Framework) respectievelijk het Financieel domein (bijlage 4 bij het Control Framework).

In Bijlage 1 van dit rapport worden de beheersdoelstellingen en -maatregelen voor het zorgdomein in detail toegelicht. De application controls en de general IT controls in bijlage 3 van het Control Framework vormen de beheersmaatregelen die in dit rapport getoetst worden.

Het Control Framework PGB2.0 wordt minimaal jaarlijks met de ketenpartners en NBA geëvalueerd onder coördinatie van de Quality/Compliance officer. Daarnaast organiseert de Quality/Compliance officer regelmatig informatiebijeenkomsten met bovengenoemde partijen om vraagstukken m.b.t. rechtmatigheid te bespreken. Waar nodig stelt de Quality/Compliance officer notities op voor de Programmaraad PGB2.0. In het Control Framework is opgenomen dat de daarin opgenomen beheersmaatregelen jaarlijks extern getoetst worden middels een ISAE3402-2 traject.

3.5.2 Tijdelijke Beheer en Ontwikkel Organisatie (TBO)

De Tijdelijke Beheer en Ontwikkel Organisatie (TBO) is ingericht door VWS om het PGB2.0 systeem te doorontwikkelen, implementeren en beheren. De TBO is een samenwerkingsverband tussen VWS als opdrachtgever en haar partners als opdrachtnemer: SVB (in haar rol van ICT-dienstverlener), ICTU en ODC-Noord.

Binnen TBO zijn de volgende management- en coördinatierollen belegd:

- Projectleider TBO, deze is verantwoordelijk voor de aansturing van onderstaande rollen.
- Servicemanager, is verantwoordelijk voor leveranciersmanagement en de serviceafspraken met de SVB, ZN en VNG.

- Release-, test- en changemanager, verantwoordelijk voor het plannen, laten testen en gecontroleerd vrijgeven van releases welke opgeleverd worden door Ictu.
- Aansluitcoördinator (2x), verantwoordelijk voor de afstemming met nieuwe toetreders tot PGB2.0.
- Information Security Officer, verantwoordelijk voor implementatie van informatiebeveiliging. Jaarlijks stelt de ISO een In Control Verklaring op de BIO op aan VWS, en begeleid hij samen met de Quality/Compliance Officer het jaarlijkse Digid assessment en externe audits op de BIO en NEN7510.
- Infra architect, verantwoordelijk voor ontwerp man de infrastructuur.
- Quality/compliance officer, verantwoordelijk voor implementatie van maatregelen m.b.t. kwaliteit en conformiteit met o.a. het Control Framework.
- Teamleider Applicatiebeheer; leidt het team van applicatiebeheerders bij Ictu.
- Teamleider Centraal Functioneel Applicatiebeheer, leidt de centrale functionele beheerders
- Service/TAB coordinator; stuurt het team Technisch Applicatiebeheerders aan en is verantwoordelijk voor operationele processen zoals incidentmanagement.

Bij bovenstaande opsomming wordt het volgende opgemerkt:

- De aansluitcoördinatie valt buiten de scope van deze beschrijving en het onderzoek
- De productowner Zorgdomein en Chief Product Owner vallen rechtstreeks onder VWS. Zij zijn verantwoordelijk voor de Integrated backlog, en in overleg met Ictu en de SVB, ZN en VNG prioriteren van backlogitems in de ontwikkeling.

De ontwikkeling van het Zorgdomein van PGB2.0 is belegd bij Ictu. Inhoudelijk wordt de ontwikkeling gestuurd door de productowners. Operationeel wordt de ontwikkeling en het applicatiebeheer bij Ictu aangestuurd door de Projectleider TBO.

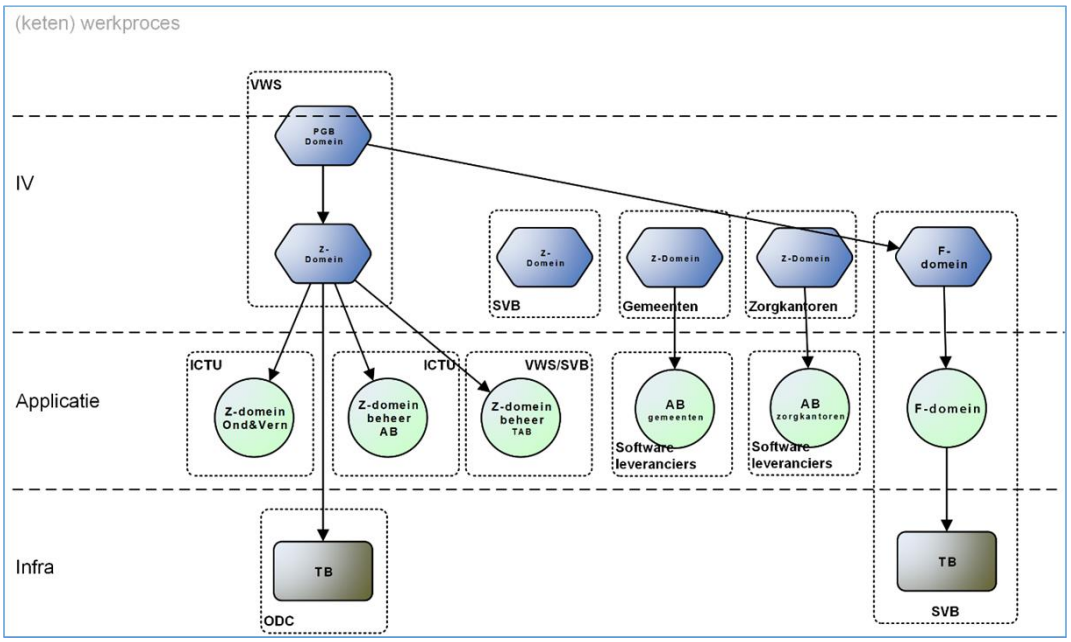
Voor de uitvoering wordt binnen TBO gebruik gemaakt van best practice procesmodellen voor de bovenstaande beheerdomeinen. Dit zijn achtereenvolgens BiSL, ASL en ITIL.

TBO levert de volgende beheerdiensten op het Zorgdomein (scope van de vermelding van VWS in sectie 1) als het Financieel domein (buiten de scope van de vermelding van VWS in sectie I).

Dienst	**Uitvoerende partij Z-domein**	**Uitvoerende partij F-domein**
Centraal Functioneel beheer	SVB	SVB
Ontwikkeling	ICTU	SVB
Applicatie Beheer	ICTU	SVB
Technisch Applicatie beheer	SVB	SVB
Carve-out:		
Technisch beheer	ODC-Noord	SVB
Infrastructuur services (IaaS)	ODC-Noord	
Continuïteit package (VMaaS)	ODC-Noord	
Server OS (PaaS)	ODC-Noord	
PaaS rollen (PaaS)	ODC-Noord	
Basisvoorzieningen infra (Maatwerk)	ODC-Noord	

Software Services (SaaS) Backup as a service (BaaS)	ODC-Noord

Onderstaande figuur licht bovenstaande opsomming toe. NB. in deze figuur ontbreekt ‘Centraal Functioneel beheer’.



Figuur 5 Beheerdomeinen PGB2.0

Ten behoeve van deze beheerdiensten worden de volgende beheerprocessen uitgevoerd door TBO:

- Wijzigingenbeheer. De release-, test- en changemanager plant in afstemming met Ictu en de product owner de backlogitems in in sprints, die per twee à drie stuks een release vormen. De releases worden op basis van vooraf gezamenlijk overeengekomen normen vrijgegeven door Ictu, waarna de releasemanager de intake-, regressie- en acceptatietesten coördineert en de Go-Nogo besluitvorming faciliteert. Meer standaard wijzigingen worden door functioneel beheerders van verstrekkers en SVB en in voorkomend geval beheerders binnen TBO ingediend bij Centraal Functioneel Beheer en vastgelegd in TOPdesk. Voor veel voorkomende wijzigingen zijn sjablonen voor de registratie en afhandeling opgesteld. Niet-standaard wijzigingen van substantiële omvang worden geagendeerd in de Change Advisory Board. De servicecoördinator rapporteert wekelijks over o.a. wijzigingen, en de Programmaraad PGB2.0 ontvangt maandelijkse voortgangsrapportages. Beide rapportages worden ook toegezonden aan de Quality/Compliance officer.
- Wachtwoordbeheer (beperkt tot medewerkers werkzaam in bovengenoemde diensten, de authenticatie van budgethouders en zorgverleners wordt buiten PGB2.0 geregeld)). De basis voor het wachtwoordmanagement wordt gevormd door de Active Directory van Microsoft v.w.b. de virtuele servers welke afgenomen worden van ODC-Noord. Wachtwoorden voor randcomponenten en tooling worden vastgelegd in Keepass. Wachtwoorden worden nimmer in plaintext vastgelegd in instructies e.d.

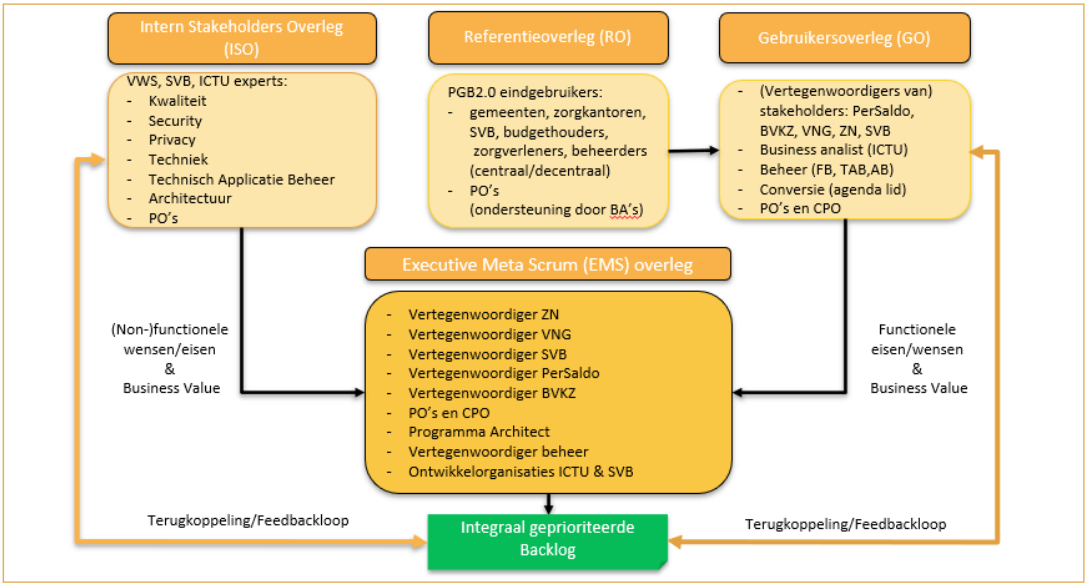
- Gebruikersbeheer (idem). De teamleiders beoordelen accountaanvragen voor nieuwe teamleden AB, cFAB en TAB. Een bijzondere categorie wordt gevormd door de zogenaamde RDS accounts: accounts voor medewerkers van SVB en verstrekkers t.b.v. toegang tot de scan- en printfaciliteiten in PGB2.0. In Q4-2021 is het periodiek controleren van gebruikersaccounts verbeterd.
- Beveiliging van componenten (binnen de gebruikersomgeving PGB bij ODC-Noord). De Information Security Offcier spreekt op regelmatige basis met ontwikkelaars van Ictu (security gerelateerde backlogitems) en Technisch Applicatie Beheerders. De Information Securiy Officer rapporteert maandelijks over risico's, incidenten en maatregelen m.b.t. informatiebeveiliging, alsmede over privacy gerelateerde zaken. De Quality/Compliance officer ontvangt deze rapporten en is aanwezig bij de maandelijkse bespreking met de functionarissen genoemd aan de start van deze paragraaf.
- Backup & Recovery (op de onderdelen binnen de gebruikersomgeving PGB bij ODC-Noord). Tijdens de controleperiode is de Backup as a service dienst van ODC-Noord aangekocht en verder ingericht, optimalisatie is nog steeds gaande. Het afgeven van backup- en restore opdrachten geschiedt door de teamleider TAB en wordt vastgelegd in TOPdesk. Ten behoeve van (proef)conversies worden regelmatig restores uitgevoerd in niet-productie omgevingen ('verse data').
- Koppelvlakken beheer (de vermelding van VWS in sectie 1 beperkt zich tot het koppelvlak tussen het Zorgdomein en Financieel Domein). De werking van de koppelvlakken vindt grotendeels automatisch plaats middels proceszekeringen, die 'klappen' zodra er iets mis is met het koppelvlak. De SVB heeft aan haar zijde een 'NOK' controle ingericht. De SVB voert maandelijks aansluitcontroles uit en escaleert waar nodig naar de Quality/Compliance officer van TBO (in de controleperiode is daar geen aanleiding toe geweest).
- Incident & Problemmanagement. Wekelijks rapporteert de servicecoördinator over incidenten en problemen en de gestelde beheersdoelen. De Quality/Compliance officer ontvangt deze rapporten.
- Servicemanagament. Wekelijks bespreken de Projectleider TAB, Servicemanager, Servicecoördinator/TAB Teamleider en de Change/Test/Releasemanager onderwerpen en issues m.b.t. de dienstverlening. Met de 'leveranciers' ICT, SVB en ODC-Noord voort de Projectleider TBO regelmatig 'dienstenoverleg'.

Wekelijks vindt er 'Beheer Backlog Refinement' overleg plaats waarin beheerszaken uit bovenstaande processen besproken worden met teamleiders cFAB, AB, TAB en de servicecoördinator.
Met ODC-Noord vindt wekelijks operationeel overleg plaats door de Service coördinator, Infra architect, Teamleider TAB over de diensten van ODC-Noord en de daarin uitgevoerde processen (patchmanagement, incident- & problemafhandeling, wijzigingsbeheer vanuit ODC-N, etc).
Tijdens de controleperiode zijn de Information Security Officer en de Teamleider TAB wekelijks gaan overleggen over security aangelegenheden.

3.5.3 Voortbrengingsproces (ontwikkeling)

Het PGB2.0-systeem wordt als een webapplicatie aangeboden aan budgethouders, zorgverleners, gemeenten, zorgkantoren en de SVB, waarbij de drie laatstgenoemde partijen zorgdragen voor aansluiting aan hun backoffice systemen ten behoeve van lokale functies zoals het inscannen en printen van documenten.

Basis voor de ontwikkeling is de Integrated backlog, welke volgens onderstaand proces tot stand komt.



Figuur 6 Voortbrengingsgproces PGB2.0

In het Voortbrengingsproces ontwikkelen ontwikkelteams met behulp van de Agile ontwikkelmethodiek in sprints nieuwe en gewijzigde functionaliteit in het PGB2.0-systeem. De PO Zorgdomein bepaalt in afstemming met het Gebruikersoverleg en ICTU, mede op basis van de roadmap, de vulling van de ontwikkelsprints. Per 2 á 3 ontwikkelsprints wordt de ontwikkelde functionaliteit door Ictu gebundeld in een release, getest, en overgedragen aan de releasemanager van TBO. Deze overdracht vindt niet eerder plaats dan dat Ictu en de PO gezamenlijk een positief vrijgaveadvies hebben afgegeven. Ten behoeve van dit vrijgaveadvies worden er een aantal controles uitgevoerd om de inhoud van de release versus de overeengekomen backlog-items te verifiëren, de impact op de performance te kunnen duiden, en de kwaliteit van de software te bepalen.

De Software Improvement Group meet in opdracht van Ictu periodiek de softwarekwaliteit van het Zorgdomein volgens haar Sigrid methode. Gemiddeld maandelijks vindt er overleg over codekwaliteit plaats en worden er expliciete ontwikkelitems benoemd en besproken om de codekwaliteit te verbeteren,

De afspraken tussen VWS en ICTU over de kwaliteit van ontwikkeling en applicatiebeheer van het zorgdomein zijn vastgelegd in een Service Level Agreement v1.1.
De metrieken zijn te vertalen naar de softwarekwaliteitsaspecten conform de ISO-25010 norm.

3.5.4 Inzet methodes voor kwaliteitsverbetering dienstverlening

De functionaliteit in het PGB2.0-systeem wordt ontwikkeld via de AGILE methodiek.
Beheerprocessen worden zo veel mogelijk ingericht op basis van ITIL, ASL en BiSL zodat gebruik wordt gemaakt van best practices beheerprocessen.
De medewerkers binnen TBO maken gebruik van de tools Confluence, Samenwerkruimtes, Topdesk en Jira.
Quality Assurance PGB2.0 is vanaf medio 2020 integraal opgezet vanuit het Programmabureau.

3.5.5 Monitoren, bewaken en controle van diensten

De manager TBO voert regelmatig Dienstenoverleg en TBO Exploitatieoverleg waarin de lopende zaken en processen besproken worden.
Iedere projectmanager rapporteert aan de programmamanager wat de stand van zaken is ten aanzien van alle aspecten zoals beschreven in het projectplan, wat de voortgang is t.o.v. de mijlpalen, welke belangrijke issues er spelen, welke risico's zich voordoen, welke activiteiten zijn uitgevoerd en welke worden uitgevoerd in de komende maand. De bundeling van deze statusupdates vormt het complete beeld over de voortgang van het programma. De Programmaraad PGB2.0 ontvangt maandelijks een exploitatierapportage van TBO, en voor elk overleg van de programmaraad een voortgangsrapportage op programmaniveau.
De Information Security Officer produceert maandelijks een Informatiebeveiligingsrapportage, en verder wordt er wekelijks gerapporteerd over incident- en problemmanagement.

Sectie IV, Toetsresultaten assurance-rapport NOREA ISAE 3402 type 2

Sectie IV, Toetsresultaten assurance-rapport NOREA ISAE 3402 type 2, PGB2.0

In deze sectie zijn de uitgevoerde auditwerkzaamheden en de bevindingen opgenomen. Voor de application controls is een andere controlebenadering gehanteerd dan voor de general IT-controls, zoals in hoofdstuk Application Controls in deze sectie te lezen is. De uitwerking van de application controls is vanwege het steunen op een test-of-one en het wijzigingsbeheer niet per application- of IT- dependent control vastgelegd, maar alleen over het geheel wordt een conclusie getrokken. Hierop uitgezonderd zijn de twee application controls die in het type I onderzoek naar opzet en bestaan per 1 juni 2020 als niet effectief waren bevonden en waar derhalve geen toereikend test-of-one resultaat beschikbaar voor was.

Voor de general IT-controls zijn de uitvoerde werkzaamheden en norm per beheersmaatregel beschreven.

4.1. Application- en IT dependent controls

Van de 54 te toetsen application controls en 4 IT-dependent controls (zie onderstaande opsomming) is de werking vastgesteld aan de hand van een aantal uitgangspunten en waarnemingen:

- De afwikkeling van de bevindingen rondom de application controls (W1-M8 t/m W1-M11, D3-M5, D3-M11, B3-M1 en B3-M2) van het ISAE 3402 type 1 per 1 juni 2020 is nagegaan. Voorafgaand aan de opdracht zijn application controls W1-M8 t/m W1-M11, D3-M5 en B3-M1 voor dit type 2 onderzoek komen te vervallen. Van de overige twee te toetsten application controls is vastgesteld dat:
    - D3-M11 betreffende een geautomatiseerde controle waarin declaraties voor bijkomende kosten middels een werktaak voorgelegd worden aan de verstrekker ontbreekt in het systeem.
    - niet inzichtelijk is gemaakt dat, met betrekking tot verwerken van de betaalstatus (B3-M2), retourinformatie over door het financieel domein verwerkte betaalopdrachten juist en volledig wordt verwerkt door het zorgdomein.
- Na het nagaan van de afwikkeling van bovengenoemde bevindingen uit het type 1 onderzoek over 2020, kon voor de overige application controls volstaan worden met test-of-one. Daarbij is gesteund op de uitkomsten van het assurance type 1 onderzoek naar opzet en bestaan op 1 juni 2020. De opzet en bestaan waren immers in dat onderzoek al vastgesteld. Als voorwaarde voor de test-of- one geldt dat:
- Verder gesteund kon worden op de goede werking van het wijzigingsbeheer én aantoonbaar is gemaakt dat zich geen wijzigingen in de application controls hebben voorgedaan in de verslagperiode. Beide zijn in dit type 2 assurance onderzoek vastgesteld.

De werking van de resterende 46 application controls en 4 IT-dependent controls is aan de hand van de volgende controle activiteiten vastgesteld.

- Een walktrough bijwonen door een voor de productie omgeving representatieve testomgeving om een beeld te krijgen van de werking van de application controls.
- Laten aantonen dat het via alternatieve routes niet mogelijk is om de application controls te omzeilen. Daarbij is gekeken naar het conversietraject en mogelijkheden om rechtstreeks te muteren op de database.
- Nagaan uitkomsten van toetsing van wijzigingenbeheer en incidentbeheer en het aanvullend uitvoeren van deelwaarnemingen om vast te stellen dat er gedurende de verslagperiode geen wijzigingen in de application controls zijn aangebracht.
- Een demonstratie van de mergefunctionaliteit, die een extra waarborg biedt ter voorkoming van het onbedoeld en onopgemerkt aanpassen van de code. Aangezien application controls hard gecodeerd zijn, biedt deze waarborg voldoende zekerheid.

Conclusie application- en IT-dependent controls

Met uitzondering van application controls D3-M11 en B3-M2 zijn de effectieve opzet, bestaan en werking van onderstaande application controls en IT-dependent controls van het control framework v1.2 in de verslagperiode vastgesteld.

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
T1-M1 Application control	*invoer* Het systeem accepteert en verwerkt alleen TKB berichten die voldoen aan de specificaties van de berichtenstandaard iPGB (voldoen aan een berichtenstandaard impliceert dat het bericht en de inhoud voldoet aan berichtdefinities, voorgeschreven codelijsten en business rules (invulinstructies).	AB-Z	Op het moment dat de TKB aangeboden wordt (realtime)
T1-M2 Application control	retourbericht Het PGB 2.0 systeem genereert voor elke ontvangen TKB (of die nu verwerkt kan worden of niet) een retourbericht aan de verstrekker met het verwerkingsresultaat.	AB-Z	Op het moment dat de TKB aangeboden wordt (realtime)
T1-M4lication control	*invoer* Het BSN uit een ontvangen TKB wordt uitgevraagd in de BRP. Het BSN moet voorkomen in de BRP, als dat het geval is wordt de informatie uit de TKB gekoppeld aan de BSN zoals opgegeven in het TKB (tevens worden verdere personalia uit het BRP overgenomen). Als het BSN niet voorkomt in het BRP wordt de TKB afgewezen.	AB-Z	Op het moment dat de TKB aangeboden wordt (realtime)
P1-M1 Application control	*autorisaties* Er zijn specifieke autorisatieprofielen voor verstrekkers, budgethouders en de SVB - Enkel de budgethouder en (eventuele) vertegenwoordiger zoals opgenomen in het TKB zijn door middel van DigiD geautoriseerd de profielgegevens in te vullen of te wijzigen - SVB kan de profielgegevens wijzigen die de budgethouder/vertegenwoordiger ook zelf zou kunnen wijzigen in het profiel. Hieronder vallen Telefoonnummer, Emailadres,	AB-Z	

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
	Bankrekeningnummer (IBAN) en Tenaamstelling IBAN. Wijzigingen kunnen alleen doorgevoerd worden via een werktaak "wijzig profielgegevens" - De verstrekker heeft dezelfde mogelijkheden als de SVB, maar alleen voor Budgethouders die een actieve TKB bij die verstrekker (cq consessiehouder) hebben.		
P1-M2 Application control	*invoer* De schermen in PGB 2.0 t.b.v. het vastleggen van profielgegevens bevatten verplichte velden opdat alle benodigde gegevens vastgelegd worden. Als er velden niet ingevuld worden, kan het profiel van de budgethouder (of de wijzigingen daarin) niet opgeslagen worden. Het betreft de volgende gegevens: Correspondentievoorkeur, Telefoonnummer 1, Emailadres & Emailadresbevesttiging (indien er correspondentievoorkeur per email wordt aangegeven), Postadres ((indien er correspondentievoorkeur per post wordt aangegeven)	AB-Z	
P2-M1 Application control	*autorisaties* Er zijn specifieke autorisatieprofielen voor verstrekkers, zorgverleners, en de SVB - De zorgverlener kan zijn eigen profielgegevens invullen of wijzigen - De SVB en Verstrekkers kunnen profielgegevens van de zorgverlener wijzigen wanneer er een werktaak "wijzig profielgegevens" bestaat. - Verstrekkers kunnen de profielgegevens van zorgverleners wijzigen wanneer daar een werktaak voor is, en deze gegevens niet uit het AGB-register komen.	AB-Z	
P2-M2 Application control	*invoer* Op BSN's van zorgverleners die door de budgethouder worden ingevoerd, wordt de 11-proef uitgevoerd; Op AGB codes die ingevoerd worden, wordt een controle op geldigheid van de AGB code uitgevoerd.	AB-Z	Op het moment dat een budgethouder de zorgverlenergegevens invoert in PGB 2.0, danwel het moment dat de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet. Op het moment dat de profielgegevens van de zorgverlener bijgewerkt worden.

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
P2-M3 Application control	*invoer* De schermen in PGB 2.0 t.b.v. het vastleggen van profielgegevens bevatten verplichte velden opdat alle benodigde gegevens vastgelegd worden. Als er velden niet ingevuld worden, kan het profiel van de zorgverlener (of de wijzigingen daarin) niet opgeslagen worden. Voor een Zorgverlener NP zijn dit: BSN of KvK, Voorletters, Naam, Geboortedatum, Geslacht, Emailadres & Emailadresbevesttiging (indien er correspondentievoorkeur per email wordt aangegeven), Postadres ((indien er correspondentievoorkeur per post wordt aangegeven), IBAN, Tenaamstelling IBAN, Land, Correspondentievoorkeur Voor een Zorgverlenersorganisatie zijn dit: Email adres, bevestig Email adres, IBAN, tenaamstelling IBAN	AB-Z	Bij het vastleggen van profielgegevens
Z1-M2 Application control	*proces functionaliteit* Het Z-domein genereert voor alle zorgovereenkomsten waar salarisadministratie gevoerd moet worden (AO en OVO 4dgn of meer, of opting-in), automatisch een bericht naar het F-Domein.	AB-Z	
Z2-M5 Application control	*invoer* Zorgovereenkomsten moeten opgesteld worden volgens modelovereenkomsten. In de digitale stroom betekent dit dat het PGB 2.0 systeem middels de invoerschermen alle noodzakelijke gegevens zoals gespecificeerd in de modelovereenkomsten uitvraagt. Als niet alle gegevens ingevuld worden kan de zorgovereenkomst niet volledig vastgelegd worden.	AB-Z	Op het moment dat de BH een ZOK opstelt in PGB 2.0, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.
Z2-M6 Application control	*proces functionaliteit* De zorgverlener geeft digitaal akkoord op de ingevoerde ZOK. Dit akkoord is herleidbaar naar de zorgverlener of instelling middels Digid, eHerkenning of de AGB code van de zorgverlener (afhankelijk van type zorgverlener).	AB-Z	Op het moment dat de zorgverlener de door hem/haar ingevoerde ZOK akkoord verklaart.

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
Z2-M7 Application control	*autorisaties* De budgethouder geeft digitaal akkoord op de ingevoerde ZOK. Als de budgethouder een wettelijk vertegenwoordiger heeft, is deze handeling voorbehouden aan de wettelijk vertegenwoordiger. Dit akkoord is herleidbaar naar de budgethouder (of diens vertegenwoordiger) omdat deze middels Digid (een niet-natuurlijke vertegenwoordiger: eHerkenning) is aangemeld aan het systeem.	AB-Z	Op het moment dat de budgethouder de door hem/haar ingevoerde ZOK akkoord verklaart.
Z2-M9 Application control	*invoer* Bij een zorgovereenkomst waarop salarisadministratie door de SVB van toepassing is, dwingt het systeem af een id-document te uploaden.	AB-Z	Op het moment dat de BH een ZOK opstelt in PGB 2.0, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.
Z2-M11 Application control	*invoer* In geval er sprake is van een ZOK arbeidsovereenkomst met minimaal 4 dagen per week werk (=bruto/netto AO) dan moet de budgethouder via het systeem een machtiging aanvinken aan de SVB voor het voeren van de salarisdadministratie en het afdragen van werkgeverslasten aan de BD.	AB-Z	Op het moment dat de Budgethouder de ZOK in het systeem akkoord verklaart, dan wel op het moment dat de Budgethouder een papieren ZOK naar de SVB (WMO/JW) of het zorgkantoor (Wlz) stuurt.
Z2-M13 Application control	*invoer* Bij Wlz: in het arbeidspatroon in de zorgovereenkomst kan er, wanneer er sprake is van maandloon, en de arbeidstijdenwet niet van toepassing is*, niet meer dan 40 uur per week vastgelegd worden (* ZOK met familielid of partner en OVO). Deze regel geldt voor zorgverleners en is daarom niet van toepassing op zorginstellingen.	Zorgkantoor	Op het moment dat het zorgkantoor de zorgovereenkomst in het systeem beoordeelt.
Z2-M16 IT dependent control	*proces functionaliteit* Het systeem geeft een signalering af indien er een mutatie plaats vindt op de zorgovereenkomst. Op basis van dit signaal vindt een inhoudelijke beoordeling (uitgezonderd automatische verlengingen van zorgovereenkomsten die binnen de restricties van de TKB blijven vallen) plaats door de SVB of verstrekker. SVB en/of de verstrekker leggen de inhoudelijke beoordeling van een zorgovereenkomst expliciet in het	SVB Gemeente Zorgkantoor	Op het moment dat er een mutatie wordt doorgevoerd op de zorgovereenkomst

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
	systeem vast, en de budgethouder en zorgverlener worden over deze beoordeling automatisch geïnformeerd.		
Z3-M1 Application control	*invoer* Het systeem beperkt de mogelijke ingangsdatum van een ZOK tot datums die op of na de ingangsdatum van de eerst beschikbare TKB in het systeem liggen.	AB-Z	Op het moment dat de Budgethouder de ZOK in het systeem opstelt, dan wel op het moment dat de Budgethouder een papieren ZOK naar de SVB (WMO/JW) of het zorgkantoor (Wlz) stuurt.
Z3-M3 Application control	*proces functionaliteit* De aangeduide wet (Wlz, Wmo, Zvw, Jw) in de zorgovereenkomst wordt elektronisch overgenomen uit de in het toekenningbericht vermelde wet.	AB-Z	Op het moment dat de BH een ZOK opstelt in PGB 2.0, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.
Z4-M1 Application control	*invoer* Het systeem bewaakt consistentie in vast te leggen gegevens per type zorgovereenkomst: *- bij een onregelmatig aantal uren kan geen vaste maandelijkse betaling vastgelegd worden*	AB-Z	Op het moment dat de ZOK in het systeem door de BH opgesteld wordt, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.
Z4-M2 Application control	*invoer* Het systeem bewaakt consistentie in vast te leggen gegevens per type arbeidspatroon in de zorgovereenkomst : *- bij een vaste maandelijkse betaling moet een weekrooster (bij ZOK AO) of aantal uren per week/maand (ZOK OVO) ingevuld worden*	AB-Z	Op het moment dat de ZOK in het systeem door de BH opgesteld wordt, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
Z4-M3 Application control	*invoer* Het systeem bewaakt consistentie in vast te leggen gegevens per type arbeidspatroon in de zorgovereenkomst *- als onregelmatige uren zijn gespecificeerd kan geen vaste reiskostenvergoeding gespecificeerd worden*	AB-Z	Op het moment dat de ZOK in het systeem door de BH opgesteld wordt, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.
Z4-M4 Application control	*invoer* Het systeem bewaakt consistentie in vast te leggen gegevens per type zorgovereenkomst : *- bij zorginstellingen kunnen geen reiskosten vastgelegd worden*	AB-Z	Op het moment dat de ZOK in het systeem door de BH opgesteld wordt, of de SVB (WMO/JW) of het zorgkantoor (Wlz) dat voor hem/haar doet.
D1-M1 IT dependent control	Papieren declaraties worden gescand en herkend door middel van applicaties AIDA en Prokey. Een medewerker valideert in een werktaak of het juiste type document is herkend, en of de gegevens juist vanaf het document herkend zijn voordat de declaratie verwerkt wordt. Onderdeel van de te herkennen gegevens is de budgethouder aan de hand van diens BSN, het bedrag en de zorgverlener.	SVB	Na ontvangst van de papieren declaratie
D2-M1 Application control	*invoer* Het systeem dwingt via verplichte invoervelden af dat de wettelijk vereiste gegevens voor declaratie worden ingevoerd. Als verplichte gegevens achterwege worden gelaten, is vastleggen van de declaratie niet mogelijk. Het betreft de volgende gegevens: - naam budgethouder - burgerservicenummer (BSN) of klantnummer SVB of adres budgethouder - welke zorg er is verleend - bij urenbriefje: op welke dagen er is gewerkt - bij factuur: welke periode er is gewerkt - het totaal aantal uren en het uurtarief zoals vermeld in de zorgovereenkomst - naam en BSN zorgverlener	SVB Budgeth.	Op het moment dat de papieren declaratie door de SVB in het systeem ingevoerd wordt Op het moment dat de budgethouder de declaratie invoert

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
D2-M2 Application control	*invoer* In de digitale werkwijze moet de budgethouder ~~e~~xpliciet akkoord geven op de ingevoerde declaratie om deze door het systeem te laten verwerken. Als de budgethouder een wettelijk vertegenwoordiger heeft, is deze handeling voorbehouden aan de wettelijk vertegenwoordiger. Doordat de budgethouder of diens vertegenwoordiger ingelogd is via Digid (een niet-natuurlijke vertegenwoordiger: eHerkenning) wordt dit beschouwd als elektronische handtekening	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger de declaratie in het systeem invoert, of als de budgethouder of diens vertegenwoordiger een door de zorgverlener ingevoerde declaratie beoordeelt.
D2-M4 Application control	autorisatie / invoer In het scherm voor het invoeren van de declaratie moet de budgethouder eerst de gecontracteerde zorgverlener (en bij meerdere zorgovereenkomsten ook de juiste zorgovereenkomst) kiezen. Vervolgens moet bij het opgeven van de verleende zorg/ondersteuning gekozen worden uit de in de zorgovereenkomst vastgelegde werkzaamheden en tarieven gekozen worden. Daarmee is het tarief op de declaratie bepaald.	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger of zorgverlener de declaratie in het systeem invoert, of de SVB dat voor de budgethouder doet
D2-M5 Application control	invoer relatie D1-M1 In het scherm voor het invoeren van de declaratie moet het aantal geleverde eenheden werk aangegeven worden voordat de declaratie opgeslagen kan worden (uren, dagdelen, e.e.a. van hoe de werkzaamheden in de ZOK gespecificeerd zijn).	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger of zorgverlener de declaratie in het systeem invoert
D2-M6 Application control	invoer relatie D1-M1 Er kunnen alleen leveringsdatum(s) op de declaratie ingevoerd worden die liggen tussen de ingangsdatum en einddatum van de tkb en de zorgovereenkomst. Tevens kan de leveringsdatum niet in de toekomst liggen.	AB-Z	Op het moment dat de budgethouder, diens vertegenwoordiger of de zorgverlener de declaratie in het systeem invoert of de SVB dat doet voor de budgethouder
D2-M7 Application control	*proces functionaliteit* Na ontvangst en verwerking van een BAB (Budget Afsluitings Bericht) van de verstrekker is het niet meer mogelijk voor de budgethouder om een declaratie in te voeren	AB-Z	

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
D3-M1 Application control	*invoer* Bij het invoeren van een declaratie moet de budgethouder eerst de gecontracteerde zorgverlener (en bij meerdere zorgovereenkomsten ook de juiste zorgovereenkomst) kiezen. Daarmee is de declarant (de budgethouder) bepaald en komen diens gegevens zichtbaar op de declaratie terecht. In de profielgegevens heeft de budgethouder verplicht zijn BSN, adres en klantnummer bij de SVB vastgelegd. Daarmee zijn de benodigde gegevens op de declaratie bepaald. * geldig betekent: de zorgovereenkomst is goedgekeurd door de verstrekker, en de datum van feitelijke levering valt tussen de ingangs- en einddatum van de zorgovereenkomst.	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger of zorgverlener de declaratie in het systeem invoert, of de SVB dat voor de budgethouder doet
D3-M2 Application control	*proces functionaliteit en invoer* Bij het invoeren van een declaratie moet de budgethouder eerst de gecontracteerde zorgverlener (en bij meerdere zorgovereenkomsten ook de juiste zorgovereenkomst) kiezen. Daarmee is de zorgverlener bepaald en komen diens gegevens zichtbaar op de declaratie terecht, en via het profiel van de zorgverlener het IBAN, KvK nummer of geboortedatum of burgerservicenummer.	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger of zorgverlener de declaratie in het systeem invoert, of de SVB dat voor de budgethouder doet
D3-M3 Application control	*invoer* Er kunnen in het systeem geen reiskosten gedeclareerd worden als de zorgverlener een zorginstelling is	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger de declaratie in het systeem invoert of de SVB dat doet voor de budgethouder
D3-M4 Application control	*invoer* Er kunnen in het systeem alleen bijkomende kosten gedeclareerd worden als er een zorgovereenkomst is gesloten met de betreffende zorgverlener	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger de declaratie in het systeem invoert of de SVB dat doet voor de budgethouder
D3-M5 Application control	Vervallen	-	-

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
D3-M6 Application control	*proces functionaliteit en invoer* Reiskosten voor zorgverleners kunnen alleen gedeclareerd worden als deze in de zorgovereenkomst benoemd zijn en goedgekeurd door de verstrekker, alleen dan presenteert de optie tot declareren van reiskosten zich aan de budgethouder. Bij vervoerskosten voor het openbaar vervoer moet de budgethouder vervoersbewijzen uploaden.	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger de declaratie in het systeem invoert of de SVB dat doet voor de budgethouder
D3-M8 Application control	*invoer* Declaraties voor vervoer van en naar 'begeleiding groep' kunnen alleen ingevoerd worden als deze in de zorgovereenkomst benoemd zijn en goedgekeurd zijn door de verstrekker, de ZOK nog geldig is of de geldigheid maximaal 10 weken geleden eindigde	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger de declaratie in het systeem invoert of de SVB dat doet voor de budgethouder
D3-M9 Application control	invoer Voor ingediende declaraties voor vervoer door middel van bijv. ov, waarbij er geen zorgovereenkomst is, die de bgh zelf heeft voorgeschoten moet de budgethouder een vervoersbewijs of factuur uploaden.	AB-Z	Op het moment dat de budgethouder of diens vertegenwoordiger de declaratie in het systeem invoert of de SVB dat doet voor de budgethouder
D3-M11 IT dependent control	*proces functionaliteit* Elke declaratie voor bijkomende kosten wordt middels een door het systeem aangemaakte werktaak ter goedkeuring aan de verstrekker aangeboden. Pas als de verstrekker de declaratie voor bijkomende kosten goedkeurt, wordt de declaratie verder verwerkt ter betaling.	Gemeente Zorgkantoor	Middels een werktaak na invoeren van de declaratie
D3-M12 Application control	*invoer* Er kan alleen een verzoek tot uitbetaling van een verantwoordingsvrij bedrag ingediend worden tijdens de looptijd van een TKB	AB-Z	
D3-M13 Application control	*proces functionaliteit en invoer* Er kan alleen een verzoek tot uitbetaling van het **verantwoordingsvrije** bedrag ingediend worden als er in de TKB een verantwoordingsvrij bedrag is toegekend, met in de Wlz een	AB-Z	Op het moment van indienen van het verzoek door de budgethouder

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
	minimum van 250,-		
D3-M14 Application control	*proces functionaliteit let op : differentiatie voor gegevens afkomstig uit de conversie.* Bij het indienen van een verzoek tot uitbetalen van een **verantwoordingsvrij** bedrag kan het bedrag niet hoger zijn dan dat wat er in de TKB gespecificeerd is (plus bij Wlz maximaal 1250,-), minus eventuele eerder uitbetaalde verantwoordingsvrije bedragen (geldt niet in situaties waarin de TKB gegevens en saldi **uit conversi**e in PGB 2.0 geladen zijn).	AB-Z	
D3-M15 Application control	*proces functionaliteit en invoer* Bij het indienen van een declaratie voor zorg en ondersteuning is het niet mogelijk werkzaamheden in rekening te brengen voor een maand waarop deze werkzaamheden al eerder gedeclareerd zijn (voorkomen dubbele declaratie). (Als er werkzaamheden voor een maand in rekening gebracht moeten worden voor een maand waarvoor al gedeclareerd is, zal de reeds ingediende declaratie voor die maand gecorrigeerd moeten worden door de budgethouder of diens vertegenwoordiger).	AB-Z	
D4-M1 Application control	*invoer* Het systeem biedt niet de mogelijkheid btw te specifcieren bij zorgkosten.	AB-Z	Voortdurend
B1-M1 Application control	*proces functionaliteit* Indien sprake van een maandloon, geeft het Z-Domein een maandelijkse opdracht tot betaling door aan het F-Domein o.b.v. het gedefinieerde maandloon in de geldige zorgovereenkomst.	AB-Z	Op het moment van de maandloonrun
B1-M2 Application control	*proces functionaliteit* Een vaste maandelijkse betaling op een ZOK die niet precies aan het begin of einde van een maand aanvangt of stopt, wordt automatisch naar rato (van totaal aantal (werk)dagen in de maand berekend.	AB-Z	Op het moment van de maandloonrun

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
B1-M3 Application control	*proces functionalitei* Het systeem stopt met aanmaken van betaalopdrachten voor maandbetalingen zodra de einddatum van de zorgovereenkomst of de TKB is bereikt.	AB-Z	Op het moment van de maandloonrun
B1-M4 Application control	*proces functionaliteit* Er worden alleen een OK2PAY bericht voor een declaratie aangemaakt indien de declaratie is goedgekeurd en ingediend door de budgethouder	AB-Z	Op het moment van indienen van een declaratie of op het moment van een run voor aanmaken maandlonen
B1-M4b Application control	*proces functionaliteit* Vóór het aanmaken van een OK2PAY bericht wordt eerst de loonsomservice aangeroepen om de werkgeverslasten te berekenen en zo het bruto bedrag te bepalen *wat in het betreffende OK2PAY bericht wordt opgenomen*. Dit geldt voor declaraties en maandlonen op basis van een ZOK AO.	AB-Z	Op het moment van indienen van een declaratie of op het moment van een run voor aanmaken maandlonen
B1-M5 Application control	Elk te betalen bedrag wordt gemaximeerd op de beschikbare hoeveelheid resterend budget (inclusief eventueel bijgestort bedrag budgethouder). Dit geldt voor: - betaling o.b.v. ingediende PGB declaraties - betaling o.b.v. ingediende declaraties bijkomende kosten - betaling o.b.v. ingediende declaraties vervoerskosten - betaling o.b.v. in ZOK vastgelegde vaste periodieke betalingen	AB-Z	Op het moment van een betaalrun
B2-M1 Application control	*proces functionaliteit* Betaalopdrachten n.a.v. door de budgethouder goedgekeurde en ingediende declaraties worden real-time gegeneerd en aan het financieel domein aangeboden. Declaraties kunnen altijd pas ingediend worden nadat de maand is verstreken. Tweemaal per week draait er een betaalrun. Maandlonen worden 'voorlopig' berekend rond de 21e van de maand - hier zit enige variatie in voor weekenden / feestdagen etc. Deze worden vervolgens meegenomen in bovengenoemde betaalruns. Vanaf de 4e dag van de volgende maand worden de maandlonen definitief berekend in verband met eventuele ziekmeldingen tussen de datum van het voorlopig maandloon en het einde van de maand. Definitieve berekeningen vinden dagelijks plaats op alle gewijzigde maandlonen in het verleden.	AB-Z	

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
B2-M3 Application control	*proces functionaliteit* Betaalopdrachten uit maandlonen worden maandelijks op de 24e van de te verlonen maand gegenereerd en aan het financieel domein aangeboden	AB-Z	
B3-M1 Application control	Vervallen		
B3-M2 Application control	*proces functionaliteit* Het resultaat van de verwerking van betaalopdrachten door het F-domein wordt verwerkt in het juiste budget, en op de juiste declaratie/ het juiste maandloon in het zorgdomein	AB-Z	
W1-M1 Application control	*proces functionaliteit en invoer* Opdrachten voor betaling van ziektegeld worden aangemaakt op basis van de zieketedatum die in een ziekmelding in het zorgdomein PGB 2.0 door de budgethouder of medewerker SVB is ingevoerd. Deze melding moet binnen 72 uur na aanvang van de ziekte gedaan worden.	AB-Z	
W1-M2 IT dependent control	*proces functionaliteit* Er wordt een werktaak 'Bereken maandloon' aangemaakt als uit de vergelijking van het voorlopige en herberekende maandloon één van volgende triggers afgaat: - Zorgverlener is gedeelte van de maand met zwangerschapsverlof - Zorgverlener is gedeelte van de maand ziek gemeld - Uitbetalen reiskosten eindigt halverwege de maand - %Arbeidsgeschiktheid is niet gedurende de hele maand gelijk - %Compensatie is niet gedurende de hele maand gelijk - Zorgverlener heeft AO, %Arbeidsgeschiktheid >0% en reiskostenvergoeding	AB-Z	Na invoeren van een ziekmelding door budgethouder of de SVB namens de budgethouder
W1-M3 Application control	*Invoer* Het tijdens de werktaak in te vullen ziekte-uren kan niet groter zijn dan het afgesproken aantal uren per maand (aantal uren afgesproken in de ZOK per week * 4.33). Als gevolg hiervan kan het totaal bedrag dat aan maandloon moet worden uitbetaald niet groter zijn	AB-Z	Tijdens afhandelen van de werktaak door SVB

Nr Soort	Beheersmaatregelen (bhm)	Uitwerking maatregel Wie	 Wanneer
	dan het afgesproken maandloon in de ZOK.		
W1-M4 Application control	*proces functionaliteit* Er kan niet meer ziekengeld betaald worden (en dientengevolge compensatie in het budget plaatsvinden) dan de omvang van het resterend budget toelaat. Indien deze situatie optreedt krijgt de budgethouder een verzoek het budget aan te vullen.	AB-Z	Tijdens afhandelen van de werktaak door SVB
W1-M8 Application control	Vervallen	-	-

4.2. General IT-Controls

Hieronder volgt per General IT-control de beschrijving van de uitgevoerde werkzaamheden en onze conclusie.

4.2.1 Wijzigingsbeheer

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat wijzigingen in de informatiesystemen op een gecontroleerde wijze worden uitgevoerd om het risico op ongeautoriseerde wijzigingen in de informatiesystemen te voorkomen. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls op het wijzigingsbeheer.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
W.1.	**Wijzigingen zijn geautoriseerd** Wijzigingen dienen van te voren te zijn geautoriseerd door de systeemeigenaar (deze kan ook gedelegeerd of op een andere wijze vertegenwoordigd zijn zoals in een change advisory board (CAB)).	*Testcriterium 1: stel vast dat er een aanvraag/verzoek aanwezig is voor de wijziging.* *Testcriterium 2: stel vast dat de wijzigingsaanvraag door de systeemeigenaar van tevoren is geautoriseerd.* Werkzaamheden: vastgesteld dat de opzetdocumentatie voor verschillende soorten wijzigingen aanwezig is en dat het verloopt via het indienen van RFC's tot en met in de productiename van wijzigingen. Wij hebben een review uitgevoerd op door Quality Assurance (hierna QA genoemd) uitgevoerde tweedelijnscontroles van 4 releases, met daarin zowel kleine als de grotere wijzigingen. Aanvullend zijn door de ADR aselect 14 wijzigingen beoordeeld, verspreid over de periode 1 april 2021-31 oktober 2021, hierbij hebben wij vastgesteld dat de aanvraag door een geautoriseerde medewerker is goedgekeurd. Bevindingen: wij constateren dat niet in alle gevallen afwijkingen van de opzet c.q. norm worden gedocumenteerd bij de door QA uitgevoerde tweedelijnscontroles (bijvoorbeeld als bepaalde werkstappen zijn overgeslagen). Hierdoor is niet duidelijk of een afwijking niet is geconstateerd	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat wijzigingen in de informatiesystemen op een gecontroleerde wijze worden uitgevoerd om het risico op ongeautoriseerde wijzigingen in de informatiesystemen te voorkomen. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls op het wijzigingsbeheer.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		of dat deze wel is geconstateerd, maar dat na afweging is besloten dat de betreffende afwijking geen noemenswaardige invloed heeft op het behalen van de (sub)beheersdoelstellingen van het Wijzigingsbeheer. Aanbeveling: wij bevelen aan om in de verslagen van de tweedelijnscontroles die door QA worden opgesteld voortaan per (sub)beheersdoelstelling de bevindingen samen te vatten c.q. (gemotiveerd) een conclusie te trekken, zodat daarmee de redeneerlijn naar de door VWS/QA op te stellen beschrijving en rapportage inzichtelijk wordt. Ook bevelen wij aan om een controlewerkprogramma (CWP) op te stellen, waarin de uit te voeren werkzaamheden zijn beschreven (wat, in welke frequentie en o.b.v. welke bescheiden). In het CWP dienen vervolgens de bevindingen (per periode, per release e.d.) chronologisch te worden opgenomen, dat is overzichtelijker en zo hoeven beschrijvingen en bevindingen maar één keer te worden genoteerd i.p.v. herhaling in elk controleverslag. In de bevindingen dient expliciete aandacht te zijn voor (regressie)testwerkzaamheden (controle en documentatie) en duiding van de stappen die in het Wijzigingsdocument wel zijn voorgeschreven maar die niet zijn gevolgd, met toelichting. Dit geldt ook voor de afwijkingen van de opzet zoals beschreven in het Wijzigingsdocument c.q. van voorliggende normen van het Wijzigingsbeheer. Hierdoor wordt inzichtelijk gemaakt dat een afwijking is geconstateerd en of deze, na afweging, wel of niet van invloed is op het behalen van de betreffende (sub)beheersdoelstelling van het Wijzigingsbeheer.	
W.1.2	**Wijzigingen worden getest**	*Testcriterium 1: stel vast dat de wijziging in een andere omgeving dan de productieomgeving is getest.*	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat wijzigingen in de informatiesystemen op een gecontroleerde wijze worden uitgevoerd om het risico op ongeautoriseerde wijzigingen in de informatiesystemen te voorkomen. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls op het wijzigingsbeheer.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	Wijzigingen worden getest in een andere omgeving dan de productieomgeving. Bij het testen is aandacht voor de belangrijkste bedrijfskritische functionaliteiten (denk hierbij aan een testscript of testplan).	*Testcriterium 2: stel vast dat voor de wijziging een testscript en/of testplan aanwezig is, waarin de belangrijkste functionaliteiten zijn beschreven.* *Testcriterium 3: stel vast dat de wijziging conform het testscript en/of testplan is getest en het bijbehorende resultaat is gedocumenteerd.* Werkzaamheden: de procedure rondom testen van wijzigingen (opzet) is ontvangen en over de verslagperiode is documentatie aangeleverd waaruit blijkt dat getest wordt in een van de productie afgescheiden testomgeving. Wij hebben een review uitgevoerd op door QA uitgevoerde tweedelijnscontroles van 4 releases, met daarin zowel kleine als de grotere wijzigingen. Aanvullend zijn door de ADR aselect 14 wijzigingen beoordeeld, verspreid over de periode 1 april 2021-31 oktober 2021. Aan de hand van schermprints in Jira en met toelichting van QA hebben wij vastgesteld dat testen plaatsvindt op basis van een Master Testplan (MTP) en van een (summier) draaiboek per release. Bevindingen: geen	
W.1.3	**Wijzigingen worden goedgekeurd met inachtneming van testresultaten.** Wijzigingen worden door de systeemeigenaar goedgekeurd op basis van gedocumenteerde testresultaten en pas daarna doorgevoerd in de productieomgeving.	*Testcriterium 1: stel vast dat de systeemeigenaar op basis van gedocumenteerde testresultaten de wijziging heeft goedgekeurd. Testcriterium 2: stel vast dat de wijziging pas na de goedkeuring door de systeemeigenaar in de productieomgeving is doorgevoerd.* Werkzaamheden: wij hebben een review uitgevoerd op door QA uitgevoerde tweedelijnscontroles van 4 releases, met daarin zowel kleine als de grotere wijzigingen. Aanvullend zijn door de ADR aselect 14 wijzigingen beoordeeld, verspreid over de periode 1 april 2021-31 oktober 2021. Wij hebben vastgesteld dat de systeemeigenaar (Product Owner) akkoord heeft gegeven	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat wijzigingen in de informatiesystemen op een gecontroleerde wijze worden uitgevoerd om het risico op ongeautoriseerde wijzigingen in de informatiesystemen te voorkomen. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls op het wijzigingsbeheer.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		op de testresultaten alvorens deze wijzigingen in de betreffende release werden opgenomen. Bevindingen: geen	
W.1.4	**Functiescheiding bestaat tussen het aanvragen, goedkeuren en doorvoeren van wijzigingen.** Er dient functiescheiding te zijn ingericht tussen het aanvragen, goedkeuren en doorvoeren van wijzigingen om onbevoegde en onbedoelde wijzigingen te beperken. Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een kritisch informatiesysteem te beheersen.	*Testcriterium 1: stel vast dat er functiescheiding is ingericht tussen het aanvragen, goedkeuren en doorvoeren van wijzigingen (zie hiervoor ook control W1.1 t/m W1.3).* *Testcriterium 2: stel vast dat alleen geautoriseerde medewerkers wijzigingen in productieomgeving kunnen zetten NB: stel hierbij ook vast dat ontwikkelaars geen wijzigingen in productie kunnen zetten.* Werkzaamheden: de beoordeelde wijzigingsprocedures borgen in opzet de noodzakelijke functiescheiding. Het bestaan en de werking hiervan zijn vastgesteld o.b.v. review van door QA uitgevoerde tweedelijnscontroles van 4 releases met daarin zowel kleine als de grotere wijzigingen. Aanvullend zijn door de ADR aselect 14 wijzigingen beoordeeld, verspreid over de periode 1 april 2021-31 oktober 2021. Ook hebben wij een demonstratie bijgewoond van het ontwikkelteam waarin aannemelijk is gemaakt dat medewerkers van dat team andere medewerkers zijn dan de beheerder(s) in de productie-omgeving. Verder hebben wij vastgesteld dat technisch applicatiebeheerders rechtstreeks op de database correcties (moeten) kunnen uitvoeren, maar dat zij met die rechten niet de software kunnen aanpassen. Bevindingen: geen	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat wijzigingen in de informatiesystemen op een gecontroleerde wijze worden uitgevoerd om het risico op ongeautoriseerde wijzigingen in de informatiesystemen te voorkomen. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls op het wijzigingsbeheer.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
W.1.5	**Periodieke controle op ongeautoriseerde wijzigingen.** Er dient periodiek controle plaats te vinden op wijzigingen aan het systeem, zodanig dat oneigenlijke wijzigingen worden gesignaleerd.	*Testcriterium 1: stel vast dat periodiek een controle heeft plaatsgevonden op wijzigingen aan het systeem.* *Testcriterium 2: stel vast dat er correctieve acties zijn ondernomen indien er naar aanleiding van de periodieke controle oneigenlijke wijzigingen zijn gesignaleerd.* Wij hebben een demonstratie van de merge-check bijgewoond en aan de hand daarvan vastgesteld dat controle op ongeautoriseerde wijzigingen plaatsvindt bij elke release en dat deze check op elk moment kan worden uitgevoerd. Voorts hebben wij vastgesteld dat opvolging plaatsvindt indien oneigenlijke wijzigingen zijn gesignaleerd. Bevindingen: hoewel voldoende aannemelijk is gemaakt dat bij een release een controle uitgevoerd wordt -en dat dit ook tussentijds kan worden uitgevoerd- op ongeautoriseerde wijzigingen, vindt dit niet separaat van de reguliere eerstelijnscontroles en ook niet periodiek plaats. Het verdient de voorkeur dat de getroffen waarborgen in het voortbrengingsproces (eerste lijn) op basis van een afzonderlijk controlewerkprogramma en periodiek worden vastgesteld. Aanbeveling: stel een controlewerkprogramma op waarin het periodiek testen van de controle op ongeautoriseerde wijzingen in tweedelijnscontroles is opgenomen.	Effectief

4.2.2 Incidentmanagement

De beheersingsmaatregelen waarborgen dat de (mogelijke) impact van incidenten op de juistheid, volledigheid en tijdigheid van verwerkingen in PGB 2.0 geminimaliseerd en waar mogelijk genihileerd worden. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls mede op het incidentmanagement.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
O3.1.	**Incidenten worden vastgelegd en vervolgstappen worden geadministreerd.** De beheerorganisatie gebruikt een Incidentmanagement systeem, waarin alle incidenten en het verloop van de oplossing geadministreerd worden.	*Testcriterium 1: stel vast dat het proces incidentmanagement is beschreven in procedure en procesbeschrijving.* *Testcriterium 1: stel vast dat incidenten worden geadministreerd. Testcriterium 2: stel vast dat vervolgstappen worden geadministreerd.* Werkzaamheden: wij hebben kennisgenomen van het incidentmanagementproces en het registratietool Topdesk. Wij hebben een review uitgevoerd van de door QA uitgevoerde controlewerkzaamheden en aselect 14 posten beoordeeld uit incidentmeldingen in de periode 1 april-31 oktober 2021 en vastgesteld dat de registratie van meldingen en vervolgstappen op de voorgeschreven wijze zijn doorlopen. Bevindingen: geen	Effectief
O3.2	**Incidenten worden gecategoriseerd en geprioriteerd.** In het incidentmanagementsysteem worden categorieën gedefinieerd. Incidenten worden na administratie ingedeeld naar categorie, waarmee de prioriteit bepaald is.	*Testcriterium 1: stel vast dat incidenten worden gecategoriseerd. Testcriterium 2: stel vast dat incidenten worden geprioriteerd.* Werkzaamheden: wij hebben kennisgenomen van de incidentcategorieën die zijn gedefinieerd en de manier waarop incidenten in Topdesk worden geregistreerd. Wij hebben een review uitgevoerd op door QA uitgevoerde controlewerkzaamheden en aselect 14 posten beoordeeld uit incidentmeldingen in de periode 1 april-31 oktober 2021 en vastgesteld dat incidenten zijn gecategoriseerd en geprioriteerd.	Effectief

De beheersingsmaatregelen waarborgen dat de (mogelijke) impact van incidenten op de juistheid, volledigheid en tijdigheid van verwerkingen in PGB 2.0 geminimaliseerd en waar mogelijk genihileerd worden. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls mede op het incidentmanagement.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		Bevindingen : geen	
O3.3	**Incidenten worden geanalyseerd naar oorzaak en mogelijke oplossingen.** Bij het behandelen van incidenten wordt vastgesteld of het incident door de melder (1e lijn), functioneel beheerder van de melder (2e lijn), TAB of FAB (3e lijn) of Technisch Beheer (4e lijn) opgepakt en geanalyseerd moet worden.	*Testcriterium 1: stel vast dat oorzaken van incidenten geanalyseerd worden en de uitkomst van de analyse wordt vastgelegd.* *Testcriterium 2: stel vast dat mogelijke oplossingen voor incidenten gezocht en vastgelegd worden.* Werkzaamheden: wij hebben kennisgenomen van de manier waarop van incidenten de oorzaak en mogelijke oplossingen worden geregistreerd en een review uitgevoerd van door QA uitgevoerde tweedelijnscontrole. Wij hebben aselect 14 incidentmeldingen van de periode 1 april-31 oktober 2021 beoordeeld en vastgesteld dat van incidenten de behandeling en oplossing zijn vastgesteld en vastgelegd. Bevindingen : geen	Effectief
O3.4	**Incidenten worden z.s.m. opgelost en de oplossing wordt vastgelegd.** Er zijn standaard tijdslijnen en kwaliteitsniveaus voor de categorieën incidenten vastgesteld, inclusief escalatieladders als deze overschreden worden. Het incidentmanagementsysteem ondersteunt het bewaken van de voortgang van het oplossen van incidenten, en signaleert als standaard	*Testcriterium 1: stel vast dat oplostijden zijn gedefinieerd. Testcriterium 2: stel vast dat de geboden oplossing wordt vastgelegd.* Werkzaamheden: wij hebben kennisgenomen van de gedefinieerde oplostijden en van de manier waarop van incidenten de oplostijden worden bepaald. Wij hebben een review uitgevoerd van controlewerkzaamheden van QA en aselect 14 posten geselecteerd uit incidentmeldingen in de periode 1 april-31 oktober 2021 en vastgesteld dat voor incidenten oplostijden zijn bepaald en op doorlooptijden zijn bewaakt. Bevindingen : geen	Effectief

De beheersingsmaatregelen waarborgen dat de (mogelijke) impact van incidenten op de juistheid, volledigheid en tijdigheid van verwerkingen in PGB 2.0 geminimaliseerd en waar mogelijk genihileerd worden. Naast de beheersdoelstelling van wijzigingsbeheer op zich, is de goede werking van de application controls hier eveneens mede van afhankelijk. In dit assurance onderzoek steunt de beeldvorming over de opzet, bestaan en werking van de application controls mede op het incidentmanagement.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	doorlooptijden overschreden worden.		
O3.5	**Incidenten worden teruggekoppeld en afgemeld aan de melder.** Het incidentmanagementsysteem ondersteunt in het afmelden van opgeloste incidenten aan de melder.	*Testcriterium 1: stel vast dat registraties van incidentmeldingen worden teruggekoppeld aan de melder.* *Testcriterium 2: stel vast dat afwikkeling van de incidentmeldingen worden teruggekoppeld aan de melder.* Werkzaamheden: wij hebben kennisgenomen van de gedefinieerde oplostijden en van de manier waarop van incidenten de oplostijden worden bepaald. Wij hebben een review uitgevoerd op controlewerkzaamheden van QA en aselect 14 posten geselecteerd uit incidentmeldingen in de periode 1 april-31 oktober 2021 en vastgesteld dat de afhandeling van incidenten aan de melder zijn teruggekoppeld. Bevindingen : geen	Effectief

4.2.3 Problemmanagement

De beheersingsmaatregelen waarborgen dat de (mogelijke) impact van problemen op de juistheid, tijdigheid en volledigheid van de verwerkingen in PGB 2.0 geminimaliseerd en waar mogelijk genihileerd worden.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
O3.6	**Problemen worden gesignaleerd en geadministreerd op basis van trendanalyses of terugkerende incidenten.**	*Testcriterium 1: stel vast dat er een procedure is voor het signaleren van problemen op basis van trendanalyse of terugkerende incidenten.* *Testcriterium 2: stel vast dat er een administratie is van terugkerende incidenten/trends.*	Effectief

De beheersingsmaatregelen waarborgen dat de (mogelijke) impact van problemen op de juistheid, tijdigheid en volledigheid van de verwerkingen in PGB 2.0 geminimaliseerd en waar mogelijk genihileerd worden.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	Problemmanagement wordt ondersteund middels de tool Topdesk.	Werkzaamheden: Wij hebben kennisgenomen van de werkafspraken voor problemmanagement in Topdesk en een review uitgevoerd op de controlewerkzaamheden van QA. Vastgesteld dat er een administratie is van terugkerende incidenten. Bevindingen: geen	
O3.7	**Problemen worden geanalyseerd op oorzaken en mogelijke oplossingen.**	*Testcriterium 1: stel vast dat problemen worden geanalyseerd op oorzaken en dat deze analyses worden vastgelegd.* *Testcriterium 2: stel vast dat problemen worden geanalyseerd op mogelijke oplossingen en dat deze analyses worden vastgelegd.* Werkzaamheden: wij hebben een review uitgevoerd op de tweedelijnscontrole van QA en kennisgenomen van de maandoverzichten waarin probleemanalyses zijn vastgelegd. Bevindingen : geen	Effectief
O3.8	**Problemen worden afhankelijk van de mogelijkheden** - **Opgelost** - **In de toekomst voorkomen** - **omzeild**	*Testcriterium 1: stel vast dat problemen worden opgelost, in de toekomst voorkomen of omzeild.* *Testcriterium 2: stel vast dat de keuze voor een van bovenstaande categorieën gemotiveerd is en vastgelegd.* Werkzaamheden: Wij hebben kennisgenomen van de manier waarop opvolging wordt gegeven aan problemen en de vastlegging daarvan. Wij hebben een review uitgevoerd op controlewerkzaamheden van QA en 4 deelwaarnemingen gedaan om vast te stellen dat problemen in een van de categorieën zijn ingedeeld. Bevindingen : geen	Effectief

De beheersingsmaatregelen waarborgen dat de (mogelijke) impact van problemen op de juistheid, tijdigheid en volledigheid van de verwerkingen in PGB 2.0 geminimaliseerd en waar mogelijk genihileerd worden.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
O3.9	**De oplossing of workaround wordt vastgelegd.**	*Testcriterium 1: stel vast dat workarounds worden vastgelegd.* Werkzaamheden: wij hebben kennisgenomen van de maandrapportages met known-errors waarin oplossingen en workarounds zijn vastgelegd. Bevindingen : geen	Effectief

4.2.4 Koppelvlakken

Koppelvlakken verbinden het Zorgdomein (TBO, VWS) en Financieel domein (SVB) met elkaar teneinde een juiste, tijdige en volledige gegevensuitwisseling te bewerkstelligen. De koppelvlakken zijn de gemeenschappelijke voorziening van VWS en SVB tussen het Zorg- en het Financieel domein en zijn daarmee hetzelfde als bij SVB. VWS maakt bij de interne beheersing van de koppelvlakken gebruik van de maandelijks opgestelde aansluiting tussen het Zorg- en Financieel domein door SVB. Het zou inefficiënt zijn om dezelfde controle tweemaal uit te voeren. Vooraf voor elk van de normen hebben wij vastgesteld dat gebruik gemaakt kan worden van de door SVB uitgevoerde interne controlewerkzaamheden. Deze zijn van belang voor het vaststellen van de opzet, het bestaan en de werking van de doelstellingen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
O2.1	**De gegevensuitwisseling tussen zorg- en financieel domein is juist, tijdig en volledig**. Tussen Z en F zijn koppelvlakken, indien een bericht goed in het F- domein is verwerkt dan wordt er een OK teruggegeven. Indien deze in het F- domein (FUSE of EBS) niet verwerkt kan worden dan wordt een NOK retour gegeven.	*Testcriterium 1: maandelijks worden controles uitgevoerd op NOK-berichten. Testcriterium 2: bevindingen uit de rapportages krijgen opvolging.* Werkzaamheden: van de maandelijks door SVB opgestelde memo met aansluiting en analyse hebben wij vastgesteld dat aansluitingen zijn gemaakt, dat verschillen zijn geanalyseerd en dat zo nodig verbeteringen hebben plaatsgevonden. In de verslagperiode 1 april-31 oktober 2021 zijn door Operational Control (SVB) 25 posten geselecteerd. Wij hebben vastgesteld dat over de uitkomsten daarvan is gerapporteerd aan de Auditdiensten.	Effectief

Koppelvlakken verbinden het Zorgdomein (TBO, VWS) en Financieel domein (SVB) met elkaar teneinde een juiste, tijdige en volledige gegevensuitwisseling te bewerkstelligen. De koppelvlakken zijn de gemeenschappelijke voorziening van VWS en SVB tussen het Zorg- en het Financieel domein en zijn daarmee hetzelfde als bij SVB. VWS maakt bij de interne beheersing van de koppelvlakken gebruik van de maandelijks opgestelde aansluiting tussen het Zorg- en Financieel domein door SVB. Het zou inefficiënt zijn om dezelfde controle tweemaal uit te voeren.

Vooraf voor elk van de normen hebben wij vastgesteld dat gebruik gemaakt kan worden van de door SVB uitgevoerde interne controlewerkzaamheden. Deze zijn van belang voor het vaststellen van de opzet, het bestaan en de werking van de doelstellingen.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		Door de ADR is een 5-tal posten van de door Operational Control uitgevoerde controle voor review geselecteerd en is vastgesteld dat voor deze posten Operational Control de juiste conclusie heeft getrokken. Bevindingen: geen	
O2.2	**De werking van het koppelvlak tussen zorg- en financieel domein wordt gemonitord.** Om te voorkomen dat de NOK berichten niet opgepakt zouden worden, is er aan de F-domein kant een bestand gegenereerd dat dagelijks een Excel oplevert.	*Testcriterium 1: monitoring op de werking van het koppelvlak vind aantoonbaar plaats.* *Testcriterium 2: bevindingen uit de monitoring krijgen opvolging.* Werkzaamheden: wij hebben via een demonstratiesessie op 25 januari 2022 en aan de hand van memo's van maandelijkse aansluitingen (april tot en met oktober 2021 en nog een over de periode januari-juni 2021) vastgesteld dat Operational Control (SVB) maandelijks de eerstelijns controles, logbestanden en rapportages raadpleegt en verschillen laat verklaren en toeziet op opvolging. Bevindingen : geen	Effectief
O2.3	**Eventuele uitval of verstoring in het koppelvlak tussen zorg- en financieel domein wordt tijdig opgelost en gecorrigeerd**	*Testcriterium 1: verstoringen worden tijdig opgemerkt. Testcriterium 2: correcties vinden tijdig plaats.* Werkzaamheden: wij hebben vastgesteld dat Operational Control (SVB) zich vergewist van uitval of verstoringen in het koppelvlak en nagaat of controles in de eerste lijn goed worden uitgevoerd. Daarbij is het begrip tijdigheid niet	Effectief

	Koppelvlakken verbinden het Zorgdomein (TBO, VWS) en Financieel domein (SVB) met elkaar teneinde een juiste, tijdige en volledige gegevensuitwisseling te bewerkstelligen. De koppelvlakken zijn de gemeenschappelijke voorziening van VWS en SVB tussen het Zorg- en het Financieel domein en zijn daarmee hetzelfde als bij SVB. VWS maakt bij de interne beheersing van de koppelvlakken gebruik van de maandelijks opgestelde aansluiting tussen het Zorg- en Financieel domein door SVB. Het zou inefficiënt zijn om dezelfde controle tweemaal uit te voeren. Vooraf voor elk van de normen hebben wij vastgesteld dat gebruik gemaakt kan worden van de door SVB uitgevoerde interne controlewerkzaamheden. Deze zijn van belang voor het vaststellen van de opzet, het bestaan en de werking van de doelstellingen.		
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	Indien wijzigingen door het zorgkantoor moeten worden gecorrigeerd dan zorgen de key-users er voor dat dit aan het betreffende zorgkantoor gecommuniceerd wordt.	nader gedefinieerd. Wij hebben vastgesteld dat geconstateerde fouten zijn gecorrigeerd of opgevangen met alternatieve maatregelen. Bevindingen: het aspect van tijdigheid is nog niet nader gespecificeerd, waardoor correcties mogelijk later dan wenselijk beschikbaar zijn. Aanbeveling: definieer het begrip tijdigheid in relatie tot een maximale doorlooptijd voor de oplossing.	
O2.4	**Periodieke aansluitcontrole Zorgdomein-Financieel domein** TBO neemt kennis van de (resultaten van de) maandelijkse en periodieke aansluitcontroles door de SVB zoals gedefinieerd in de beheersmaatregelen op het financieel domein, en analyseert waar van toepassing verschillen en oplossingen samen met de SVB.	*Testcriterium 1: QA ontvangt de maandelijkse rapportages van OC SVB. Testcriterium 2: QA analyseert de gerapporteerde resultaten van de aansluitcontroles.* Werkzaamheden: wij hebben aan de hand van de maandrapportages (zie O1.1) en een demonstratie hebben wij vastgesteld dat er een periodieke aansluitcontrole is uitgevoerd en dat deze door QA is geanalyseerd. Bevindingen: geen	Effectief

4.2.5 Wachtwoordbeheer

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat systemen voor wachtwoordbeheer interactief behoren te zijn en dat wachtwoorden van geschikte kwaliteit worden gekozen. Als algemeen punt bij wachtwoordbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
L1.1	**Wachtwoorden worden periodiek gewijzigd.** Alle wachtwoorden van beheerders dienen periodiek te worden gewijzigd, met een maximum van 12 maanden. Voor initiële wachtwoorden (bijvoorbeeld bij een nieuw account) dient deze wijziging al direct bij het eerste gebruik afgedwongen te worden. Wachtwoorden van systeemaccounts kunnen een uitzondering zijn, maar rondom wachtwoorden van systeemaccounts dienen wel beheersmaatregelen te zijn ingericht (denk hierbij aan een enveloppe procedure).	*Testcriterium 1: stel vast dat alle wachtwoorden van gebruikers en beheerders periodiek (maximaal 1 jaar) worden gewijzigd.* *Testcriterium 2: stel vast dat initiële wachtwoorden direct bij het eerste gebruik gewijzigd dienen te worden.* *Testcriterium 3: stel vast dat er voor wachtwoorden van systeemaccounts een aanvullende procedures (bijvoorbeeld enveloppe procedure) aanwezig is indien de wachtwoorden voor systeemaccounts zijn uitgezonderd van het algemene wachtwoordbeleid.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan per mei 2021) en DigiD assessments (april en oktober 2021) waarin deze norm grotendeels is meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd.	Effectief
L1.2	**Wachtwoorden zijn van adequate sterkte.** Een wachtwoord moet van voldoende complexiteit zijn, anders dient multifactor authenticatie gebruikt te worden. Ga er van uit dat ieder wachtwoord minstens 8 alfanumerieke tekens bevat, zowel hoofdletters als	*Testcriterium 1: stel vast dat de wachtwoordlengte meer dan 8 karakters bevat.* *Testcriterium 2: stel vast dat het wachtwoord aan complexiteitseisen moet voldoen: alfanumerieke tekens, zowel hoofd als kleine letters, minstens één nummer en één speciaal teken.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021) en DigiD assessments (april en oktober 2021) waarmee deze norm grotendeels is	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat systemen voor wachtwoordbeheer interactief behoren te zijn en dat wachtwoorden van geschikte kwaliteit worden gekozen. Als algemeen punt bij wachtwoordbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	kleine letters, minstens één nummer en één speciaal teken.	meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd.	
L1.3	**Twee-factor authenticatie wordt gebruikt bij onvertrouwde zones.** Voor toegang vanuit een onvertrouwde omgeving dient, twee-factor authenticatie te worden gebruikt.	*Testcriterium 1: stel vast dat voor toegang vanuit een onvertrouwde omgeving, twee-factor authenticatie wordt gebruikt.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021) en DigiD assessments (april en oktober 2021) waarmee deze norm grotendeels is meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd.	Effectief
L1.4	**Vergrendeling bij inactiviteit.** Na een periode van maximaal 15 minuten inactiviteit dient de toegang tot de applicatie te worden vergrendeld. Voorbeelden hiervan zijn het automatisch vergrendelen van een werkstation na een periode geen gebruikersinput te hebben ontvangen of het verlopen van de sessie in een webbrowser.	*Testcriterium 1: stel vast dat na een periode van maximaal 15 minuten inactiviteit de toegang tot de applicatie wordt vergrendeld.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021) en DigiD assessments (april en oktober 2021) waarmee deze norm grotendeels is meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd.	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat systemen voor wachtwoordbeheer interactief behoren te zijn en dat wachtwoorden van geschikte kwaliteit worden gekozen. Als algemeen punt bij wachtwoordbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
L1.5	**Wachtwoorden worden alleen versleuteld opgeslagen.** Wachtwoorden mogen niet in originele vorm (plaintext) worden opgeslagen, maar dienen in plaats daarvan versleuteld te worden.	*Testcriterium 1: stel vast dat wachtwoorden niet in de originele vorm (plaintext) zijn opgeslagen.* *Testcriterium 2: stel vast dat wachtwoorden versleuteld zijn.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021) en DigiD assessments (april en oktober 2021) waarmee deze norm grotendeels is meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd.	Effectief
L1.6	**Gebruikersaccounts dienen geblokkeerd te worden na een vooraf ingesteld aantal van vijf foutieve inlogpogingen.** Nadat maximaal 5 keer achter elkaar een foutief wachtwoord is opgegeven voor een account dient deze geblokkeerd te worden en geen nieuwe inlogpogingen te accepteren om zo brute-force aanvallen tegen te gaan.	*Testcriterium 1: stel vast dat na maximaal vijf keer achter elkaar een foutief wachtwoord is opgegeven het account wordt geblokkeerd.* *Testcriterium 2: stel ook vast dat het account minimaal 15 minuten wordt geblokkeerd of dat een beheerder nodig is om het account vrij te geven.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021) en DigiD assessments (april en oktober 2021) waarmee deze norm grotendeels is meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd.	Effectief

4.2.6 Gebruikersbeheer

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
L2.1	**Gebruikersaccounts hebben alleen de toegangsrechten die voor hun functie noodzakelijk is.** Beheerders krijgen slechts toegang tot functionaliteit (rol) die zij uit hoofde van hun functie nodig hebben waarbij functievermenging wordt uitgesloten (need to know, need to use). Daartoe is een beschrijving beschikbaar welke rollen en rechten per applicatie bij een functie horen. Hierbij is het van belang dat ongewenste functievermenging (conflicterende rechten) zowel binnen een applicatie als over applicaties heen wordt voorkomen.	*Testcriterium 1: stel vast dat een autorisatiematrix aanwezig is waarin in opzet is beschreven welke functies welke rollen/autorisatierechten behoren te krijgen.* *Testcriterium 2: stel vast dat een functiescheidingsmatrix aanwezig is waarin in opzet is beschreven welke functievermenging (conflicterende rechten/rollen) ongewenst is.* *Testcriterium 3: stel vast dat gebruikers slechts toegang tot functionaliteit (rol) hebben gekregen die zij uit hoofde van hun functie nodig hebben.* Werkzaamheden: wij hebben kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021) en DigiD assessments (april en oktober 2021) waarmee deze norm grotendeels is meegenomen. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021). Wij hebben deelwaarnemingen op 13 april en 29 oktober 2021 van QA beoordeeld en vastgesteld dat geen afwijkingen zijn geconstateerd. Bevinding 1: het op need to know basis toekennen van beheerautorisaties steunt op instellingen in Topdesk. Er geen ‘kant en klare’ autorisatie/rollen matrix beschikbaar voor de diverse beheerdersrollen. Er is in zowel opzet, bestaan als werking aandacht voor het toekennen van autorisaties. Medewerkers krijgen de autorisaties die voor het werk nodig zijn, echter zonder dat de afweging plaatsvindt of er sprake is van te uitgebreide rechten. Daardoor wordt onvoldoende specifiek invulling gegeven aan de beheersdoelstelling van het waarborgen van voldoende functiescheiding	Niet effectief Restrisico laag

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		Aanbeveling: stel een autorisatiematrix op waarin functiescheiding op basis van het need-to-know principe wordt uitgewerkt en waarbij expliciet wordt gemaakt welke bevoegdheden elke rol bevat. Richt vervolgens de rollen die via Topdesk worden uitgegeven in lijn met de autorisatiematrix in en onderhoud beide. Wij schatten het restrisico in als laag omdat voldoende aannemelijk is gemaakt dat gezien de geringe omvang van de organisatie men elkaar voldoende goed kent om het risico van onterecht te ruim uitgegeven toegang van beheerdersaccount te voorkomen; men weet uit het hoofd wie de beheerders zijn en wie welke rechten heeft en hoort te hebben.	
L2.2	**Gebruikersaccounts en toegangsrechten zijn geautoriseerd.** Het verlenen en muteren van beheerderssaccounts en toegangsrechten vindt plaats na goedkeuring door een bevoegde functionaris. Er is een actueel mandaatregister aanwezig waaruit blijkt welke personen beslissende bevoegdheden hebben voor het verlenen van een bepaald type (niveau) toegangsrechten danwel functieprofielen.	*Testcriterium 1: stel vast dat een actueel mandaatregister aanwezig is waaruit blijkt welke personen beslissingsbevoegdheden hebben voor het verlenen van een bepaald type (niveau) toegangsrechten dan wel functieprofielen.* *Testcriterium 2: stel vast dat het verlenen en muteren van gebruikersaccounts en toegangsrechten na goedkeuring door een bevoegde functionaris heeft plaatsgevonden.* *Testcriterium 3: stel vast dat het verlenen en muteren van toegangsrechten conform de aanvraag (en autorisatiematrix) heeft plaatsgevonden.* Werkzaamheden: wij hebben het proces van toegang verlenen beoordeeld en de autorisatie van toegangsverzoeken voor beheerdersaccounts onderzocht. Wij hebben een review uitgevoerd op de door QA uitgevoerde tweedelijnscontrole. Bevinding: het verlenen en muteren van beheerdersaccounts en toegangsrechten vindt niet plaats op basis van een expliciet vastgelegd mandaatregister; autorisaties worden verstrekt die voor het werk nodig zijn.	Niet effectief Restrisico laag

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		Op dit moment is er één type cFAB en AB, en twee types TAB (junior en senior), en daarmee een gering onderscheid. Wij beoordelen deze maatregel als niet effectief met een laag restrisico. Het ontbreken van een mandaatregister en expliciet opgestelde matrix van bevoegdheden wordt afgevangen door onderscheid naar cFAB, AB en TAB, waarvoor via een formeel proces toegangsrechten worden verleend. Aanbeveling: stel een mandaatregister op waarin is vastgelegd welke personen beslissingsbevoegdheden hebben voor het verlenen van welke type toegangsrechten.	
L2.3	**Functiescheiding bestaat tussen aanvragen, autoriseren en doorvoeren van wijzigingen in gebruikersaccounts en toegangsrechten.** Er bestaat functiescheiding tussen het aanvragen, autoriseren en doorvoeren van wijzigingen in beheerdersaccounts en toegangsrechten.	*Testcriterium 1: stel vast dat er functiescheiding bestaat tussen het aanvragen, autoriseren en doorvoeren van wijzigingen in gebruikersaccounts en toegangsrechten.* Werkzaamheden: wij hebben kennisgenomen van het assurancerapport BIO (opzet en bestaan mei) waarin deze norm gedeeltelijk is meegenomen en vastgesteld geen materiele afwijkingen zijn geconstateerd. Wij hebben kennisgenomen van de procedures voor het doorvoeren van wijzigingen in gebruikersaccounts en beheerdersaccounts en een review uitgevoerd op door QA uitgevoerde tweedelijnscontrole. Bevindingen: geen	Effectief
L2.4	**Uitdiensttredingen worden tijdig verwerkt.**	*Testcriterium 1: stel vast dat de toegangsrechten en het gebruikersaccount van de uitdiensttreder (tijdig) zijn ingetrokken.*	Niet effectief Restrisico laag

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	Uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen.	*Testcriterium 2: stel vast dat het intrekken van gebruikersaccounts en toegangsrechten na goedkeuring door een bevoegde functionaris heeft plaatsgevonden.* Werkzaamheden: wij hebben procesbeschrijving en procedures voor intrekken van toegangsrechten bestudeerd en kennisgenomen van BIO audit en NEN 7510 assurance rapporten (opzet en bestaan mei 2021) en DigiD assessments (opzet en bestaan april en oktober 2021) waarmee deze norm gedeeltelijk is mee genomen en vastgesteld in de verslagperiode een afwijking was geconstateerd, die in november was opgelost. Wij hebben kennisgenomen van de maandelijkse rapportages informatiebeveiliging en privacy (april tot en met oktober 2021) en de controlerapportage van QA. Bevinding: gedurende de verslagperiode zijn de rechten van één uitdienstreder niet ingetrokken. Ook werden controles niet voldoende frequent uitgevoerd. Zoals TBO zelf constateerde is er is onvoldoende zekerheid dat het intrekken van rechten als gevolg van uitdiensttredingen gedurende de verslagperiode voldoende zijn bewaakt en tijdig zijn verwerkt. Wij beoordelen deze maatregel als niet effectief met een laag restrisico omdat uit de controle bleek dat slechts van één voormalig medewerker de rechten niet tijdig waren ingetrokken en inmiddels acties zijn ondernomen om het controle- en beheersingsproces op orde te brengen. Deze verbetering blijkt ook uit de her-assessment DigiD. Aanbeveling: controleer periodiek de geldigheid van uitgegeven en ingetrokken toegangsrechten en neem de rapportages hierover op als evidence voor het aantoonbaar maken van de beheersmaatregelen van het Control Framework.	

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
L2.5	**Beheeraccounts zijn zo veel mogelijk beperkt en verklaard.** Het aantal beheeraccounts is beperkt en verklaard, en staat in logische verhouding tot de beheerders en of ICT afdeling.	*Testcriterium 1: stel vast dat het aantal beheerderaccounts is beperkt en verklaard.* Werkzaamheden: de procedure voor het toekennen en intrekken van beheeraccounts onderzocht/gecontroleerd en aan de hand van een door QA uitgevoerde tweedelijnscontrole (november 2021, op basis van binnen de verslagperiode vallende evidence) van uitgegeven en ingetrokken rechten het aantal beheeraccounts nagegaan. Bevinding: het aantal benodigde technisch applicatiebeheerders is niet verklaard. Er is alleen een differentiatie gemaakt tussen junior en senior en niet naar beheerobjecten. Wij beoordelen beheersmaatregel als niet effectief met een laag restrisico omdat het om een beperkt aantal beheeraccounts gaat en er differentiatie is aangebracht tussen enkele soorten beheerders accounts. De kans op misbruik of onterecht te veel uitgegeven beheerdersrechten is beperkt. Aanbeveling: ga na hoeveel beheeraccounts minimaal nodig zijn en breng meer differentiatie aan in beheeraccount. Maak de onderbouwing hiervoor expliciet.	Niet effectief Restrisico laag
L2.6	**Gebruikersaccounts en beheerderaccounts zijn persoonsgebonden en verklaard.** Gebruikersaccounts en beheeraccounts dienen altijd persoonsgebonden te zijn, zodat handelingen altijd te herleiden zijn naar één verantwoordelijke.	*TC1: stel vast dat gebruikersaccounts en beheeraccounts altijd persoonsgebonden zijn.* *TC2: stel vast dat er procedures aanwezig zijn m.b.t. eventuele generieke accounts (zoals systeem-, service, interface accounts).* Werkzaamheden: de procedure voor het toekennen en intrekken van beheeraccounts bekeken en aan de hand van een door QA uitgevoerde tweedelijnscontrole (november 2021, op basis van binnen de verslagperiode	Niet effectief Restrisico midden

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		vallende evidence) van uitgegeven en ingetrokken rechten het aantal beheeraccounts nagegaan. Bevinding: een niet persoonsgebonden testaccount staat gedurende de verslagperiode nog open. Dit is een bij de TBO bekend punt, waaraan in de verslagperiode nog geen opvolging aan is gegeven. Ook blijkt een in maart op inactief gezet testaccount in oktober nog actief te zijn geweest, terwijl deze in de rapportage van november nog of weer op inactief staat. Door het gebruik van niet persoonsgebonden gebruikersaccounts zijn (ongeoorloofde) handelingen van die accounts achteraf niet meer te herleiden naar één verantwoordelijke. Wij beoordelen deze maatregel als niet effectief met als restrisico midden. Weliswaar zijn slechts enkele niet persoonsgebonden gebruikersaccounts aanwezig, maar worden deze zonder onderliggende verklaring soms tussentijds actief gemaakt en is niet te achterhalen of zich ongeoorloofde activiteiten hebben voorgedaan met deze accounts. Aanbeveling: controleer meer frequent op uitgegeven en ingetrokken rechten en zorg voor adequate en tijdige (bv binnen dag of een week, afhankelijk van de aard van de afwijking) afwikkeling van bevindingen. Controleer het controleoverzicht op betrouwbaarheid.	
L2.7	**Gebruikersaccounts hebben geen directe toegang tot onderliggende componenten.** Eindgebruikers hebben geen directe toegang tot de onderliggende componenten (zoals de database).	*Testcriterium 1: stel vast dat eindgebruikers geen (directe) toegang hebben tot de onderliggende componenten (zoals de database en applicatieserver).* Werkzaamheden: wij hebben vastgesteld dat een DigiD assessment (opzet en bestaan in mei 2021) is uitgevoerd en de daarin opgemerkte tekortkoming eind oktober 2021 is opgelost. Alleen budgethouders verkrijgen toegang via DigiD toegang tot het Zorgdomein. Van andere eindgebruikersgroepen die toegang	Niet effectief Restrisico laag

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
		krijgen via bijvoorbeeld eHerkenning (vertegenwoordiger) of VECOZO (gemeenten) geen lijncontroles of audits aangetroffen. Bevinding: gezien de aard van de bevinding uit het DigiD assessment en het feit dat pas aan het einde van de verslagperiode is vastgesteld dat de afwijking is opgelost, is niet met voldoende zekerheid te stellen dat deze beheersmaatregel effectief heeft gewerkt. Daarnaast is ook het bereik van de DigiD assessment te beperkt om een beeld te vormen voor alle eindgebruikers van het Z-Domein. Wij beoordelen deze beheersmaatregel daarom als niet effectief met als restrisico laag omdat het, de uitkomsten van de DigiD assessment in acht nemende, onwaarschijnlijk is dat andere eindgebruikers zich wel toegang tot onderliggende componenten hebben kunnen verschaffen. Aanbeveling: zorg naast het uitvoeren van DigiD assessments voor vergelijkbare controles op toegang vanuit zorgkantoren, gemeentes en eventuele andere externe partijen.	
L2.8	**Alle accounts en toegangsrechten worden periodiek geëvalueerd en de uitkomsten opgevolgd.** Toegangsrechten op onderliggende componenten dienen periodiek, minimaal jaarlijks, geëvalueerd te worden. dit interval dient te zijn beschreven in het toegangsbeleid en zijn bepaald op basis van het	*Testcriterium 1: stel vast dat het interval van de periodieke evaluatie in het toegangsbeleid is bepaald (op basis van het risiconiveau).* *Testcriterium 2: stel vast dat de toegangsrechten en gebruikersaccounts minimaal eens per jaar zijn geëvalueerd.* *Testcriterium 3: stel vast dat de uitkomsten van de evaluatie en de opvolging daarvan zijn vastgelegd.* Werkzaamheden: review van de tweedelijnscontrole van QA en vastgesteld dat deze een afwijking van de norm signaleert.	Niet effectief Restrisico midden

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de logische toegang tot informatiesystemen is beperkt tot daartoe bevoegde personen. Aan gebruikers en beheerders toegewezen rechten zijn overeenkomstig de te vervullen functie en zijn geautoriseerd door daartoe bevoegde personen. Als algemeen punt bij gebruikersbeheer geldt dat de aangedragen evidence en waarnemingen, minimaal zijn omdat vooraf de norm niet geoperationaliseerd is naar aantal te nemen deelwaarnemingen en aan de aan de onderbouwende bescheiden te stellen eisen.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	risiconiveau. De uitkomsten van de evaluatie en de opvolging daarvan worden vastgelegd.	Bevinding: toegangsrechten worden onvoldoende periodiek geëvalueerd. Hierdoor ontbreekt een actueel inzicht in mogelijke kwetsbaarheden door onbedoelde onterecht openstaande bevoegdheden. Wij beoordelen deze beheersmaatregel als niet effectief met als restrisico midden omdat een periodieke controle een belangrijk beheersinstrument is om tijdig te kunnen acteren op ongeoorloofde handelingen vanwege kwetsbaarheden in toegangsrechten en accounts. Het is een van de basismaatregelen die het vangnet vormt voor als eerstelijns beheersmaatregelen falen.	

4.2.7 Beveiliging van componenten

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
L3.1	**Er is een actueel inzicht in de applicaties en onderliggende componenten.** Een randvoorwaarde om te beoordelen of de IT-infrastructuur voldoende is beveiligd is een accuraat inzicht in de beoogde opzet van de IT-infrastructuur (de architectuur) en een actueel inzicht in de werkelijk geconfigureerde hard- en software.	*TC1: stel vast dat een actuele systeemplaat/landschap beschikbaar is met alle servers en componenten in samenhang, die relatie hebben met PGB2.0 (ontwikkel-, test-, acceptatie - en productieomgeving).* *TC2: stel vast dat de werkelijk geconfigureerde hard- en software m.b.t. de servers en componenten in samenhang, die relatie hebben met PGB2.0, beschikbaar zijn.* Werkzaamheden: wij zijn nagegaan of een Configuratie Management Database (CMDB) of vergelijkbare administratie aanwezig is van de applicaties en onderliggende componenten in het landschap. Wij hebben een review uitgevoerd van de door QA uitgevoerde tweedelijnscontrole. Kennisgenomen van de uitkomsten de uitgevoerde Nessusscans die inzicht geven in de het aanwezige systeemlandschap. Kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021). Bevinding: in opzet is er geen procedure en procesbeschrijving aanwezig die voor deze norm gehanteerd kan worden voor de verslagperiode. De organisatie heeft aangegeven momenteel bezig te zijn met het ontwerpen van het proces Configuratiemanagement waarvan de implementatie van dit proces buiten de verslagperiode ligt van dit onderzoek. Door het ontbreken van een dergelijk proces/inrichting is een accuraat inzicht van de IT-infrastructuur niet geborgd.	Niet effectief Restrisico hoog

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		Momenteel wordt een Nessus scan gebruikt voor het verkrijgen van inzicht in de werkelijke geconfigureerde hard- en software. De volledigheid m.b.t. de IT- Infrastructuur en eventuele wijzigingen in de verslagperiode van deze scan is niet aangetoond. De uitvoering van een periodieke controle tussen de opzet en de daadwerkelijk geconfigureerde hard- en software is niet ingericht. Randvoorwaardelijk heeft deze norm L3.1 een uitwerking voor de andere L3 normen. Configuratiemanagement heeft voorts als doel om o.a.: - Verbeteren van het zicht op de onderhoudsstatus van IT-componenten (lifecycle, patches, versies etc.); - Kunnen leveren van ondersteunende informatie voor andere beheerprocessen zoals het incidentmanagement, change- en releasemanagement, securitymanagement en disaster recovery. Wij beoordelen deze beheersmaatregel als niet effectief met een hoog restrisico omdat de centrale basis ontbreekt die een goede beheersing en onderhoud van alle componenten in de IT-infrastructuur ondersteunt teneinde deze veilig (en continu) te laten functioneren. Aanbeveling: rond zo snel mogelijk de inrichting van het configuratiemanagement af, zodat een sterke basisadministratie voor de andere beheerprocessen beschikbaar komt.	

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
L3.2	**Alertering op nieuwe kwetsbaarheden is ingeregeld en systemen worden periodiek gecontroleerd op technische kwetsbaarheden.** Er is formeel een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal periodieke (geautomatiseerde) controle op de aanwezigheid van kwetsbaarheden in de te toetsen systemen, een risicoafweging en navolgbare afwerking daarvan of risicoacceptatie.	*TC1: stel vast dat een formeel proces is ingericht voor het beheer van technische kwetsbaarheden.* *TC2: stel vast dat een controle op de aanwezigheid van kwetsbaarheden in de te toetsen systemen heeft plaatsgevonden, waarbij een ook een risicoafweging en navolgbare afwerking daarvan of risico-acceptatie heeft plaatsgevonden.* Werkzaamheden: kennisgenomen van de procesbeschrijving van het vulnerability management en van de maandelijkse Nessuscans. Kennisgenomen van de manier waarop risico-afweging en afwerking of risico- acceptatie plaatsvindt. Kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021). In opzet is een formeel proces beschreven m.b.t. het vulnerability managementproces dat zich beperkt tot een zestal middelen/systemen. De organisatie heeft aangegeven dat deze beschrijving niet meer de daadwerkelijke scope weergeeft omdat meerdere middelen/systemen nu onderdeel zijn van de Nessus scan. In de verslagperiode is elke maand een Nessusscan uitgevoerd. Bevinding: hoewel wij deze beheersmaatregel als effectief beoordelen omdat de maandelijkse scans in de praktijk worden uitgevoerd en geëvalueerd, zijn de volledigheid	Effectief

		van de IT-Infrastructuur in de Nessusscans en eventuele	

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		wijzigingen hierin gedurende de verslagperiode niet aangetoond. Hierdoor bestaat een onzekerheid over de volledigheid van deze scans. Een periodieke controle om de werking van het vulnerability managementproces als geheel aantoonbaar te maken is in de verslagperiode niet ingericht. Aanbeveling: zie overkoepelende aanbeveling over operationaliseren control framework.	
L3.3	**Systemen worden tijdig gepatcht en geüpdatet.** Zodra kwetsbaarheden bekend zijn dienen de te beoordelen IT-systemen tijdig te worden gepatcht en geüpdatet. De tijdigheid wordt bepaald aan de hand van de urgentie van de kwetsbaarheid. Het patchen vindt plaats volgens de reguliere procedure of via een goedgekeurde noodprocedure.	*TC1: stel vast dat patches zijn beoordeeld (bijv. urgentie/prioriteit). TC2: stel vast dat patches tijdig zijn uitgerold.* Werkzaamheden: kennisgenomen van het beschreven patchmanagementproces. Review uitgevoerd op de tweedelijnscontrole en kennisgenomen van aangeleverde aanvullende informatie over patchmanagement. Kennisgenomen van overeenkomsten met OCD Noord en van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021). Bevinding: de conceptbeschrijving patchmanagement (13 december 2019, concept) beperkt zich tot een zestal middelen/systemen. Deze scope is in verhouding tot de gehele IT-infrastructuur beperkt. In de DAP met ODC-Noord is beschreven wat hun taken zijn t.a.v. patchmanagement. Een periodieke	Niet effectief Restrisico midden

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		controle om de werking aantoonbaar te maken voor de in scope zijnde systemen en componenten is voor de verslagperiode niet ingericht. Het bestaan is wel aangetoond. Wij beoordelen deze beheersmaatregel al niet effectief met als restrisico midden omdat de actualiteit van de procedure (opzet) niet is geborgd en de volledigheid van de componenten/systemen waarover patchmanagement van toepassing zou moeten zijn is niet aangetoond. Inzicht in de volledigheid heeft een relatie met L3.1 Aanbeveling: breid het bereik van het patchmanagementproces uit zodanig dat hierin de gehele IT-infrastructuur in scope is. Stel een definitieve versie formeel vast.	
L3.4	**Systemen maken geen gebruik van standaard wachtwoorden of backdoor accounts.** Standaard wachtwoorden van systemen en onderliggende componenten dienen te worden	*TC1: stel vast dat standaard wachtwoorden van systemen en onderliggende componenten gewijzigd zijn in de productieomgeving.* Werkzaamheden: wij hebben een review uitgevoerd op de tweedelijnscontroles en kennisgenomen van aangedragen beleidsdocumenten en periodieke rapportages. Kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021).	Niet effectief Restrisico midden

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
	gewijzigd alvorens deze in productie worden genomen.	Bevinding: hoewel in de aangedragen onderbouwingen geen afwijkingen zijn gesignaleerd, is de basis (alleen instellingen van de Windows accounts en eenmalige waarneming eind oktober 2021) ontoereikend om deze beheersmaatregel als effectief te evalueren. Een periodieke controle om de werking aantoonbaar te maken is voor de verslagperiode niet aanwezig. Het bestaan is wel aangetoond. Wij beoordelen deze beheersmaatregel als niet effectief met als restrisico midden omdat de actualiteit van de procedure (opzet) niet is geborgd en de volledigheid van de componenten/systemen waarover het beleid van toepassing zou moeten zijn is niet aangetoond. Inzicht in de volledigheid heeft een relatie met L3.1 Aanbeveling: richt een maandelijkse interne controle in om gedurende een hele verslagperiode vast te stellen dat instellingen zodanig zijn ingericht dat standaard wachtwoorden gewijzigd dienen te worden. Voer dit uit voor alle componenten binnen bereik van de IT-infrastructuur.	
L3.5	**Het besturingssysteem draait geen onnodige services.**	*TC1: stel vast dat softwarecomponenten en services die niet noodzakelijk zijn voor het functioneren van de IT-service zijn verwijderd of gedeactiveerd om beveiligingsrisico's te beperken.*	Niet effectief Restrisico laag

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen. Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	Softwarecomponenten en services die niet noodzakelijk zijn voor het functioneren van de IT-service zijn verwijderd of gedeactiveerd om beveiligingsrisico's te beperken.	Werkzaamheden: wij hebben een review uitgevoerd op tweedelijnscontroles en kennisgenomen van aangedragen beleidsdocumenten en periodieke rapportages. Kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021). Bevinding: de aangeleverde protocollen services en poorten zijn geen definitieve documenten, bevatten nog wijzigingsvoorstellen waarvan de laatste in 2020 zijn gedaan. Het is onzeker welke protocollen in de verslagperiode leidend waren en welke uitgangspunten golden en in hoeverre de volledige scope van de IT-infrastructuur werd geraakt. Een periodieke controle om de werking in de verslagperiode aantoonbaar te maken is niet ingericht, wel is enkele onderbouwing aangedragen die het bestaan van de beheersmaatregel aantoont. Wij beoordelen deze beheersmaatregel als niet effectief met als restrisico laag, omdat het hoewel het onzeker was welke protocollen in de verslagperiode leidend waren en welke uitgangspunten golden en in hoeverre de volledige scope van de IT-infrastructuur werd geraakt, wel onderbouwing is aangedragen die het bestaan van de beheersmaatregel aantoont. Aanbeveling: actualiseer de protocollen services en poorten en zorg hierin voor een bereik over de hele IT-infrastructuur. Richt een proces van continue	

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		evaluatie en verbetering in voor het actueel houden van deze protocollen. Stel definitieve versies formeel vast.	
L3.6	**Het interne netwerk is gescheiden van andere vertrouwde omgevingen.** Zonering binnen de technische infrastructuur vindt plaats conform de uitgangspunten die zijn vastgelegd in een operationeel beleidsdocument, waarbij minimaal sprake is van scheiding tussen vertrouwde en onvertrouwde netwerken.	*TC1: stel vast dat een operationeel beleidsdocument beschikbaar is.* *TC2: stel vast dat de zonering binnen de technische infrastructuur conform de uitgangspunten uit het operationeel beleid is ingericht, waarbij minimaal sprake is van scheiding tussen vertrouwde en onvertrouwde netwerken.* Werkzaamheden: wij hebben een review uitgevoerd op tweedelijnscontroles en kennisgenomen van aangedragen beleidsdocument, uitkomsten van Nessusscans en schermprints van een overzicht van wijzigingen op de IT- infrastructuur gedurende de verslagperiode. Kennisgenomen van de rapporten BIO audit en NEN 7510 assurancerapporten (opzet en bestaan mei 2021). Bevinding: hoewel aannemelijk is dat voor PGB2.0 zonering is toegepast, is niet vast te stellen of dit op een effectieve manier heeft gefunctioneerd. Het document High Level Design Infrastructuur PGB20 beschrijft de globale instellingen, netwerkarchitectuur, kaders en richtlijnen. Er wordt niet op technisch detailniveau ingegaan op instellingen van routers, firewalls, virtualisatie, (virtuele) servers en de overige COTS oplossingen. Het document PGB2.0 Netwerkbeveiliging heeft als doel om eisen te stellen aan de hosting partij van Infrastructure as a Service (IaaS) om zodoende bij te dragen aan	Niet effectief Restrisico laag

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar
o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		een stabiele, betrouwbare en veilige dienstverlening. Het document dateert van 11 november 2019 versie 1.0 . In hoofdstuk 4 onderdeel 6 'Zonering' staat opgenomen:" *Er wordt gebruik gemaakt van zonering zodat risico's binnen een zones geïsoleerd kunnen worden, de gehanteerde maatregelen binnen de zones of koppelvlakken zijn voor TBO inzichtelijk.* " Het is niet aantoonbaar gemaakt dat maatregelen zijn genomen om zonering in te richten en of deze maatregelen in de verslagperiode hebben gewerkt. Een periodieke controle om de werking gedurende de verslagperiode aantoonbaar te maken is niet ingericht. Wij beoordelen deze beheersmaatregel als niet effectief met als restrisico laag, omdat op High Level in opzet zonering is aangetoond. Aanbeveling: actualiseer de beleidsdocumenten en zorg hierin voor een bereik over de hele IT-infrastructuur. Richt een proces van continue evaluatie en verbetering in voor het actueel houden van deze protocollen. Stel definitieve versies formeel vast.	
L3.7	**Netwerk-verkeer en componenten worden actief gemonitord.**	*Testcriterium 1:* S*tel vast dat actieve monitoring van het netwerkverkeer en de componenten plaatsvindt.* *Testcriterium 2: stel vast dat een opvolging wordt gegeven aan beveiligingsincidenten en -gebeurtenissen.*	Niet effectief Restrisico laag / midden

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
	Actieve monitoring van het netwerkverkeer en de componenten vindt plaats zodat beveiligingsincidenten en - gebeurtenissen in een vroeg stadium worden gedetecteerd. Hier moet men denken aan misbruik door gebruikers van informatiesystemen (outsider en insider threats) die van invloed zijn op de integriteit van de gegevens die de jaarrekening beïnvloeden.	Werkzaamheden: wij hebben een review uitgevoerd op controlewerkzaamheden van de door QA uitgevoerde tweedelijnscontrole en kennisgenomen van aangedragen beleidsdocument logging en monitoring. Interviews gehouden met QA en betrokken bij monitoring betrokken functionarissen. Bevinding: in opzet zijn er geen procedure en/of procesbeschrijving aangeleverd die inzicht geven in de manier waarop actieve monitoring van het netwerk en de componenten in de verslagperiode heeft plaatsgevonden en op welke manier daar verantwoording over is afgelegd. De organisatie geeft aan dat eind oktober 2021 een IDS/IPS is geïmplementeerd. Dit valt echter zodanig beperkt binnen de verslagperiode dat wij deze beheersmaatregel niet als effectief kunnen aanmerken. Wij beoordelen deze beheersmaatregel als niet effectief met als restrisico laag, (ten tijde van uitbrengen rapport) / midden (ten tijde van verslagperiode), omdat: hoewel over het begin van de verslagperiode geen beschrijving kon worden aangeleverd aan de hand waarvan is vast te stellen of de juiste en volledige zaken zijn gemonitord, is wel vastgesteld dat in de verslagperiode actieve monitoring op het netwerk en componenten heeft plaatsgevonden. TBO	

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat de systemen en de onderliggende componenten zijn beveiligd om het risico op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies te voorkomen.

Wij hebben voor onderstaande normen geen vooropgezette tweedelijnscontroles aangetroffen die aantoonbaar opzet en werking vaststellen en aantonen of tenminste aannemelijk maken dat de PBG2.0 hierover in control is. De normen zijn door de organisatie niet geoperationaliseerd naar o.a. gestandaardiseerde periodieke controles, of vooraf beschreven objecten en populaties, met gedefinieerde verwachte uitkomsten en de manier van handelen bij geconstateerde afwijkingen. Hierdoor was op voorhand geen toereikende controle informatie beschikbaar voor o.a. de verantwoording over de normenset. Samen met de interne auditor hebben wij zo veel mogelijk controle informatie verzameld om toch een toereikend beeld te krijgen over de opzet en bestaan van de beheersmaatregelen. Niet voor alle beheersmaatregelen is dit gelukt. In onderstaande tabel zijn onze bevindingen toegelicht.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
		geeft aan dat eind oktober 2021 het IDS/IPS proces beter is beschreven, en het IDS/IPS is aangevuld met Elastic Stack en dat ook de nieuwe DigiD assessment een goedkeuring opleverde. Dit valt echter zodanig beperkt binnen de verslagperiode dat wij deze beheersmaatregel over de verslagperiode niet als effectief kunnen aanmerken. Aanbeveling: stel een procedure en procesbeschrijving op waarin de manier van actieve monitoring is beschreven en sluit daarbij aan op het in oktober 2021 geïmplementeerde IDS/IPS. Richt een proces in van periodieke interne controle op de uitkomsten van de monitoring.	

4.2.8 Back-up en recovery

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat back-ups in overeenstemming met het back-upbeleid worden gemaakt en dat backups hersteld kunnen worden.

Norm	Beheersmaatregel	Uitgevoerde testen	Oordeel ADR
O1.1	**De periodiciteit van, en het type gegevens op, de back-up sluiten**	*Testcriterium 1: stel vast dat TBO afspraken met klanten en ODC-N maakt omtrent de periodiciteit, de soort (OS/DB) en retentietijd van back-ups zijn vastgelegd (bijvoorbeeld SLA, DAP, etc.).*	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat back-ups in overeenstemming met het back-upbeleid worden gemaakt en dat backups hersteld kunnen worden.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	aan bij het belang van de voor de jaarrekening kritische systemen. De periodiciteit van de back-up dient aan te sluiten bij de maximaal toegestane periode waarover gegevens verloren mogen raken. Stel vast dat de back-up de juiste systemen en data bestanden omvat die relevant zijn voor de jaarrekening.	*Testcriterium 2: stel vast dat de periodiciteit van de back-up, soort back-up en retentietijd van back-ups (back-upschema) aansluit bij de afspraken met de klanten of in de standaard dienstverlening van ODC-N.* Werkzaamheden: wij hebben een review uitgevoerd op de door QA uitgevoerde tweedelijnscontrole. Kennisgenomen van de procedure Back-up en Recovery en het informatiebeveiligingsbeleid PGB2.0 en de daarin opgenomen bepalingen voor Back-up en restore. Kennisgenomen van de DVA met ODC-N en van de servicerapportages. Kennisgenomen van ICV ODC-N (opzet en bestaan november 2021) Bevinding: een in het informatiebeveiligingsbeleid voorgeschreven continuïteitsplan ontbreekt, waardoor mogelijk in geval van calamiteiten onvoldoende de beschikbaarheid van gegevens in de voor de jaarrekening kritieke systemen is gewaarborgd. Gezien de aard van deze bevinding en de kleine kans op calamiteiten zien wij hierin geen aanleiding om deze beheersmaatregel als niet-effectief aan te merken. Aanbeveling: kom met ODC-N overeen dat een calamiteitenplan wordt opgesteld, onderhouden en dat maatregelen conform het calamiteitenplan worden ingericht.	
a	**De back-up gegevens worden op een veilige locatie bewaard waarbij de integriteit van de back-up gewaarborgd blijft.** Stel vast, nadat in O1.1 is bepaald dat de back-up tijdig en volledig tot stand	*Testcriterium 1: stel vast op welke wijze de back-ups worden opgeslagen. Testcriterium 2: stel vast dat de opgeslagen back-up beveiligd is tegen onbevoegde wijzigingen.* *Testcriterium 3: stel vast dat de back-ups op dusdanige afstand van de bron zijn opgeslagen dat een mogelijke calamiteit bij de bron geen effect heeft op de back-ups.* *Testcriterium 4: stel vast dat back-up jobs worden gemonitord en bij fouten/niet gelopen back-ups correctieve acties worden uitgevoerd.*	Effectief

De beheersingsmaatregelen waarborgen met een redelijke mate van zekerheid dat back-ups in overeenstemming met het back-upbeleid worden gemaakt en dat backups hersteld kunnen worden.			
Norm	**Beheersmaatregel**	**Uitgevoerde testen**	**Oordeel ADR**
	is gekomen, op welke wijze de back-up wordt opgeslagen. Stel vast dat de opgeslagen back-up beveiligd is tegen onbevoegde wijzigingen en op dusdanige afstand van de bron is opgeslagen dat een mogelijke calamiteit bij de bron geen effect heeft op de back-up.	Werkzaamheden: wij hebben een review uitgevoerd op de door QA uitgevoerde tweedelijnscontrole. Kennisgenomen van de procedure Back-up en Recovery en het informatiebeveiligingsbeleid PGB2.0 en de daarin opgenomen bepalingen voor Back-up en Restore. Kennisgenomen van de DVA met ODC-N en van de servicerapportages. Kennisgenomen van ICV ODC-N (opzet en bestaan november 2021) Bevinding: geen	

O1.3	**Het kunnen terugzetten van de back-up (recovery) wordt periodiek getest.** Om te bepalen of back-ups ook correct kunnen worden teruggezet is het van belang te bepalen of de recovery procedure betrouwbaar heeft gefunctioneerd. Dit dient minimaal jaarlijks te worden getest.	*Testcriterium 1: stel vast dat de uitgevoerde recovery test conform de recovery procedure is uitgevoerd.* *Testcriterium 2: stel vast dat er een uitwijktest conform de procedure (en/of afspraken met de klant) is uitgevoerd.* Werkzaamheden: review uitgevoerd op de door QA uitgevoerde tweedelijnscontrole. Kennisgenomen van de procedure Back-up en Recovery en het informatiebeveiligingsbeleid PGB2.0 en de daarin opgenomen bepalingen voor Back-up en restore. Kennisgenomen van de DVA met ODC-N en van de servicerapportages. Kennisgenomen van ICV ODC-N (opzet en bestaan november 2021) Bevinding: geen	Effectief