Deloitte Risk Services B.V.
Schenkkade 47
2595 AR Den Haag
Postbus 90721
2509 LS Den Haag
Nederland
www.deloitte.nl

Sociale Verzekeringsbank
T.a.v. mevrouw N.A. Vermeulen MBA
Van Heuven Goedhartlaan 1
Postbus 1100
1180 BH AMSTELVEEN

Datum	Behandeld door	Onze referentie
15-10-2014	Niek IJzinga	RS/ib/14-1520.1

Onderwerp
Rapport IT-onderzoek trekkingsrecht PGB

Geachte mevrouw Vermeulen,

In overeenstemming met onze offerte van ref RS/ib/14-1329.1 van 2 september jl. hebben we samen met de Audit Dienst van de SVB een onderzoek naar de IT-aspecten van het programma trekkingsrecht PGB binnen de SVB uitgevoerd. Hiermee is invulling gegeven aan het verzoek van het Ministerie van VWS aan de SVB om een dergelijk onderzoek uit te laten voeren.

Hierbij bieden wij u het rapport aan met de onderzoeksbevindingen. Conform onze opdracht beperkt dit rapport zich tot bevindingen uit het onderzoek. Er zijn geen conclusies of aanbevelingen in opgenomen. Het is de verantwoordelijkheid van de Raad van Bestuur van de SVB om, indien zij dit noodzakelijk acht, naar aanleiding van dit onderzoek acties uit te zetten.

Wij vertrouwen erop u door middel van dit rapport voldoende geïnformeerd te hebben over de resultaten van onze werkzaamheden ten aanzien van het onderzoek naar de IT-aspecten van trekkingsrecht PGB. Mocht u naar aanleiding van dit rapport nog vragen en/of opmerkingen hebben, neem dan s.v.p. contact op met Niek IJzinga via 06 – 535 98 623 of nijzinga@deloitte.nl.

Met vriendelijke groet,

Deloitte Risk Services B.V.

drs. R.B. Stout RE RA CISA CISSP

Deloitte.

Rapport
IT-onderzoek
trekkingsrecht PGB

Sociale Verzekeringsbank

Colophon

Deloitte Risk Services B.V.

Versie: 1.0 (definitief)

Datum: 15-10-2014

Samengesteld door:

Ir. J.N. (Niek) IJzinga, senior manager, Deloitte Risk Services

Ir. J. (Jan) Vos, senior manager, Deloitte Risk Services

Goedgekeurd door:

Drs. R. (Rob) Stout RE RA CISA CISSP, partner, Deloitte Risk Services

Ter attentie van:

Mw. N.A. Vermeulen MBA, Voorzitter Raad van Bestuur, SVB

Inhoudsopgave

1. Inleiding

1.1 Achtergrond

Met ingang van 1 januari 2015 wordt het trekkingsrecht PGB ingevoerd. Vanaf die datum verstrekken de zorgkantoren in het kader van de Wet Langdurige Zorg (WLZ) de trekkingsrechten en de gemeenten in het kader van de Wet Maatschappelijke Ondersteuning (WMO) en de Jeugdwet. Trekkingsrecht is een systematiek van budgetbeheer waarbij dit door een derde wordt uitgevoerd. De budgethouder (de zorgafnemer) blijft zelf bepalen welke zorg bij wie wordt afgenomen.

De SVB heeft de opdracht van VWS gekregen om PGB services te verlenen en een systeem van trekkingsrechten te ontwikkelen en beheren waarin trekkingsrechten PGB worden geadministreerd. Hiertoe is in 2014 binnen de SVB het programma Trekkingsrecht PGB gestart.

Het Ministerie van VWS heeft SVB verzocht een onderzoek naar drie IT-aspecten van het IT-project Trekkingsrecht PGB uit te laten voeren. De SVB heeft Deloitte Risk Services is gevraagd om in nauwe samenwerking met de Audit Dienst (AD) van de SVB op korte termijn dit IT-onderzoek uit te voeren.

1.2 Doelstelling

De doelstelling van het onderzoek is om inzicht te verschaffen in de feitelijke situatie ten aanzien van een aantal IT-gerelateerde aspecten van het IT-project Trekkingsrecht PGB van de SVB. De resultaten van het onderzoek stellen de Raad van Bestuur in de gelegenheid om aan het Ministerie van VWS te rapporteren over de mate waarin de SVB “in control” is ten aanzien van deze aspecten van het programma.

1.3 Reikwijdte

Het object van onderzoek is de IT-oplossing. Hiermee wordt bedoeld het applicatielandschap en de onderliggende IT-infrastructuur die de uitvoering van trekkingsrecht PGB door SVB mogelijk maakt. Het gaat hier om de backoffice-applicatie Nestor en de portalen MijnPGB, MijnWMO, MijnZK en MijnZKBeheer.

De volgende aspecten van de IT-oplossing zijn onderzocht:

1. *Performance*
   Bij dit aspect gaat het primair om de snelheid (response-, doorvoer- en verwerkingstijden) zoals gebruikers die ervaren. Het middelenbeslag en de capaciteit zijn slechts onderdeel van het onderzoek voor zover ze de snelheid beïnvloeden.

2. *Beveiliging*
Hierbij gaat het om de kwaliteitsattributen vertrouwelijkheid (de mate waarin de IT-oplossing waarborgt dat gegevens alleen toegankelijk zijn voor diegenen die geautoriseerd zijn), integriteit (de mate waarin de IT-oplossing aanpassing van software en gegevens verhindert) en verantwoording (de mate waarin acties van een entiteit getraceerd kunnen worden naar die specifieke entiteit). Andere kwaliteitsattributen worden slechts onderzocht voor zover ze een directe relatie hebben met de attributen vertrouwelijkheid, integriteit en verantwoording.

3. *Haalbaarheid van de datum 1 januari 2015*
Het onderzoek beperkt zich voor wat betreft de haalbaarheid tot die onderdelen die op 1 januari 2015 operationeel moeten zijn. De operationele aspecten worden buiten beschouwing gelaten; er wordt enkel naar het ICT-ontwikkel-, test- en beheerproces gekeken.

De te onderzoeken aspecten zijn nader uitgewerkt in de vorm van vragen in het “Memo IT-audit SVB TR-SVB” van het Ministerie van VWS, d.d. 31 juli 2014.

De implementatie van de nieuwe functionaliteiten in de gebruikersorganisaties (intern binnen het SVB Service centrum PGB (SSP) en extern in het publieke domein) inclusief alle voorbereidingsaspecten zoals change management, opleidingen, communicatie, zijn geen object van onderzoek. Ook vragen rond een business case, kosten en opbrengsten zijn niet aan de orde.

1.4 Vraagstelling

Elk te onderzoeken aspect (performance, beveiligbaarheid en haalbaarheid) is onderzocht aan de hand van een aantal hoofdvragen. De hoofdvragen zijn afgestemd met de AD SVB en het Ministerie van VWS. Deze hoofdvragen zijn expliciet opgenomen in het hoofdstuk bevindingen. De rapportage van de bevindingen volgt de structuur van deze hoofdvragen.

Bij de detailbevindingen worden tevens de specifieke deelvragen, zoals aangereikt door het Ministerie van VWS, geadresseerd. In appendix A is een overzicht opgenomen van detailbevindingen uit het onderzoek die betrekking hebben op deze specifieke deelvragen.

1.5 Aanpak

Het onderzoek heeft plaatsgevonden tussen 27 augustus en 30 september 2014. Het uitgevoerde onderzoek berust op documentonderzoek ondersteund door interviews. Een overzicht van de geraadpleegde documentatie is opgenomen in Appendix C . Daarnaast zijn activiteiten uitgevoerd om te observeren hoe de gekozen werkwijze ten uitvoer wordt gebracht. Waar mogelijk is gebruik gemaakt van onderzoeksresultaten van de Audit Dienst (AD) van de SVB uit eerdere onderzoeken.

Het onderzoek is uitgevoerd in samenwerking met de AD SVB. De AD heeft bijgedragen met het afnemen van interviews en andere onderzoeksactiviteiten. De interviews zijn afgenomen door tenminste twee onderzoekers (één van de AD en één van Deloitte). De lijst met geïnterviewde personen is opgenomen in Appendix B .

Deloitte is leidend geweest bij de opzet van het onderzoek en de planning en draagt de eindverantwoordelijkheid voor deze rapportage. Er zijn notities gemaakt voor het onderzoeksdossier

door SVB/Deloitte. Gezien de korte doorlooptijd zijn er geen interviewverslagen gemaakt die zijn teruggekoppeld aan de geïnterviewden. Het concept rapport met bevindingen wordt door de primaire stakeholders binnen de SVB gereviewd voordat het definitief wordt uitgebracht.

De aanpak van dit onderzoek heeft de volgende fasering gevolgd:

Fase 1: Initiatie

Tijdens deze eerste fase heeft het team zich ingewerkt in het IT-project Trekkingsrecht PGB bij de SVB (hierna te benoemen als IT-project), door middel van een startbijeenkomst, het bestuderen van documentatie en het voeren van enkele verkennende gesprekken.

Tijdens de initiatiefase zijn nadere afspraken gemaakt over de samenwerking en rolverdeling tussen de AD van de SVB en Deloitte. De beschikbare relevante documentatie is in deze fase deels geïdentificeerd en aan Deloitte ter beschikking gesteld. In deze fase is ook de vorm van het eindrapport op hoofdlijnen afgestemd tussen Deloitte en SVB.

Verder is er een gedetailleerd werkprogramma opgesteld en is een initiële lijst van te interviewen personen samengesteld. Deze lijst, evenals de lijst met documentatie, is gedurende de rest van het project voltooid.

Fase 2: Quick Scan

Het eerste deel van het onderzoek betrof het uitvoeren van een Quick Scan om de belangrijkste risico's en bevindingen ten aanzien van performance, beveiliging en haalbaarheid te identificeren. Hiertoe is het eerste deel van het werkprogramma uitgevoerd. De toetsen die in deze fase zijn uitgevoerd, zijn primair gericht geweest op het aan het licht brengen van de grootste risico's om de belangrijkste bevindingen tussentijds te kunnen rapporteren.

De werkzaamheden in deze fase bestonden met name uit het afnemen van interviews en het nader opvragen en bestuderen van documentatie, rapportages en verslagen. Ook is er nader onderzoek gedaan naar de relevante applicaties en onderliggende infrastructuur.

Fase 3: Terugkoppeling tussenresultaten

Op basis van de bevindingen uit fase 2 zijn de tussenresultaten mondeling afgestemd binnen het onderzoeksteam. Het betrof de eerste tussenresultaten van het onderzoek die in fase 4 nader zijn onderzocht. Er is hierbij vooral aandacht geschonken aan de belangrijkste bevindingen met potentieel de hoogste risico's.

De tussenresultaten zijn mondeling teruggekoppeld aan het programma- en project management van de SVB en aan de programma manager en kwaliteitsfunctionaris van het Ministerie van VWS. Het doel van deze tussentijdse terugkoppeling was om de belangrijkste bevindingen tussentijds te kunnen rapporteren. Dit maakte het mogelijk om het project te kunnen bijsturen naar aanleiding van de tussentijdse bevindingen.

Fase 4: Vervolgonderzoek

Tijdens deze fase is het werkprogramma verder verfijnd en is het tweede deel van het werkprogramma uitgevoerd. De werkwijze is gelijk aan die van het eerste deel. De belangrijkste bevindingen uit de Quick Scan zijn nader onderzocht en er is informatie verzameld om de specifieke vragen vanuit het ministerie van VWS te kunnen beantwoorden.

Fase 5: Opstellen eindrapportage

In deze fase is het eindrapport samengesteld. De conceptrapportage is binnen de SVB gereviewd op onjuistheden. Reviewcommenaar is verwerkt waarna het definitieve rapport is uitgebracht.

1.6 Gebruik van dit rapport

Wij merken op dat onze werkzaamheden geen accountantscontrole inhouden. Dit onderzoek is niet uitgevoerd in het kader van een assurance-opdracht en derhalve wordt geen zekerheid verstrekt omtrent de getrouwheid van de informatie.

Het is de verantwoordelijkheid van de (geautoriseerde) gebruikers van dit rapport van bevindingen om te beoordelen of de uitgevoerde activiteiten en de bevindingen in het rapport in het perspectief van het geheel van de hen ter beschikking staande informatie en hun risicoperceptie aan de door hen te stellen eisen voldoen. De SVB is zelf verantwoordelijk voor het trekken van conclusies en, indien dit door de SVB noodzakelijk wordt geacht, naar aanleiding hiervan vervolgacties uit te (doen) voeren.

Het onderzoek is in korte tijd uitgevoerd. Daarnaast willen wij benadrukken dat dit onderzoeksrapport slechts bedoeld is voor gebruik door de SVB en het Ministerie van VWS ten behoeve van het in de opdrachtformulering omschreven doel. Verspreiding naar overige partijen is slechts toegestaan na voorafgaande schriftelijke toestemming van Deloitte.

2. Bevindingen

2.1 Performance

De bevindingen ten aanzien van het aspect performance zijn gerubriceerd aan de hand van negen onderzoeksvragen.

2.1.1 Wat zijn de eisen ten aanzien van responsetijden, doorvoer- en verwerkingstijden voor de oplossing met betrekking tot verschillende bedrijfsfuncties die de oplossing dient te ondersteunen?

Voor responsetijden op zowel de portalen als op Nestor, geldt de enige eis dat deze niet afneemt ten opzichte van de situatie bij PGB 9. Voor verwerkingstijden van de nachtelijke batches geldt dat de performance hiervan ook niet mag afnemen en dat deze binnen het nachtelijke tijdswindow moeten blijven passen. Deze eisen zijn geformuleerd door het SSP.

De uitgangssituatie ten aanzien van performance-karakteristieken voor PGB 9 is niet vastgelegd. Er kan dus niet objectief worden vastgesteld of PGB 10 aan de eisen voldoet.

Volgens het Master testplan stijgt het aantal geprognotiseerde actieve budgethouders van 33.000 naar 168.000 en stijgt het aantal SSP-medewerkers naar verwachting van 146 naar 305. Volgens nadere opgave SVB groeit het aantal medewerkers nog door naar 350. De verwachting is dat de Nestor-database ongeveer in omvang zal vervijfvoudigen ten opzichte van de database in PGB 9.

Met de verwachte vervijfvoudiging van de omvang van de Nestor database zullen de diverse processen worden verzwaard. Het PID geeft aan dat dit mogelijk negatieve gevolgen zal gaan hebben voor de performance.

2.1.2 Uit welke componenten bestaat de oplossing (infra, systemen, applicaties) en hoe vertalen de performance eisen zich naar eisen aan deze componenten?

Het project is initieel gestart als een releasematige uitbreiding van bestaande systemen. In het voorjaar van 2014 bleken de wijzigingen zo structureel te zijn dat werd besloten tot een separaat project. Er is toen geen architect aangesteld die gedurende het hele project de totaaloplossing overziet en die de architectuurkeuzes maakt.

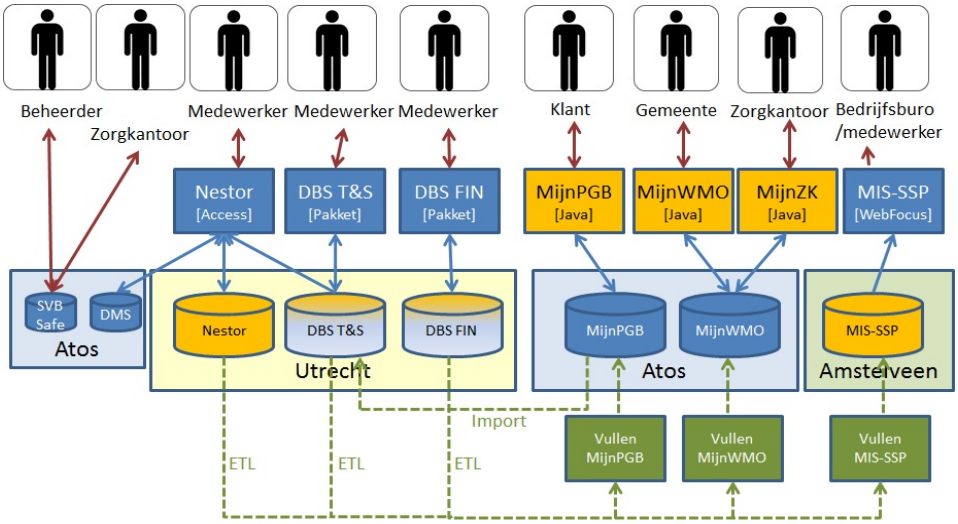
Er is een (concept) projectstartarchitectuur (PSA) opgesteld. Deze geeft echter op een hoog abstractieniveau kaders voor hoe de benodigde performance in de oplossing wordt geborgd. De PSA stelt verder dat er in de infrastructuur niets essentieels zal veranderen.

Er is een overzicht van het applicatielandschap voor PGB 10 binnen de SVB dat in meerdere documenten en presentaties wordt gehanteerd (zie Figuur 1). Dit overzicht heeft een hoog abstractieniveau en bevat de belangrijkste interfaces, maar bijvoorbeeld de interface met de belastingdienst ontbreekt. Het plaatje is niet bij alle betrokken ITB Beheer Services en Infrastructuur

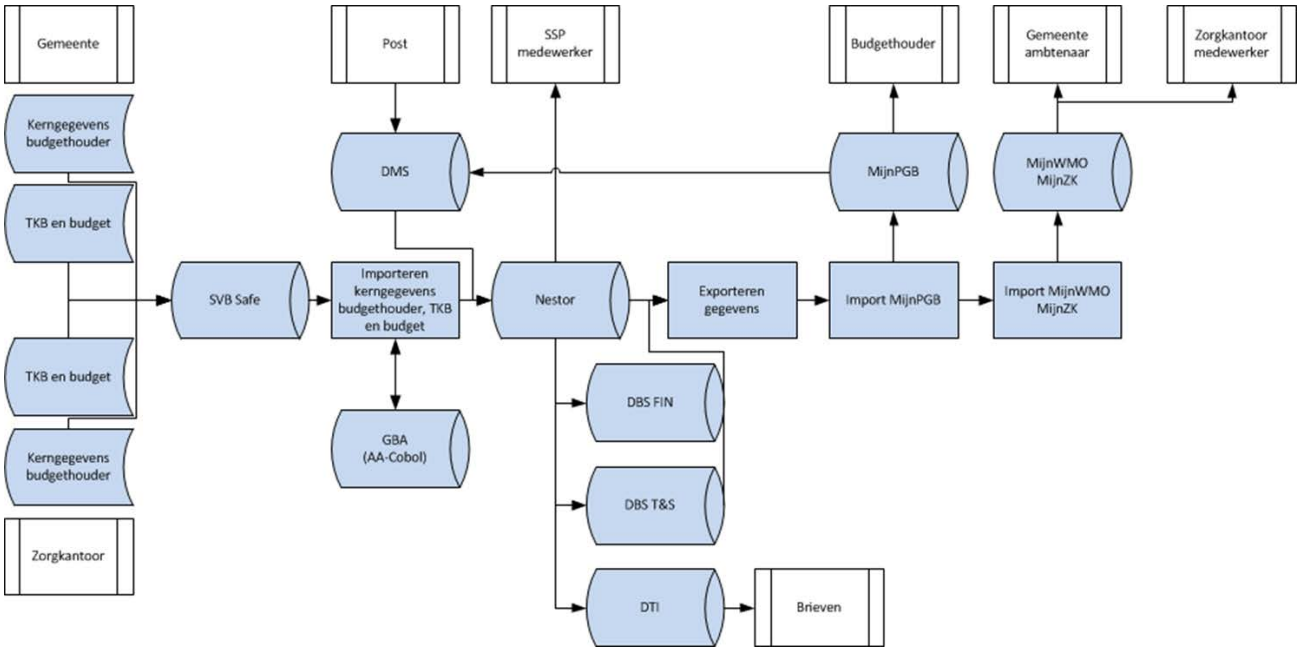
(BSI) medewerkers bekend. Figuur 2 biedt een overzicht van de informatiestromen, de betrokken databases en componenten zoals dit is opgesteld door het project.

Er is tijdens het onderzoek geen ontwerp van de technische infrastructuur van PGB 10 aangetroffen. Voor wat betreft de portalen past de technische infrastructuur wel volledig in de huidige portaalinfrastructuur benadering.

De eis dat de performance ten opzichte van PGB 9 niet mag afnemen, is niet expliciet vertaald naar individuele componenten uit Figuur 1 of Figuur 2. Voor wat betreft de performance-eisen aan de technische infrastructuur, zoals het Websphere-platform voor de portalen, wordt er door de technisch beheerders van SVB op basis van ervaring van uitgegaan dat er geen wijzigingen zullen hoeven te worden doorgevoerd. Wanneer dat toch het geval is, zal het project dat tijdig dienen aan te geven.



Figuur 1: applicatielandschap



Figuur 2: informatiestromen overzicht

2.1.3 Welke architectuurkeuzes zijn er gemaakt om ervoor te zorgen dat de oplossing aan de eisen tegemoet komt?

Er is gekozen om binnen de infrastructuur geen structurele wijzigingen aan te brengen ten opzichte van PGB 9. Dit geldt voor de portaalinfrastructuur, de databases en de netwerkinfrastructuur.

In verband met performanceproblemen zijn de Nestor servers al vóór de start van het project verhuisd van Amstelveen naar Utrecht (waar de gebruikers zitten). De bandbreedte tussen Amstelveen en Utrecht is ruim voldoende. De problemen werden volgens ITB/BSI waarschijnlijk veroorzaakt door netwerk latency waar de applicatie niet tegen kon.

Er loopt een vooronderzoek naar de doorontwikkeling van PGB waarbij de architectuur van de oplossing grondig zal worden herzien in het licht van toekomstige functionele en niet-functionele eisen (inclusief performance). De eventuele doorontwikkeling zal niet meer in 2014 starten. De doorontwikkeling van PGB viel buiten de reikwijdte van dit onderzoek.

In het project is Nestor herbouwd. Dit werd noodzakelijk geacht in verband met de onderhoudbaarheid van de applicatie en de introductie van meerwettigheid. Als gevolg van de herbouw is de performance van Nestor niet verhoogd. Dit was ook geen doel van de herbouw. Gebruikers ervaren de responstijden van Nestor-nieuw wel als sneller. Dit komt o.a. omdat schermen eerst worden neergezet voordat data wordt opgehaald. De database onder Nestor (Oracle) is met de herbouw van Nestor identiek gebleven en niet geherstructureerd. De structuur van de database is bewust niet gewijzigd, omdat dat als een te groot risico werd gezien.

2.1.4 Welke delen van de oplossing zijn bepalend t.a.v. de performance, m.a.w. waar zitten eventuele bottlenecks?

Er is geen model van de oplossing gemaakt op basis waarvan bottlenecks en performance-gedrag van de oplossing exact kan worden voorspeld. Op basis van praktische ervaring met de oplossing en monitoring door de Compuware tooling bestaat binnen het project de consensus dat:

a. De portaalapplicaties en de onderliggende infrastructuur waarschijnlijk geen performance bottlenecks zullen hebben, al mogen de performancekenmerken van MijnSVB niet zonder meer worden geëxtrapoleerd naar de andere portalen zoals MijnZK.
b. De capaciteit van benodigde interne en externe netwerkverbindingen voldoende is voor de groei in het kader van PGB 10.
c. De performance van de nieuwe Nestor applicatie nauwgezet moet worden gevolgd om indien nodig ingrepen te plegen.
d. De exportbatch vanuit de Nestor-database op dit moment nog net binnen het nachtelijke tijdswindow past, maar dat dat mogelijk binnenkort niet meer het geval is.

De performance van Nestor wordt ten tijde van dit onderzoek door het project als acceptabel ingeschat, maar er is geen zekerheid dat dit met de toename van de gegevens in de productiedatabase ook zo blijft. De performance van Nestor wordt door verschillende betrokkenen als aandachtspunt genoemd. Volgens hen zou door de groei van de data in de database het systeem traag kunnen worden. Als mogelijke verbeteringen om dit risico te beperken zijn genoemd het aanpassen van de workflow voor gebruikers van Nestor en de bijbehorende gebruikersinterfaces en het herstructureren van de database. Dit zijn beide maatregelen waarvan implementatie voor 1/1/2015 niet realistisch wordt geacht.

De duur van de nachtelijke exportbatch neemt langzaam toe met de vulling van de database en loopt op 30 september 2014 tegen de 10 uur. Als uiteindelijke oplossing hiervoor is de “verservicing” van de oplossing genoemd. Binnen SVB wordt gewerkt aan een lange termijn oplossing waarbij de architectuur van PGB wordt gewijzigd en er een realtime oplossing tot stand komt. Er wordt dan gebruikt gemaakt van services en één database voor zowel SSP- als portaal-gebruikers, het gebruik van batches zal (grotendeels) vervallen. Dit wordt echter niet voor 2015 gerealiseerd.

Over de performance van DBS-T&S, DBS-Fin zijn tijdens het onderzoek geen gegevens verzameld. In het laatste kwartaal van 2014 wordt door de leverancier van het betreffende pakket nog een nieuwe release opgeleverd. Er zijn door betrokkenen binnen de SVB geen zorgen over de performance hiervan naar voren gekomen tijdens het onderzoek.

Het Document Management Systeem (DMS) wordt voor meerdere SVB toepassingen gebruikt. Dit is een systeem dat ook door Nestor wordt aangesproken. Er heeft geen analyse plaatsgevonden of en in welke mate DMS een performanceprobleem voor PGB oplevert, maar de verwachting van de projectleiding is dat dit geen knelpunt zal opleveren.

2.1.5 Welke performance-eisen zijn er gesteld aan de IT-dienstverleners (zoals Atos)?

Atos levert infrastructuurdiensten ten bate van de oplossing. Voor een overzicht op hoog abstractieniveau wordt verwezen naar Figuur 1. Ten aanzien van de performance in productieomgevingen is vastgelegd dat Atos een “host-responsetijd” van minder dan 0,5 seconde

garandeert gedurende 98% van de tijd. Als er beschikbaarheids- of performanceproblemen zijn met de SVB-portalen, worden deze door de SVB of door Atos opgemerkt en via de Service Desk bij oplosteams belegd. Dit is in het verleden met reeds bestaande portalen ook voorgekomen. De SVB bemerkt dit dan doorgaans als eerste. De feitelijke performance van de portalen in productie is bij ITB/BSI niet bekend. Op de productieomgeving bij Atos heeft de SVB alleen toegang tot foutlogging.

Het proces voor het doorvoeren van infrastructurele wijzingen is dat de ITB/BSI aan Atos gewijzigde performance eisen voor de infrastructuurcomponenten doorgeeft. Atos vertaalt deze eisen naar concrete infrastructuurontwerpen en implementeert deze na accordering door ITB/BSI. Er is één overkoepelend contract tussen SVB en Atos. Performance monitoring op applicaties en rapportage hiervoor wordt nog niet bij Atos afgenomen. Atos heeft wel Compuware tooling geïnstalleerd en is daarmee in staat om dit te leveren.

2.1.6 Op welke manier kan de oplossing worden geschaald indien performance problemen gaan optreden?

De acceptatie- en productieomgevingen voor de portalen die op infrastructuur bij Atos draaien kunnen volgens ITB/BSI, indien noodzakelijk, op korte termijn op verzoek worden opgeschaald. Dit vindt dan plaats door het bijschakelen van processorcapaciteit en/of geheugencapaciteit.

Voor het vergroten van de performance van de Oracle-database die van belang is voor de exportbatch en de performance van Nestor, wordt het optimaliseren van database queries toegepast. De performance van deze queries kan nauwkeurig worden gevolgd met de Compuware tooling.

De PSA geeft aan dat in een zo vroeg mogelijk stadium duidelijk moet zijn dat de neergezette infrastructuur de uitbreiding van functionaliteit en de toegenomen werklast aan kan. Er is binnen het project tot op heden nog geen aanleiding gevonden om de infrastructuur op te schalen in termen van de hoeveelheid beschikbaar geheugen of processorcapaciteit.

2.1.7 Hoe wordt het aspect performance geborgd in het Agile ontwikkelproces?

Het Agile ontwikkelproces richt zich primair op het ontwikkelen van functionaliteit. Soms wordt performance in scrum meetings besproken. Indien bepaalde componenten performanceproblemen veroorzaken, wordt dit in eerste instantie door technisch beheer uitgezocht en zal als dat nodig is, de code worden geoptimaliseerd. Een voorbeeld hiervan was het ophalen van adresgegevens uit de AA-systemen wat een te lange doorlooptijd had. Door aanpassing van de code is men er in geslaagd dit aanmerkelijk te versnellen.

Systeembeheer en functioneel beheer SSP en de netwerkbeheerder gebruiken Compuware tooling om performanceproblemen te onderzoeken. De Service Desk heeft ook een dashboard. De beheerorganisatie moet er nog mee leren werken en er is (nog) geen structurele inbedding bij systeembeheer, de Service Desk en specialisten.

2.1.8 Hoe wordt de performance geëvalueerd / getest?

Het PID geeft aan dat er een plan voor performance-onderzoek klaar ligt en dat dit plan binnen het project zal worden uitgevoerd. Er is een detail testplan (DTP) performance voor het project opgesteld, dit DTP is nog niet volledig uitgewerkt.

Het Master testplan geeft aan dat performancetesten zullen worden uitgevoerd en dat grote aantallen gebruikers zullen worden gesimuleerd. Voor wat betreft de simulatie van grote aantallen gebruikers op de portalen is een dergelijke test nog niet uitgevoerd. De benodigde tooling om een dergelijke simulatie uit te voeren is ook niet voor handen. Er bestaan bij ITB/BSI echter weinig zorgen ten aanzien van de performance van de portalen, omdat er met deze infrastructuur al ruime ervaring is binnen de SVB en bij Atos. MijnSVB heeft miljoenen gebruikers terwijl dat op dezelfde infrastructuur draait.

De performance van Nestor en de onderliggende database wordt d.m.v. de Compuware tooling gemonitord. Dat geldt ook voor de doorlooptijden van de exportbatch. De export wordt in de testomgeving beproefd waarbij representatieve aantallen (budgethouders, zorgverleners en zorgovereenkomsten) worden gesimuleerd. Uitgewerkte plannen voor stress testen van Nestor zijn er niet. Het SSP is qua bemensing op 30 september 2014 praktisch op (meer dan) volle sterkte. Alleen zal de aard van de activiteiten richting 2015 nog wijzigen.

2.1.9 Hoe is geborgd dat voldoende performance-expertise in het project beschikbaar is?

Er is een tester in het project betrokken die is aangemerkt als performance tester. Deze houdt zich bezig met de performance monitoring. Hij heeft, m.u.v. performance testen gericht op batchjobs, geen feitelijke performance testen uitgevoerd zoals die zijn beschreven in het DTP Performance

De afdeling ITB/BSI levert database management expertise aan het project. Bovendien is de procesmanager capacity management betrokken bij het project in verband met de introductie van Compuware tooling.

2.2 Beveiliging

De bevindingen ten aanzien van het aspect beveiliging zijn gerubriceerd aan de hand van negen onderzoeksvragen.

2.2.1 Is er een business impact analyse voor de aspecten beschikbaarheid, integriteit en vertrouwelijkheid voor Trekkingsrecht PGB uitgevoerd onder verantwoordelijkheid van de business verantwoordelijke?

Er is voor het project geen Business Impact Analyse (BIA) uitgevoerd met betrekking tot beveiligingsaspecten. Het project bouwt echter voort op een bestaande situatie (bestaande portalen), Toen gedurende het project bleek dat er een nieuw portaal (MijnZK) moest worden gebouwd is niet alsnog een BIA uitgevoerd.

2.2.2 Is er een beveiligingsrisicoanalyse uitgevoerd?

Er is voor het project geen beveiligingsrisicoanalyse uitgevoerd om te bepalen welke maatregelen voor de beveiliging van belang zijn. Beveiligingsaspecten worden door SSP primair als een ITB aangelegenheid beschouwd.

2.2.3 Aan welke beveiligingseisen moet de oplossing voldoen en hoe hangen deze samen met wettelijke kaders / regelingen?

Er zijn geen expliciete eisen gesteld aan de beveiliging van de oplossing. In het PID zijn - behalve de toegangsbeveiliging voor toegang tot MijnZK - geen specifieke aandachtpunten ten aanzien van informatiebeveiliging aangegeven.

Vóór 2014 werd door de SVB de ISO27002 (‘Code voor Informatiebeveiliging’) standaard als uitgangspunt voor de informatiebeveiliging gehanteerd. Begin 2014 is een nieuwe CISO aangetreden om informatiebeveiliging binnen de SVB een nieuwe impuls te geven. De beveiligingsrichtlijn die de SVB in 2014 heeft geadopteerd, is de BIR. De BIR biedt echter weinig concrete handvaten voor IT-ontwikkeling en IT-beheer en is binnen de SVB nog niet uitgewerkt in nadere beleidsuitgangspunten of -richtlijnen. De SVB heeft 2016 als einddatum voor het volledig voldoen aan de BIR.

De BIR is niet verplicht voor zelfstandige bestuursorganen zoals de SVB, maar wordt door uitvoeringsinstanties wel steeds meer omarmd. De SVB heeft zich in 2014 samen met een aantal andere ketenpartners tot doel gesteld om te gaan voldoen aan de BIR. Ten aanzien van privacy is de Wet Bescherming Persoonsgegevens van toepassing. Er is in het kader van het project geen specifieke analyse uitgevoerd naar de privacy-aspecten. Het programma Trekkingsrechten van het Ministerie van VWS heeft wel een Privacy Impact Analyse (PIA) laten uitvoeren op het totale programma. Dit heeft er onder andere toe geleid dat de SVB geen zorginformatie zal gaan verwerken.

Het projectmanagement handboek van de SVB gaat onder meer in op eisen aan de op te leveren producten (acceptatiecriteria) en hoe deze dienen te worden gecontroleerd. Het gaat echter niet concreet in op beveiligingscriteria.

2.2.4 Welke beveiligingsmaatregelen (o.a. op de gebieden identificatie, authenticatie, autorisatie, monitoring & logging, systeem integriteit, data integriteit, vertrouwelijkheid van data) zijn in het ontwerp van de oplossing opgenomen?

Het ontwerp van de oplossing is primair vastgelegd door middel van “use cases”. Niet functionele aspecten, waaronder beveiligingseisen, zijn over het algemeen niet beschreven. De use cases schenken aandacht aan logische toegangsbeveiliging voor zover dit nieuw is voor de oplossing. Zo is er een ontwerp van de functionaliteit van de MijnZK-beheeroplossing die het beheer van accounts, credentials en rechten ondersteunt. Het overzicht van de containers en de productbacklog bevatten slechts sporadisch informatie over beveiligingsmaatregelen. Dit betreft dan vooral de toegangsbeveiliging. Informatie over andere beveiligingsmaatregelen zoals monitoring en logging, integriteit, data- of netwerkbeveiliging, rubricering e.d. ontbreekt.

Klanten authenticeren zich aan MijnPGB door middel van DigiD, gemeenteambtenaren via GemNet en zorgkantoormedewerkers met de oplossing die SVB zelf heeft gebouwd op basis van het eerder ontwikkelde “twinternet”-concept. Aangezien het “twinternet”-concept niet past in de SVB doelarchitectuur is dit een tijdelijke oplossing. Er was aanvankelijk voorzien om dat door middel van VeCoZo beveiliging te regelen, maar de realisatie daarvan zou waarschijnlijk te lang gaan duren. Met het raamwerk voor eHerkenning was binnen de SVB geen ervaring.

Voor SSP-applicaties hoeft niet apart ingelogd te worden. Gebruikers loggen één keer in via single sign on en krijgen daarmee ook toegang tot Nestor. AD-autorisatiegroepen worden gebruikt om de toegang tot de applicatie te beheersen. Binnen Nestor krijgen gebruikers een rol toegewezen. De rapportage IT-audits uit 2013 van de Audit Dienst geeft aan dat verbetering van het autorisatiebeheer binnen SVB wenselijk is. Dit heeft vooral betrekking op controle van toegekende rechten door de tweede lijn. Dit verbeterpunt betreft daarmee in principe ook PGB trekkingsrechten.

Op het gebied van beveiligingsmaatregelen in de infrastructuur zijn tijdens het onderzoek geen concrete beschrijvingen aangetroffen. Op de DigiD-sites van de SVB wordt bij Atos een Intrusion Detection Service (IDS) afgenomen. Dagelijks ontvangt SVB een rapportage van het internetverkeer van de dag ervoor. De rapportage uit dit systeem moet nog worden getuned op de van belang zijn risico-indicatoren. Het proces voor de afhandeling van de rapportages door de SVB is nog niet ingericht.

2.2.5 Welke processen, procedures en verantwoordelijkheden zijn gedefinieerd voor het afhandelen van beveiligingsincidenten en –calamiteiten?

Het incident management proces wordt aangestuurd door de service desk van de SVB. De verschillende oplosgroepen worden vervolgens aangesproken en indien nodig ook Atos. Bij beveiligingsincidenten verloopt dit gelijksoortig, alleen worden dan extra maatregelen getroffen die de vertrouwelijkheid van het incident borgen, zodat alleen de daartoe geautoriseerde medewerkers inzage hebben in de gemelde beveiligingsincidenten.

Bij het IT-project betrokken personeel van het SSP en van ITB weten niet of er organisatie overstijgende incident- en calamiteitenprocedures voor PGB Trekkingsrechten zijn. Deze worden door ITB/BSI wel belangrijk geacht.

2.2.6 Welke beveiligingseisen zijn er gesteld aan de IT-dienstverleners (zoals Atos)?

Atos beheert een belangrijk deel van de infrastructuur waarop de IT-oplossing draait. Bij de aanbesteding is van Atos geëist dat de bestaande IB-richtlijnen worden geïmplementeerd.

Atos deelt over het algemeen geen concrete informatie met SVB ten aanzien van hoe ze beveiliging heeft ingericht. Het verminderen van de kwetsbaarheden van IT-componenten voor cyberaanvallen wordt “hardenen” genoemd. Atos heeft richtlijnen voor het hardenen van servers. SVB heeft geen toegang tot deze richtlijnen. Atos verstrekt wel ISAE 3402 aan de SVB.

2.2.7 Hoe wordt het aspect beveiliging geborgd in het Agile ontwikkelproces?

Er zijn geen specifieke security richtlijnen voor projecten of voor systeemontwikkeling binnen de SVB. Bij de ontwikkeling van de applicaties op de portalen wordt er in de praktijk wel aandacht aan het minimaliseren van kwetsbaarheden in de code geschonken. Er zijn binnen het java-team best practices ontwikkeld ten aanzien van veilige software ontwikkeling door leerervaringen vanuit code reviews en penetratietests op een wiki te zetten gedurende de projecten. Het feit dat er als sinds lange tijd met dezelfde ontwikkelframeworks wordt ontwikkeld op de portalen reduceert het risico van niet ontdekte security kwetsbaarheden in de code van de portalen. Er wordt structureel static source code security analysis toegepast voor de applicaties op de portalen. Dit gebeurt d.m.v. de tool Fortify van HP. De bevindingen uit de tool worden allemaal geanalyseerd en indien relevant ook opgelost.

Binnen het dotNet team (Nestor) wordt geen gebruik gemaakt van static source code security analysis tooling. Het project geeft aan dat beveiliging bij de ontwikkeling en het beheer van deze interne applicatie in het algemeen minder aandacht vergt dan bij de portalen.

2.2.8 Welke beveiligingstests worden er uitgevoerd (abuse cases, vulnerability scans, penetratietests)?

Er wordt getest op functionele situaties die niet mogen voorkomen, zoals op de acceptatie van foute invoer en ongeautoriseerd inloggen. Er zijn echter geen expliciete abuse cases gedefinieerd waarop getest moet worden. De documenten op gebied van testen (productrisicoanalyse, voorbeeld regressietest, reviewprocedure) bevatten nauwelijks non-functionele aspecten zoals beveiliging of performance. De productrisicoanalyse identificeert wel voor performance belangrijke use cases.

2.2.9 Er is in 2013 een DigiD-assessment uitgevoerd op onder andere MijnPGB door een externe partij. Hier maakte ook een penetratietest deel van uit. In juni 2014 is door een externe partij ook een penetratietest uitgevoerd op MijnWMO en MijnZK. Daarbij zijn bevindingen gedaan die door SVB worden opgevolgd, bevindingen met hoge prioriteit zijn direct opgelost. Hoe is geborgd dat voldoende beveiligingsexpertise in het project beschikbaar is?

Het SSP heeft weinig kennis van informatiebeveiliging. Zij gaat er vanuit dat beveiligingseisen primair door ITB worden geformuleerd en de aansturing van dit thema ook niet bij het SSP ligt.

Er is een Security Officer binnen ITB. Hij heeft de IT-projectleider desgevraagd advies gegeven over een specifiek beveiligingsvraagstuk (toegang van zorgkantoren en MijnZK beheer). Hij is niet bezig geweest met andere security aspecten van de oplossing.

Er zijn geen senior ontwikkelaars / testers in de scrum teams zijn die zijn gespecialiseerd in beveiliging. De teams geven aan voldoende inzicht in te hebben in mogelijke kwetsbaarheden in code om hier aandacht aan te schenken en beveiligingsproblemen dit zich voordoen op te lossen.

2.3 Haalbaarheid

De bevindingen ten aanzien van het aspect haalbaarheid zijn gerubriceerd aan de hand van zeven onderzoeksvragen.

2.3.1 Wat zijn de belangrijkste factoren die de haalbaarheid per 1/1/15 van het project beïnvloeden?

Deze deelvraag brengt de belangrijkste bevindingen uit de overige onderzoeksvragen t.a.v. haalbaarheid samen.

Het gebruik van Agile/scrum als ontwikkelmethodiek levert in de huidige praktijk van het IT-project Trekkingsrecht PGB volgens het SSP een groot voordeel op in het werken met veelal nog abstracte functionele eisen die in samenwerking tussen partijen verder geconcretiseerd moeten worden. Agile werken is binnen SVB een bewuste keuze waarbij het IT-project de voortrekkersrol heeft gekregen. Het eerste Agile project binnen de SVB was PGB 9 in 2013. Er is brede steun binnen de organisatie voor deze keuze.

Het SSP heeft in juli 2014 een minimaal benodigde scope op hoofdlijnen geduid die datgene moet bevatten wat noodzakelijk is om vanaf 1/1/2015 het basisproces van facturering tot uitbetaling te kunnen doorlopen. Bij aanvang van het onderzoek ontbrak een duidelijke afbakening en concretisering van deze minimale scope. Het SSP heeft door middel van de productbacklog (PBL) versie 7 d.d. 26/09/2014 een minimale scope gedefinieerd. Alle PBL items die voor 1/1/2015 moeten zijn gerealiseerd zijn daarin gemarkeerd.

Veel tot de 'minimale' scope behorende onderwerpen zijn uitgewerkt tot ‘functional requirements’ die aan het IT-project in opdracht kunnen worden gegeven. Een aantal onderwerpen behoeft nog een nadere uitwerking.

Vanaf 26/09/2014 is het mogelijk om te sturen op de gedefinieerde minimale scope van oplevering zoals gedefinieerd in de PBL. De planning is op een hoger abstractieniveau. Deze is niet volledig gerelateerd aan de PBL.

Op basis van PBL versie 7 en recente versterkingen van het projectteam is tijdens het onderzoek de planning geactualiseerd. De nieuwe planning geeft aan dat de gevraagde en beschikbare capaciteit op macro niveau in balans is. De projectleiding stelt dat realisatie van de minimum scope de komende periode continue bewaking en sturing vereist, omdat er nauwelijks ruimte zit in de planning.

Er bestaan nog verschillen van inzicht ten aanzien van de verantwoordelijkheden van partijen zoals SVB/SSP, VWS, SZW, gemeenten en zorgkantoren en hoe deze verantwoordelijkheden in de praktijk worden ingevuld. Het SSP ziet in deze onduidelijkheden een risico voor het accepteren van de minimale scope en daardoor onjuiste verwachtingen bij ketenpartners. Het programma Trekkingsrecht werkt aan een opzet voor een structurele governance. Dit betreft aspecten zoals het tot stand komen en goedkeuren van functional requirements, de overeenstemming met externe partijen over de minimale scope voor 1/1/2015 en voorbereidingen voor de live gang zoals de ketentesten.

2.3.2 Is er een geaccordeerd en stabiel Programma van Eisen voor plateau 1 samengesteld dat de functionele en niet-functionele specificaties op hoofdlijnen definieert?

Er is geen compleet en stabiel Programma van Eisen aangetroffen tijdens het onderzoek. Het programmaplan en het Project Initiation Document (PID) gaan niet uit van een Programma van Eisen maar definiëren de scope door per plateau clusters van functionaliteiten te benoemen. Voor niet-functionele aspecten zoals performance en security zijn geen specifieke eisen benoemd.

Voordat gevraagde functionaliteiten voldoende SMART zijn gedefinieerd om door het IT-project te worden gerealiseerd is nog een proces van uitwerking nodig. Dit behoeftestellingsproces wordt uitgevoerd en wordt 'van idee naar backlog' genoemd. Ideeën worden in stappen geconcretiseerd. Deze beginnen in container 3 (idee) en eindigen in container 1 (functional requirement). In container 1 gekomen zijn ze geschikt voor verfijning en realisatie door het IT-project.

Het uitwerken van 'ideeën' vindt plaats door de SVB samen met externe stakeholders in zogenaamde ‘spinoff’ werkgroepen. Het IT-project is hiervoor niet verantwoordelijk, het project levert ad hoc ondersteuning. De spinoff werkgroepen werken onder de eindverantwoordelijkheid van de VWS stuurgroep.

Gedurende de uitwerking komen ideeën in de zogenaamde productbacklog (PBL) van het IT-project. De PBL is in de praktijk de verzameling van alle uitgewerkte en niet uitgewerkte wensen van het programma PGB trekkingsrechten. Alle items in de backlog zijn op basis van hun prioriteit gerangschikt. Deze prioriteit wordt door SSP bepaald na overleg met het IT-project PGB.

Tijdens de tweede helft van september 2014 heeft het definiëren van de minimale scope veel aandacht gekregen van SSP en het IT-project. In die periode zijn een fors aantal onderwerpen uitgewerkt en deze staan nu in container 1. Nog enkele onderwerpen staan in container 2 en behoeven nadere uitleg of besluitvorming. De ‘product owner’ heeft vervolgens namens SSP de PBL versie 7 d.d. 26/09/2014 uitgebracht, waarin alle PBL items die voor 1/1/2015 moeten zijn gerealiseerd zijn gemarkeerd. Ook de upgrade van DBS FIN behoort tot deze minimale scope. Deze upgrade moet door ITB/BSI worden uitgevoerd.

De minimale scope is hiermee voor het IT-project gedefinieerd en behoeft op een beperkt aantal onderwerpen nog nadere verdieping.

2.3.3 Wat wordt er gedaan om de op te leveren producten en diensten, met de juiste functionaliteit en kwaliteit, tijdig te realiseren?

Om deze vraag te beantwoorden wordt ingegaan op de werkwijze, de capaciteit van de realisatieteams, de productiviteit van de teams en de gebruikte documentatiestandaard. Al deze factoren hebben invloed op kwaliteit en tijdigheid.

Om producten en diensten met de juiste kwaliteit en tijdigheid te realiseren gebruikt het IT-project de Agile/scrum ontwikkelmethodiek. Deze methodiek is binnen de SVB voor het eerst toegepast bij het project PGB 9. Er wordt gewerkt met twee scrum teams die in sprints van 2 weken nieuwe functionaliteiten toevoegen aan het systeem. Volgens planning worden vervolgens één of meerdere sprints productief gemaakt in een release.

De methode is intern geëvalueerd en verbeterpunten zijn benoemd. De betrokken partijen (opdrachtgever SPP, ITB, functioneel beheerders, gebruikers en ontwikkelaars) zijn eensgezind van mening dat de methodiek bijdraagt aan kwaliteit en snelheid van ontwikkeling. Ook is de interactie tussen partijen sterk verbeterd, mede daardoor kan er beter worden omgegaan met nog niet goed uitgewerkte requirements.

De capaciteit van de scrum teams is geleidelijk uitgebreid. Het aantal beschikbare mensuren/maand is vanaf juni tot september toegenomen van ongeveer 2870 tot 3650 mensuren/maand. Grootschalige uitbreiding van de huidige scrum teams wordt door de projectleiding niet zinvol geacht omdat het de komende maanden niet meer bij zou dragen aan de realisatiekracht. Vanuit de scrum teams wordt een beroep gedaan op capaciteit van functioneel beheer voor het verduidelijken van functionele eisen. Deze capaciteit is schaars, het project ziet dit als een risico voor de realisatie. Er zijn extra medewerkers bij functioneel beheer aangetrokken maar het is niet zeker of deze al volledig zijn ingewerkt.

Vanaf begin oktober wordt alleen nog gewerkt aan het nieuwe Nestor, het oude Nestor systeem blijft wel productief tot 1/1/2015. Het team wat werkte aan het oude Nestor systeem krijgt bijscholing om met Nestor-nieuw te gaan werken, daarbij zal de samenstelling van de scrum teams worden aangepast om een betere mix aan ervaring met het nieuwe Nestor te bewerkstelligen en de productiviteit te optimaliseren. Tot begin december worden sprints uitgevoerd, daarna is dit niet meer mogelijk vanwege andere activiteiten (zoals het voorbereiden van de live gang).

De scrum teams in het IT-project zijn verantwoordelijk voor het opstellen van zogenaamde ‘use cases’, deze use cases bevatten feitelijk het functioneel ontwerp van de oplossing. Omdat toepassing van Agile/scrum meer de focus legt op het kort-cyclisch opleveren van werkende software dan op allesomvattende documentatie, vormt dit de belangrijkste documentatie die gedurende de realisatie wordt opgeleverd.

2.3.4 Wat wordt er gedaan om de op te leveren producten en diensten te testen en vervolgens door de opdrachtgevers te laten accepteren?

Het project gebruikt de testmethodiek TMap (test management approach van Sogeti). De unittest wordt gedaan door de ontwikkelaar. Dat gebeurt met behulp van een automatisch mechanisme bij het in- en uitchecken van code. De systeemtest wordt uitgevoerd door het scrum team. Deze test neemt bij de testaanpak een centrale plaats in en daarom worden concrete testspecificaties geschreven die aansluiten op de bovengenoemde ‘use cases’ en de daarin gedocumenteerde procesflow. De use cases in combinatie met de testspecificaties vormen de kern van de documentatie die een scrum team oplevert.

Het project streeft naar ‘zero defects’ bij systeemtesten en bij oplevering. Daartoe wordt sinds juni 2014 een kwaliteitsinhaalslag gemaakt op alle bestaande use cases en testspecificaties. Deze documentatie wordt ook opgeleverd aan de afdeling testmanagement van het ITB.

Nog niet alle use cases en testspecificaties zijn op het beoogde niveau, nog circa 50% behoeft aanpassingen. Zij worden aangepast als de functionaliteit wordt 'geraakt' tijdens het ontwikkelproces. Doordat testcapaciteit volgens de testcoördinator niet de meest kritieke resource is, ligt de extra effort die hieraan de komende tijd moet worden besteed niet op het kritieke pad.

Er is een productrisicoanalyse (PRA) opgesteld. Deze geeft een kwalitatieve inschatting van de functionele en de performancerisico's. De functionele risico's, de performancerisico's en beveiligingsrisico's zijn niet expliciet benoemd. Het is geen product op basis van een risicoanalyse van de gebruikersorganisatie maar een inschatting van risico's door de projectorganisatie waaraan de gebruikersorganisatie heeft bijgedragen. Afhankelijk van de PRA en ervaring van de teams wordt de diepgang van het testen bepaald.

De gebruikersacceptatietest wordt uitgevoerd door SSP onder leiding van de gemandateerde 'productowner' (functioneel beheer). Deze test is deels gebaseerd op de cases van de systeemtesten en deels gebaseerd op exploratief testen (ervaring) door de gebruikers. Op basis van deze test accepteert de productowner namens de opdrachtgever SSP de opgeleverde functionaliteit.

Het PID gaat uit van de vooronderstelling dat per 1/7/2014 een automatische regressietesttool beschikbaar is. Dat is echter op 30/9/2014 nog niet het geval. Lopende het onderzoek is wel een Proof of Concept hiervoor uitgevoerd. Het introduceren hiervan zal volgens de projectleiding waarschijnlijk geen positieve bijdrage meer leveren aan de haalbaarheid per 1/1/2015. Testen worden vooralsnog handmatig uitgevoerd, met de invoering van de regressietesttool kan op termijn wel worden bespaard op mankracht.

Binnen het project bestonden gedurende het onderzoek nog mogelijkheden om op korte termijn de testcapaciteit te vergroten. Dat is in deze periode ook gebeurd.

2.3.5 Wat wordt er gedaan om de op te leveren producten en diensten op 1/1/2015 in beheer te kunnen nemen?

De betrokken beheerders (zowel van de SVB als van Atos) zijn vanaf de ontwikkeling betrokken bij de beheeraspecten van het project (databases, infrastructuur, exploitatie). Hiermee wordt een goede overdracht tussen het project (ontwikkeling) en de beheerorganisatie ITB/BSI beoogd.

Er worden gedetailleerde draaiboeken opgesteld voor ingebruikname van nieuwe releases in de live-omgeving. In het draaiboek worden ook de activiteiten van de diverse beheerders beschreven. In de draaiboeken wordt aangesloten op bestaande formats en eerdere PGB implementaties. Wel ziet BSI een verhoogd risico in december 2014 i.v.m. de benodigde resources voor de implementatieactiviteiten en de samenloop met diverse eindejaaractiviteiten zoals jaarwerk, jaarafsluitingsbatches etc.

De bestaande Service Level Agreement (SLA) tussen het SSP en ITB benoemt verantwoordelijkheden, systemen en kosten. De SLA specificeert geen service levels en/of prestatie-indicatoren waarover gerapporteerd wordt. Alleen voor incident- en changemanagement worden prestatie-indicatoren benoemd. Het beheer is vooral gebaseerd op het beheer van afzonderlijke IT-componenten, er is geen integrale monitoring van de service levels. De huidige SLA sluit niet aan bij het systeemlandschap zoals dat vanaf 1/1/2015 moet draaien t.b.v. PGB trekkingsrechten, terwijl dit wel nodig word geacht voor de borging voor het adequaat beheren en bewaken van de vereiste service levels.

Er is één SVB breed contract met Atos waar ook de dienstverlening t.b.v. SVB/SSP is ondergebracht.

Het project bereidt de invoering van beheertooling (Compuware) voor om het SSP IT landschap te kunnen monitoren en daarmee een basis te leggen voor het meten van af te spreken servicelevels (bijvoorbeeld op de aspecten beschikbaarheid, gebruik, performance). SSP ondersteunt de introductie van deze tooling. De Compuware tooling draait nu op het interne SSP-landschap. Er is nog geen overeenkomst met ITB om dit als structureel onderdeel van het beheer te gaan toepassen. Er zijn initiële gebruikers, maar er is nog geen stevige inbedding binnen de processen en procedures van het ITB/BSI. Daarvoor zijn afspraken binnen de SLA SSP-ITB 2015 nodig.

Atos gebruikt ook de Compuware tooling waarop zou kunnen worden aangesloten om het integrale SSP landschap te monitoren. De huidige overeenkomst met Atos voorziet hier nog niet in.

2.3.6 Wat wordt er gedaan door het project om de live-gang per 1/1/2015 in de gebruikersorganisaties te ondersteunen?

De ondersteuning die vanuit het IT-project wordt geleverd om de live-gang per 1/1/2015 bij de gebruikers te ondersteunen is gericht op de gehele keten.

De release van 1/10/2014 biedt functionaliteit om stamgegevens (budgethouders, beschikkingen, zorgcontracten) te laden, deze gegevens komen veelal vanuit gemeenten en zorgkantoren. De gegevensmigratie wordt ondersteund door interfaces, veelal in combinatie met functionaliteit in het systeem zodat SSP gebruikers de gegevens kunnen nabewerken en/of controleren. Per 1/10/2014 zijn de interfaces naar ketenpartners bevroren.

Daarnaast ondersteunt het project de uitvoering van een ketentest. SVB/ITB en SVB/SSP stellen zich beiden op het standpunt dat zij ondersteunend zijn en dat het Ministerie van VWS de regie heeft over deze test. SSP stelt zich daarbij op als één van de spelers binnen het programma van VWS. Er zijn zorgen bij SSP en het IT-project over het vermogen bij de ketenpartners (zorgkantoren en gemeenten) om hun deel van de ketentest in te vullen en over de regierol van het Ministerie van VWS daarbij.

Het project heeft een rol bij het verwerken van de proefbestanden. Bestanden van zorgkantoren en gemeenten worden eerst getest voordat deze in productie worden genomen. Het projecttestteam controleert alle zorgkantoren en ongeveer 10% (de eerste 30 bestanden) van de gemeenten. Daarna worden de controles aan een reguliere team over gelaten.

Ten behoeve van communicatie met gemeenten moeten nog XML-schema definities ontwikkeld worden. Signalen en overzichten bouwt de SVB zelf, een ander deel t.b.v. toekenningsbeschikkingen wordt door Vecozo gebouwd.

Het opstellen van gebruikershandleidingen voor SSP-gebruikers en voor externe gebruikers is geen taak voor het IT-project, deze taak wordt uitgevoerd door SSP/Functioneel beheer.

2.3.7 Functioneert de projectbesturing en projectbeheersing, binnen de gebruikte combinatie van Agile/scrum en Prince 2, zodanig dat risico's effectief worden beheerst?

Om deze vraag te beantwoorden wordt ingegaan op de projectbeheersingsmethodiek en een aantal beheersingsaspecten op stuurgroepniveau. Daarnaast wordt vooral ingegaan op planning als

stuurinstrument omdat dit het belangrijkste instrument is in relatie tot de haalbaarheidsvraag. Stuurinstrumenten als business case, financiële sturing en leveranciers management vallen buiten de scope van het onderzoek.

Volgens het handboek projectmanagement SVB moet een Prince2 aanpak voor projectmanagement worden gevolgd. Tussen Prince2 en Agile/scrum bestaan aanzienlijke methodische verschillen. Prince2 is product gedreven en steunt op een heldere specificatie en scope van het op te leveren product, die per fase verder wordt aangescherpt. Bij Agile/scrum is de scope juist variabel, Agile/scrum kan wel goed om gaan met onduidelijkheden in de specificaties. Het programmaplan geeft helder aan dat deze afwijking van Prince2 is geaccepteerd en goedgekeurd.

Het programmaplan Trekkingsrechten en het PID geven niet aan hoe met deze verschillen in de praktijk wordt omgegaan. Wel is er een document beschikbaar: ‘Projecten in een gecontroleerde en wendbare omgeving”. Dit document geeft aan dat beide systematieken kunnen worden gecombineerd, maar werkt dat niet concreet uit. In het IT-project is dit verder geen vorm gegeven en is dit geen aandachtspunt van de leidinggevenden.

De Prince2 richtlijn voor sturing van een IT-project wordt vanuit het programma op een niet standaard manier ingevuld. De projectleider van het IT-project maakt geen deel uit van het projectenoverleg van het programma. De stuurgroep van het IT-project wordt in de praktijk ingevuld door een bestaand overleg: De SSP Information Board (SIB). In dit reguliere overleg spreken het SSP en ITB over IT en de afstemming tussen SSP en ITB. De benoemde leden van de stuurgroep treffen elkaar in dit overleg. De verslagen laten een operationeel gericht overleg zien. Het SIB vult daarmee de behoefte aan operationele sturing en afstemming met de andere PGB-projecten in. De meer bestuurlijke rol van een stuurgroep raakt hierdoor op de achtergrond. Er zijn bij het ITB zorgen over het stakeholder management, er is niet voorzien in onafhankelijke project assurance, er is geen expliciete haalbaarheidstoets voor het project uitgevoerd, er wordt blijkens de verslagen vanuit de stuurgroep niet gestuurd op basis van management by exception.

Prince2 vraagt om een productgerichte aanpak en een planning van deliverables (producten). In de huidige situatie stelt de projectleider een planning op in samenwerking met de vertegenwoordiger van de senior user van het SSP, de functioneel beheerders en de teamleads uit het project. Deze planning is niet op basis van de deliverables uit de PBL maar op een hoger en abstracter niveau (de zogenaamde ‘pijlenplaat’). Deze keuze is gemaakt omdat voor een deel van de functionaliteiten op de PBL uitwerkingen nog ontbreken.

Activiteiten buiten de realisatie van de PBL zijn niet in een planning vastgelegd. Dit betreft zaken zoals ondersteuning van spinoff werkgroepen, faciliteren van ketentesten en andere ad hoc ondersteuning. De projectleiding houdt echter in de berekening van beschikbare uren op macro niveau rekening met de inzet voor deze activiteiten. Een andere activiteit die niet door het IT-project zelf wordt uitgevoerd is de noodzakelijke upgrade van DBS/FIN. Deze moet worden uitgevoerd door ITB/BSI en ligt op het kritieke pad voor de livegang per 1/1/2015.

Aan het begin van het onderzoek bestond er in de planning een significant verschil tussen de ramingen van de benodigde capaciteit en de beschikbare capaciteit. Gedurende de tweede helft van september 2014 is echter veel werk verzet om de minimale scope voor 1/1/2015 scherper te definiëren en op basis daarvan de haalbaarheid van de planning beter te onderbouwen. Er is nog

geen éénduidige relatie gelegd tussen de planning en PBL-items (deliverables). Met het leggen van deze relatie kan de planning verder worden verdiept.

Volgens de projectleiding heeft op de nieuwe planning netto ‘de-scoping’ plaatsgevonden. Daarnaast bevat de nieuwe planning een aantal items die voor een deel kunnen overlopen naar 2015. Ook is rekening gehouden met enige ruimte voor herstelwerkzaamheden. De nieuwe planning gaat uit van een geactualiseerde beschikbaarheid van resources waarin de recente toevoegingen aan de teams zijn verwerkt. In de planning van 26/9/2014, zijn de beschikbare resources en de gevraagde resources nu op macro niveau in balans.

Appendix A Detailbevindingen

Performance

1. **Is of wordt er een Performance test, load- en stresstest uitgevoerd? Worden de resultaten besproken? Is de performance voldoende gebleken?**

   Er worden performance testen en loadtesten uitgevoerd in de Nestor omgeving met betrekking tot de batchjobs.

   De resultaten van deze testen worden besproken en vertaald naar verbetermaatregelen. De performance in de Nestor omgeving, op basis van een te verwachten load met een te verwachten omvang van de database, is nog niet aangetoond.

   Performance test, load en stresstesten zijn gepland voor de portalen en achterliggende processen m.b.v. Compuware tooling. Het is nog niet duidelijk hoe hier invulling aan wordt gegeven.

2. **Wordt de performancetest enkel op de structurele toepassing (na 1-1-2015) uitgevoerd of ook op het proces van initiële gegevenslevering?**

   Er zijn tijdens het onderzoek geen structurele performance testen aangetroffen voor de initiële gegevensleveringen.

3. **Zijn de performance eisen SMART beschreven en afgestemd met opdrachtgever en overige ketenpartners? (aantal concurrent users, hoeveelheid data, response tijden etc.)?**

   De performance eisen zijn niet SMART beschreven. Voor responsetijden op zowel de portalen als op Nestor geldt dat de enige eis is dat deze niet afnemen ten opzichte van de situatie bij PGB 9. Voor verwerkingstijden van de nachtelijke batches geldt dat de performance hiervan ook niet mag afnemen en dat deze binnen het nachtelijke tijdswindow moeten blijven passen.

4. **Hoe wordt omgegaan met foutafhandeling binnen zowel Nestor als de portals. Foutafhandeling kan een grote impact hebben op de performance, zoals rollbacks, foutroutines etc.**

   Bij het transporteren van software naar een volgende omgeving in de ontwikkelstraat wordt gekeken naar de foutlogging, mede omdat dit een effect kan hebben op de performance. Op basis hiervan wordt besloten of de change kan worden doorgevoerd of dat met de ontwikkelaars wordt gekeken om de oorzaak van fouten te achterhalen.

5. **Vindt er een actieve monitoring plaats om eventuele performance verliezen tijdig te signaleren?**

   We onderscheiden twee vormen van monitoring: actief en passief. Met behulp van Compuware tooling vindt passieve monitoring plaats om o.a. de performance van m.n. de Oracle database te monitoren.

Gedurende het ontwikkeltraject wordt het monitoren vooral aan geplande testen gekoppeld. Daarnaast bereidt het project de invoering van Compuware tooling voor om het SSP IT landschap continue te kunnen monitoren en daarmee een basis te leggen voor het meten van af te spreken servicelevels (zoals performance, gebruik, beschikbaarheid). SSP sponsort de introductie, de Compuware tooling draait nu op het interne SSP landschap. Er zijn nog geen afspraken met ITB om dit als structureel onderdeel van het beheer te gaan toepassen. Er zijn initiële gebruikers, maar er is geen goede inbedding binnen de processen en procedures van het ITB/BSI. Daarvoor zijn afspraken binnen de SLA SSP-ITB 2015 nodig.

6. **Wordt door Nestor gebruik gemaakt van een zogeheten 'Distributed Architecture' en zo ja op welke wijze worden de verschillende (hardware)componenten dan met elkaar geïntegreerd?**

   Er is een duidelijke scheiding tussen applicatielaag en datalaag. Bij de herbouw van Nestor wordt een strakke scheiding in lagen gevolgd (schermen, business logica, database interactie). De databases (Oracle voor Nestor en SQL voor T&S) bevinden zich nu nog op 2 machines. Op zeer korte termijn zullen deze migreren naar virtuele servers en dan op 1 machine staan. De applicatieserver is gescheiden van de databaseserver.

7. **Is de lijncapaciteit voldoende tussen de werklocatie en het computer-/datacenter; (snelheid / bandbreedte)? Zo niet, kan er bij problemen extra privileges gegeven worden aan Nestor ten opzichte van de andere applicaties?**

   Op basis van ervaringen met performanceproblemen zijn de Nestor servers al voor de start van het project verhuisd van Amstelveen naar Utrecht (waar de gebruikers zitten). De bandbreedte tussen Amstelveen en Utrecht is ruim voldoende. De problemen werden volgens ITB waarschijnlijk veroorzaakt door netwerk latency waar de applicatie niet tegen bestand was. Inmiddels werken ook gebruikers in Amstelveen middels een VDI-oplossing die wel voldoet.

8. **Zijn er andere applicaties die tijdens piekuren ook gebruik maken van dezelfde lijncapaciteit en die daardoor kunnen interfereren met het gebruik van Nestor? Zo ja, is het mogelijk om deze over andere infrastructurele componenten te laten lopen?**

   Niet van toepassing, zie vraag 7.

9. **Beschikt de applicatieserver over voldoende capaciteit?**

   Het is niet duidelijk waar de bottleneck zit die de performance van Nestor bepaalt. Dit kan zowel aan de zijde van de database als aan de applicatieve kant zitten. De applicatie wordt herbouwd vanwege meerwettigheid en onderhoudbaarheid, de herbouw is niet gericht op performance verbetering.

10. **Is er een aparte dataserver of zijn applicatieserver en dataserver geïntegreerd? Als er sprake is van een aparte dataserver is deze voldoende op de taken afgesteld (opslag en capaciteit); Wordt deze ook gebruikt voor andere applicaties / opslag?**

    De Nestor applicatieserver is gescheiden van de database server. Tussen 1 oktober 2014 en 1 januari 2015 zijn zowel Nestor-oud en Nestor-nieuw productief en maken gebruik van dezelfde database.

11. **Is de afstand tussen de werklocatie en computer-/datacenter beperkt?**

    Voor de SSP gebruikers is dat het geval, zowel de Nestor servers als de gebruikers bevinden zich op dezelfde locatie in Utrecht. Via een VDI-oplossing kan ook vanaf andere locaties worden gewerkt.

12. **Zijn er infrastructurele beperkingen, bijvoorbeeld aantal aansluitingen, netwerk, routers, die de snelheid mogelijk beperken? Indien dit het geval is, is er bij het ontwerp rekening mee gehouden?**

    Volgens het netwerkinfrastructuurteam van ITB zijn dit soort knelpunten op locatie Utrecht niet aanwezig.

13. **Staat het gebruik van Nestor toe om op te schalen met extra infrastructurele componenten? (uitbreiding netwerk bijvoorbeeld)**

    Dit wordt niet nodig geacht, zie vraag 12.

14. **Wordt het gebruik van de infrastructuur gemonitord en zijn er afspraken wanneer moet worden opgeschaald?**

    Er zijn zover bekend geen afspraken hierover gemaakt.

15. **Indien blijkt dat het maximaal aantal gebruikers die tegelijk Nestor gebruiken wordt overschreden, is het dan mogelijk om bepaalde groepen te negeren? Bijvoorbeeld de invoer van de gegevens door te laten gaan en de administratie wordt beperkt of zelfs de toegang ontzegd.**

    De gebruikers van Nestor zijn grotendeels tezamen gehuisvest op één locatie. In principe is het mogelijk hierover op de bedrijfsvloer afspraken te maken als dit nodig is. Ook over ongewenste queries die overdag draaien kunnen door overleg nadere afspraken worden gemaakt.

16. **Worden componenten ‘gelockt’ tijdens het gebruik door een gebruiker en hebben de andere gebruikers daar dan ‘last’ van.**

    Locken van records is een standaard functionaliteit van het DBMS om integriteit te bewaken. Dit kan gevolgen hebben voor gebruikers.

17. **Wordt er gebruik gemaakt van een aparte webserver voor het afhandelen van de portals? Zo ja is er per portal sprake van een ‘eigen’ webserver en is het mogelijk om meerdere webservers per portal te (gaan) gebruiken? Is er dan enkel sprake van opschalen met virtuele servers of ook met fysieke servers?**

    Ja. Atos beheert webservers die zijn gepositioneerd binnen de DMZ en die gescheiden zijn van de applicatieservers buiten de DMZ. Indien nodig kan Atos op verzoek van SVB de infrastructuur opschalen.

18. **Is de applicatieserver gescheiden van de dataserver of zijn deze geïntegreerd in één server?**

    Voor elke omgeving (test, acceptatie en productie) is er een aparte IBM PowerPC met AIX 6.1. Deze hardware wordt niet met andere klanten van Atos gedeeld. Binnen één zo'n omgeving draaien aparte LPARs met DB2 en Websphere. Binnen een Websphere instance zijn er aparte cellen (JVMs) met de verschillende applicaties (MijnSVB, Glas, MijnPGB). Aan JVMs kan minimum en maximum geheugen worden toegekend.

19. **Wordt het gebruik van de infrastructuur gemonitord en zijn er afspraken wanneer moet worden opgeschaald?**

    Atos monitort het gebruik van de portalen. De manier waarop Atos hier invulling aan geeft is binnen SVB niet bekend.

20. **Maakt Nestor gebruik van data die opgehaald moet worden uit andere applicaties / databases. Te denken valt hierbij aan bijvoorbeeld GBA. Is hier sprake van een directe (remote) aanroep of gebeurt dit op een ander wijze. Heeft dit een grote impact op de verwerkingstijd vanwege de afhankelijkheid met de andere applicatie?**

    Volgens de project startarchitectuur (PSA) maakt Nestor gebruik van de Nestor database en de DBS T&S database, daarnaast is er een koppeling met het Document Management System. Het ophalen van gegevens vindt plaats door een directe koppeling via de databases van Nestor, DBS/Talent en DBS/Fin. Daarnaast is er m.b.v. bestandsuitwisseling ook een koppeling met AA voor GBA-gegevens. Deze koppelingen hebben volgens het IT-project geen grote impact op de verwerkingstijd van Nestor.

21. **Worden tijdsintensieve handelingen die veel capaciteit vragen, slechts beperkt (of niet) toegestaan tijdens piektijden?**

    Intensieve batches worden gedurende de nachtelijke uren gedraaid. Er wordt gemonitord op het dagelijks gebruik, als gebruikers (te) tijdsintensieve queries gebruiken dan kan ITB daar op ingrijpen.

22. **Is er een procedure die zorgt dat als een gebruiker meerdere vragen aan Nestor stelt zoals het opvragen van meerdere rapporten, dat deze een lage prioriteit krijgen of zelfs worden geweigerd binnen de piekuren.**

    Nee, een dergelijke procedure is niet bekend. Zie vraag 21.

23. **Is het als gebruiker mogelijk om meerdere keren in Nestor in te loggen en als dit zo is, heeft dit dan een impact op de snelheid van Nestor?**

    Een gebruiker kan meerdere keren inloggen op Nestor. Het is bij het project onbekend of dit invloed heeft op de performance.

24. **Wordt er gebruik gemaakt van caching en is daar een onderscheid gemaakt in statische data en zeer aan verandering onderhevige data?**

    Caching wordt geregeld door standaard componenten zoals DBMS en operating systeem.

25. **Wordt de communicatie gemonitord en zijn er afspraken wanneer moet worden geëscaleerd?**

    De compuware monitor tooling maakt het mogelijk om de hele keten te monitoren (servers, netwerkcomponenten, transacties). Er zijn nog geen concrete afspraken over grenswaarden en te volgen procedures.

26. **Maken de portals gebruik van data die opgehaald moet worden uit andere applicaties / databases. Te denken valt hierbij aan bijvoorbeeld GBA. Is hier sprake van een directe (remote) aanroep of gebeurt dit op een ander wijze. Heeft dit een grote impact op de verwerkingstijd vanwege de afhankelijkheid met de andere applicatie?**

    Nee, volgens de Project Start Architectuur maken de portalen alleen gebruik van de databases MijnPGB en MijnWMO. Het vullen van deze databases gebeurd vanuit SVB middels exports uit de Nestor, DBS T&S en DBS Fin databases. Er is vanuit MijnPGB daarnaast een uitgaande informatiestroom naar DMS.

27. **De gebruiker kan via verschillende browsers het portal benaderen. Is de impact die een browser heeft op de snelheid van het portal bekend en is er reden om een of meerdere browsers te adviseren?**

    Dit wordt door SVB als een zaak voor Atos beschouwd. Zij dienen de portal zo aan te bieden dat gebruikers van verschillende browsers er gebruik van kunnen maken.

28. **Als de verwerking langer duurt dan verwacht wordt door de gebruiker, wordt er dan een melding gegeven zodat duidelijk wordt hoe lang de vertraging duurt?**

    Dergelijke meldingen zijn niet voorzien.

29. **Is het als gebruiker mogelijk om meerdere sessies van het portal tegelijk open te hebben en zo ja heeft dit dan invloed op de performance van het portal.**

    Het wordt door ITB onwaarschijnlijk geacht dat dit een impact heeft op de performance.

30. **Wordt er gebruik gemaakt van caching en is daar een onderscheid gemaakt in statische data en zeer aan verandering onderhevige data? Zijn er afspraken gemaakt hoelang de data in de cache wordt bewaard?**

    Caching wordt geregeld door standaard componenten zoals DBMS en operating systeem.

31. **Wordt de communicatie gemonitord en zijn er afspraken wanneer moet worden geëscaleerd?**

    De Compuware monitoring tooling maakt het mogelijk om de hele keten te monitoren (servers, netwerkcomponenten, transacties). Er zijn nog geen concrete afspraken over grenswaarden en te volgen procedures.

32. **Is de data dusdanig gestructureerd dat er voldoende rekening is gehouden met opvragen van data? (Omvang, veel gebruikt) Wordt gebruik gemaakt van indexen, zijn de queries geoptimaliseerd en is de database goed getuned?**

    De structuur van de database is overgenomen van PGB 9. Er heeft geen analyse van de bestaande database structuur plaatsgevonden op basis van te verwachten omvang en gebruik na 1/1/2015. Er wordt gebruik gemaakt van indexen. De performance wordt gemonitord en indien noodzakelijk worden queries geoptimaliseerd.

33. **Is het mogelijk om extra indexen toe te voegen?**

    Ja, dit wordt standaard door Oracle ondersteund. Of een extra index leidt tot verbetering van de performance zal van geval tot geval moeten worden bekeken.

34. **Wordt data 'gelockt' en indien dit zo is, heeft dit impact op de performance?**

    Ja, er wordt gebruik gemaakt van locking. Dit heeft impact op de performance, batches worden indien nodig geoptimaliseerd om de impact van locks te verkleinen.

35. **Is er sprake van complexe berekeningen cq controles in tijdskritische onderdelen? Zo ja, is de code beoordeeld op eventuele impact op de performance?**

    Nee, er is waarschijnlijk geen sprake van complexe berekeningen. De code wordt initieel niet beoordeeld op performance impact. Wel wordt uitgegaan van goed vakmanschap. Bij het monitoren wordt bepaald waar de tijdskritische processen zitten en kan op basis daarvan worden besloten om bepaalde code te optimaliseren.

36. **Wordt voor complexe queries gebruik gemaakt van stored procedures om de snelheid te bevorderen?**

    Nee, volgens de ontwikkelaars wordt er geen gebruik gemaakt van stored procedures.

37. **Zijn de queries zo lean mogelijk gemaakt. Dus geen overbodige data opvragen?**

    Bij het programmeren wordt niet geoptimaliseerd naar performance. Wel wordt uitgegaan van goed vakmanschap. Bij het monitoren wordt bepaald waar de tijdskritische processen zitten en kan op basis daarvan worden besloten om bepaalde code te optimaliseren.

38. **Zijn tijdkritische queries op performance getuned?**

    De opzet is dat m.b.v. performance monitoring de tijdkritische queries worden ontdekt. Die kunnen dan, indien nodig, verder op performance worden geoptimaliseerd.

39. **Wordt het gebruik van de data en de database gemonitord en is bekend wanneer er moet worden geëscaleerd.**

    De Compuware monitoring tooling maakt het mogelijk om de hele keten te monitoren (database, servers, netwerkcomponenten, transacties). Er zijn nog geen concrete afspraken over grenswaarden en de te volgen procedures.

40. Heeft het DBMS geautomatiseerde hulpmiddelen om de performance, geautomatiseerd of handmatig, te tunen?

Een Oracle DBMS bevat dergelijke hulpmiddelen. Er wordt gebruik gemaakt van Oracle Enterprise Manager om rapporten te draaien, in het vervolg kunnen daarop maatregelen worden getroffen.

Beveiliging

1. **Wordt door de SVB, minimaal één keer per jaar, een security assessment uitgevoerd om vast te stellen dat het security niveau gehandhaafd blijft?**

   Er vindt geen jaarlijkse evaluatie van de complete set van beveiligingsmaatregelen plaats.

   Wel voert de AD in een roulerende controlebenadering risico-gestuurd IT-audits uit, waarbij de SSP-omgeving deel uitmaakt van de audituniverse. Autorisatiemanagement is een jaarlijks terugkerende audit. Ook vindt een jaarlijkse Digid-assessment plaats.

2. **Is er een procedure voor als er een security incident plaatsvindt? Wat gebeurt er bijvoorbeeld bij een ddos aanval, of als het systeem wordt gehackt of als een medewerker fraudeert? (deze laatste is meer van procedurele aard)**

   Het incident management proces wordt aangestuurd door de service desk. De verschillende oplosgroepen worden vervolgens aangesproken en indien nodig ook Atos. Bij beveiligingsincidenten verloopt dit gelijksoortig, alleen worden dan extra maatregelen getroffen die de vertrouwelijkheid van het incident borgen, zodat alleen de daartoe geautoriseerde medewerkers inzage hebben in de gemelde beveiligingsincidenten.

3. **Is er een procedure (geautomatiseerd / handmatig) om vast te stellen of er getracht is in te breken op de systemen? Wordt er bijvoorbeeld bijgehouden of en zo ja hoe vaak er sprake is van niet succesvol inloggen?**

   Voor wat betreft toegang tot Nestor is dit centraal geregeld in het SVB Identity Management Systeem. Aanvullend wordt in de database van Nestor het volgende gelogd:
   - de aanlog aan de database (user en tijdstip);
   - fouten in de verwerking (voor analysedoeleinden);
   - foute combinatie userid/wachtwoord; na 10 mislukte pogingen wordt de user gelocked.

   De portalen zijn in beheer bij Atos. Er is een Intrusion Detection service die de portalen monitort. Hier moeten volgens ITB nog wel verbeteringen in worden aangebracht. Details van de infrastructurele beveiligingsvoorzieningen bij Atos zijn bij SVB niet bekend.

4. **Wordt op de portal(s) een penetratietest uitgevoerd om vast te stellen dat deze veilig is? Worden de portals nog op een andere wijze gecontroleerd op mogelijk beveiligingslekken? Denk hierbij onder andere aan code-inspectie.**

   Ja. De portalen zijn alle drie dit jaar onderworpen aan een penetratietest. Er wordt voor de applicatiecode op de portalen gebruik gemaakt van Static Source Code Security Analyse tooling (HP Fortify).

5. **Wordt getest of de portals beschermd zijn tegen de grootste bedreigingen voor webapplicaties die momenteel bekend zijn? Op www.owasp.org staat als voorbeeld een top 10 grootste bedreigingen van webapplicaties.**

   Door het onafhankelijk laten uitvoeren van penetratietesten en het toepassen van Static Source Code Security Analyse tooling kan er vanuit worden gegaan dat de grootste 10 bedreigingen van OWASP tijdens het testen worden ontdekt.

6. **Voldoet men aan de normen uit de NEN-ISO/IEC 27001, welke verplicht is gesteld voor de Nederlandse overheid? Zo niet, is er dan een goede onderbouwing waarom hiervan is afgeweken?**

   De BIR is door de SVB in 2014 geadopteerd. Het invoeringsproces is gaande. Voordien hanteerde de SVB de NEN-ISO/IEC 27001 als uitgangspunt voor security management.

7. **Zijn er security richtlijnen (en worden deze ook adequaat nageleefd) voor de ontwikkelaars en testers?**

   Er zijn geen specifieke security richtlijnen voor projecten of voor systeemontwikkeling binnen de SVB. Bij de ontwikkeling van de trekkingsrechten applicaties op de portalen wordt er in de praktijk wel aandacht aan het minimaliseren van kwetsbaarheden in de code geschonken.

8. **Is er voor het gebruik van de applicatie specifieke toegangscontrole? Moet er bijvoorbeeld apart worden ingelogd of wordt enkel gebruik gemaakt van Active Directory autorisaties?**

   Voor SSP-applicaties hoeft niet apart ingelogd te worden. Gebruikers loggen één keer in via single sign on en krijgen daarmee ook toegang tot Nestor als zij daar via de centrale autorisatietool de rechten voor hebben gekregen. AD-autorisatiegroepen worden gebruikt om de toegang tot de applicatie te beheersen. De users van Nestor zijn bekend in de database en moeten de juiste rollen/rechten hebben, voordat een wijziging in de data kan worden aangebracht.

9. **Zijn er verschillende rollen onderkend en worden deze ook als zodanig gehanteerd? Is er bijvoorbeeld onderscheid gemaakt in de rollen Inzien/Muteren en enkel Inzien?**

   Binnen Nestor krijgen gebruikers een rol toegewezen op basis waarvan hun rechten worden toegekend.

10. **Vindt er logging plaats, zodat achteraf vastgesteld kan worden welke medewerker gegevens heeft opgevoerd of aangepast? Zo ja, is dit voldoende om achteraf een audit trail uit te voeren?**

    Mutaties op adressen en betaaladressen van de Budgethouders en Zorgverleners worden m.b.v. databasetriggers gelogd. Sinds kort worden ook de wijzigingen in de status-accorderen van de zorgovereenkomsten gelogd. Bij de klantcontacten worden mutaties in het Vraag en Antwoord veld gelogd met een timestamp en userid.

    Voor het overige zijn wijzigingen in de T&S of DBS-data is niet traceerbaar. Deze systemen kennen een vaste user voor de benadering van de database en eigenaren van tabellen. De wachtwoorden van deze tabeleigenaren zijn niet aanpasbaar en zwak, maar ook niet bekend bij de gebruikers.

    Binnen de beschikbare rubrieken kan een audit trail gemaakt worden (dat kan buiten de applicatie of binnen de applicatie zijn geregeld)

11. **De gegevens binnen de genoemde systemen zijn vertrouwelijk van aard en zijn zeer privacygevoelig. Is er een procedure (en wordt die ook adequaat nageleefd) waarin het gebruik, opslag en vernietiging van verkregen gegevens van de ketenpartners staat beschreven. De bestanden met budgethouders die zijn gebruikt voor het aanschrijven van de budgethouders hebben een specifieke retentieperiode en moeten afgeschermd worden**

tegen onbevoegd gebruik. Dit geldt ook voor alle log-, backupbestanden en eventuele emails.

Er is een procedure voor het afvoeren van data. De data wordt bewaard in een koffer in de serverruimte. Indien nodig wordt deze data afgevoerd via Facilities door een hiervoor gespecialiseerd bedrijf. Tevens is er een shredder aanwezig waarmee cd/dvd's worden vernietigd die niet meer nodig zijn. Overige data die via batches op de servers komen zijn op de reguliere wijze op serverniveau beveiligd. Cd/dvd's die bewaard moeten blijven worden bewaard in een afsluitbare kast waar maar een beperkt aantal mensen toegang toe hebben. De standaard bewaartermijn van backups is 3 maanden. Voor Oracle databases is dat 2 weken.

Daarnaast is tijdens het onderzoek naar voren gekomen dat zich in de A-omgeving copy-databases van de productieomgeving (Nestor,T&S en DBS) bevinden waarvan de persoonsgegevens niet depersonificeerd zijn.

12. **Welk DBMS wordt gebruikt en zijn er voldoende maatregelen genomen om de database te beveiligen? Denk hierbij een encryptie, en of de database enkel benaderbaar is vanuit de applicatie en niet via het netwerk.**

    Voor Nestor wordt gebruik gemaakt van Oracle DBMS. Er wordt geen encryptie in de database toegepast. De databases zijn ook vanaf het netwerk te benaderen via SQL+ en Studio. De rol van een gewone Nestor-gebruiker is echter niet toereikend om gegevens uit de database op te halen.

13. **Worden backup bestanden op een beveiligde lokatie bewaard, zodat deze niet toegankelijk zijn voor onbevoegden?**

    Backup-bestanden worden bewaard in de serverruimte van de SVB in Amstelveen. Deze ruimte is alleen toegankelijk voor bevoegd personeel d.m.v. bijzondere autorisatie via de toegangspas. Backup bestanden worden ook nog op een externe locatie (het 2e Rekencentrum te Utrecht) bewaard. Dagelijks worden duplicaat-tapes gemaakt van de tapes in Amstelveen en deze worden naar Utrecht verzonden. Ook daar worden ze opgeslagen in een afgesloten serverruimte die alleen toegankelijk is voor bevoegd personeel door middel van pas-autorisatie.

14. **Zijn de diverse hardwarecomponenten dusdanig ingericht dat onbevoegd kopiëren van gegevens niet mogelijk is? Denk hierbij aan het niet mogelijk zijn van data kopiëren naar een usb of mail.**

    De standaardwerkstations bieden geen USB aansluiting voor dataopslag (softwarematig afgesloten). Het is echter mogelijk dat de optie wordt geboden, na aanvraag voor een rol met deze optie. De servers kennen de mogelijkheid van USB-aansluiting in het geheel niet.

    Het is mogelijk de resultaten van een raadpleegquery (als de user over een query user beschikt) via eMail te verzenden. De query-users werken onder een persoonlijk userid. Zij maken gebruik van query-opdrachten in Access, .NET en SQL. Zij worden via een aanvraag (Rfc) opgevoerd en niet via iDM/RBAC. Er is bestaat een aantal query-users. Dit kan van invloed zijn op performance en (privacy) beveiliging.

15. **Worden de computers automatisch vergrendeld (niet aan te passen door de gebruiker) als deze gedurende enige tijd niet gebruikt zijn?**

    De werkstations worden standaard na enige tijd geblokkeerd. Dit geldt ook voor VDI.

16. **Zijn er voor gebruik Nestor naast de medewerkers authenticatie ook restricties welke computers gebruik mogen worden?**

    Er zijn geen restricties vanaf welke computer Nestor gebruikt mag worden. Het is wel mogelijk dat er een bepaalde software-component op de computer geïnstalleerd moet worden voordat men met Nestor aan de slag kan. Binnen de SVB wordt dit door de gebruiker zelf geïnitieerd door middel van het SVB-softwaredistributie mechanisme.

Haalbaarheid

1. **Wordt door de SVB, gedurende het project, een haalbaarheidstoets (of meerdere) uitgevoerd om vast te stellen of de gewenste functionaliteit en hoedanigheid te realiseren valt voor 1 januari 2015?**

   Er is voorafgaand of gedurende het IT-project geen expliciete haalbaarheidstoets uitgevoerd.

2. **Is er een productrisico-analyse uitgevoerd? Zo ja, gaat deze breder dan de functionaliteitsrisico's en zijn de Non-Functionals en procesrisico's ook meegenomen?**

   Er is een productrisicoanalyse beschikbaar. Deze bevat een kwalitatieve inschatting van de grootte van functionele en performance risico's. De functionele risico's, de performancerisico's en beveiligingsrisico's zijn niet expliciet benoemd. De productrisicoanalyse is niet gebaseerd op een analyse van de risico's in de gebruikersorganisatie maar een inschatting van risico's waaraan SSP en de projectorganisatie aan hebben bijgedragen. Het is niet duidelijk wie formeel de eigenaar is.

3. **Voor het kunnen (blijven) uitvoeren van een regressietest tijdens de sprints, is geautomatiseerde ondersteuning door middel van een tool noodzaak. Is de selectie van de tool al afgerond? Is er voldoende kennis van de tool aanwezig en gaat de introductie niet (te) veel van de testcapaciteit kosten?**

   Het PID gaat uit van de vooronderstelling dat per 1/7/14 een automatische regressietesttool beschikbaar is, dit tool is echter nog niet beschikbaar. Binnen het project wordt gewerkt aan de introductie van een geautomatiseerd regressietesttool. Lopende het onderzoek wordt de Proof of Concept uitgevoerd. Om de introductie van dit tool te realiseren moeten de bestaande use cases als test cases worden ingevoerd (> 800 st). Hiervoor wordt extra testcapaciteit ingehuurd. Het introduceren ligt niet op het kritieke pad voor de livegang van 1/1/2015. Testen worden vooralsnog handmatig uitgevoerd, met de invoering van automatisch regressietesten kan in de toekomst worden bespaard op mankracht. Het onderzoeksteam heeft als voorbeeld van de uitwerking van testcases voor regressietesten het document inzake budgetbeheer ontvangen. Dit document is behoorlijk in detail uitgewerkt. Dit ondersteunt de opmerkingen uit de interviews dat aan regressietesten aandacht wordt besteed, maar dat dit tot heden wel een handmatige activiteit is.

4. **Er wordt gebruik gemaakt van een combinatie van Agile/Scrum met Prince 2. Is er voldoende ervaring met deze manier van werken binnen de SVB en zo niet, zijn er maatregelen gedefinieerd om deze aanpak los te laten cq aan te passen indien blijkt dat 1 januari 2015 in gevaar komt?**

   Alle betrokken partijen van opdrachtgever, opdrachtnemer, functioneel beheerder, gebruiker tot ontwikkelaar zijn eensgezind dat de methodiek bijdraagt aan kwaliteit en snelheid van ontwikkeling. Ook is de interactie sterk verbetert en kan er beter worden omgegaan met nog niet goed uitgewerkte requirements die verdere concretisering (tussen partijen) behoeven. Het proces in de spinoff werkgroepen en vervolgens in de scrum teams is daarop berekend. Dit in tegenstelling tot een traditionele waterval methodiek waarbij uitgewerkte SMART requirements een vereiste zijn om succesvol een IT-project te starten. Agile werken is vanuit ITB/Ontwikkeling een zeer bewuste keuze waarbij project PGB de voortrekkersrol heeft gekregen, er is steun voor deze keus gezocht en gevonden bij SVB/SSP. Het gebruik van Agile/scrum is binnen PGB 9

geëvalueerd en verbeterpunten zijn benoemd. Er zijn geen maatregelen gedefinieerd (exit strategie) waarmee deze methodiek op korte termijn kan worden losgelaten.

5. **In welke mate conformeert het project zich aan Handboek: Beschrijving Projectmethodiek Prince2 binnen de SVB V0.6 1 december 2013? Zijn de afwijkingen gespecificeerd?**

   Volgens het handboek projectmanagement SVB moet een Prince2 aanpak worden gevolgd. Prince 2 en Agile/scrum hebben belangrijke methodische verschillen. Het programmaplan geeft helder aan dat deze afwijking van Prince2 is geaccepteerd en goedgekeurd. Het programmaplan specificeert de afwijkingen niet. Wel is er een document geschreven: ‘Projecten in een gecontroleerde en wendbare omgeving.' Dit document geeft aan dat beide systematieken kunnen worden gecombineerd maar werkt dat niet concreet uit. In het project is dit verder geen vorm gegeven en het is geen aandachtspunt van leidinggevenden.

   Het handboek SVB vraagt om de invulling van een onafhankelijke project assurance rol, deze is niet aangetroffen.

   De invulling van de sturing van het IT-project vanuit het programma wordt niet volgens het handboek SVB ingevuld. De rol van de stuurgroep (project board) wordt in de praktijk gedaan door een staand overleg: Het SIB. In dit overleg spreken SSP en het IT-bedrijf over IT en de afstemming tussen SSP en IT bedrijf. De stuurgroepleden treffen elkaar in dit overleg. De verslagen laten een erg operationeel gericht overleg zien. Het SIB vult daarmee de behoefte aan een operationele sturing en alignment met de andere PGB projecten in. De meer afstandelijke stuurgroeprol (project assurance, stakeholder management) raakt hierdoor op de achtergrond.

6. **Is er een overzicht met op te leveren producten zoals documentatie? Is er een norm welke documentatie vanuit beheer gewenst is? Is de set met op te leveren documentatie voldoende voor een adequaat beheer in 2015?**

   Het IT-project is verantwoordelijk voor het functioneel ontwerp. Dit wordt in de documentatie vormgegeven door middel van het opstellen van ‘use cases‘. Deze use cases bevatten feitelijk het functioneel ontwerp met daarbij uitwerkingen voor flows, schermopzet en ontwerpbeslissingen. Daarnaast wordt testdocumentatie gemaakt. De testspecificatie is gebaseerd op de usecases en de daarin gedocumenteerde procesflow. Afhankelijk van de PRA en ervaring wordt de diepgang van het testen bepaald (de hoeveelheid mogelijke procespaden versus de te testen procespaden). In de documentatie worden de te testen overgangen aangegeven en te verwachten testresultaten gespecificeerd. Op dit niveau is er dus sprake van uitgewerkte acceptatiecriteria. Het IT-project streeft naar zero defects bij oplevering. Daarvoor wordt een kwaliteitsinhaalslag gemaakt op alle bestaande use cases en testspecificaties.

   Ten behoeve van de overdracht naar beheer worden er gedetailleerde draaiboeken voor ingebruikneming nieuwe releases in de live-omgeving opgesteld. Dit gebeurt volgens een vast template en sluit aan op eerdere implementaties van PGB 9. In het draaiboek worden ook de activiteiten van de diverse beheerders beschreven. De procescoördinator Beheer geeft aan dat de documentatie afdoende is voor beheer.

   Omdat bij toepassing van agile/scrum de focus meer ligt op het kortcyclisch opleveren van werkende software dan op allesomvattende documentatie vormt dit de belangrijkste documentatie

die gedurende de realisatie wordt opgeleverd. Er is geen expliciete norm voor op te leveren documentatie aangetroffen.

7. **Zijn de functionele requirements die per 1 januari 2015 in productie moeten zijn, voldoende (SMART) beschreven?**

   Het programmaplan benoemt hoofdfuncties en definieert clusters van te realiseren functionaliteiten. Het PID werkt dit niet verder uit. Deze eisen zijn niet SMART, voordat requirements aan het IT-project in opdracht kunnen worden gegeven is nog een heel proces van uitwerking nodig. Om eisen voldoende SMART te maken is een behoeftestellingsproces ontworpen 'van idee naar backlog'. Afgelopen 2 weken (15 - 29 sep) is veel werk verzet om het 'minimum requirement' voor 1/1/2015 scherper te definiëren. De productowner heeft met PBL versie11.7 (overhandigd 26/09/2014) een minimum requirement aangegeven. Alle PBL items die voor 1/12015 moeten zijn gerealiseerd zijn gemarkeerd. Nog niet alle gemarkeerde items zijn zodanig uitgewerkt (container 1) dat zij aan het IT project in opdracht kunnen worden gegeven.

8. **Is er een overzicht met welke activiteiten er uitgevoerd moeten worden en welke onderlinge afhankelijkheden er zijn?**

   Prince 2 vraagt een product gerichte aanpak en vertaling naar activiteiten. Door middel van de product backlog (PBL) worden de gevraagde producten (te realiseren functionaliteiten) grotendeels vastgelegd. De planning is niet gemaakt op basis van deze PBL, maar op een hoger en abstracter niveau (‘pijlenplaat’). Deze keus is gemaakt omdat voor een deel van de PBL-items de benodigde uitwerkingen nog ontbreken. Er is derhalve geen éénduidige relatie gelegd tussen de planning en PBL-items. Met het ter beschikking komen van PBL versie 11.7 (met gemarkeerde minimale scope) kan een helderder relatie worden gelegd tussen de planning en de items uit de PBL.

   Activiteiten buiten de realisatie van de productbacklog zijn niet in een planning vastgelegd. Dit betreft zaken zoals ondersteuning van spinoff werkgroepen, faciliteren van ketentesten en andere ad hoc ondersteuning.

9. **Is er een actueel projectdossier aanwezig en wordt deze ook door de projectleden gebruikt? Is het projectdossier volledig?**

   Er is een actueel projectdossier aanwezig. Opgevraagd en bestudeerd zijn zaken als projectrapportage, projectdocumentatie, stuurgroepoverleg (ingevuld door SIB), teamoverleg, riskregister en issueregister.

10. **In 2014 wordt naast de ontwikkeling van de applicatie voor 1 januari 2015 ook de gegevens omtrent budgethouders, zorgverleners en zorgcontracten ingewonnen en geregistreerd. In de praktijk zal dit betekenen dat een zwaar beroep zal worden gedaan op enkele functionarissen zoals de functioneel beheerders. Is er voldoende kennis en capaciteit beschikbaar om beide activiteiten parallel te laten verlopen?**

    De uitvoering van genoemde voorbereidingsactiviteiten bij SSP valt buiten de scope van het onderzoek. Wel is bij het onderzoek gebleken dat de capaciteit van functioneel beheer schaars is en een risico vormt voor realisatie en de nog benodigde uitwerking van functionele requirements. De komende tijd is steeds één van de twee ervaren functioneel beheerders aanwezig. Wel zijn twee extra medewerkers aangetrokken.

11. **Zijn er mogelijkheden om op te schalen naar meer ontwikkelaars en testers? Is/zijn er dan voldoende kennis/mensen beschikbaar om de extra capaciteit aan te sturen en te ondersteunen?**

    Binnen het huidige project zijn beperkt mogelijkheden aanwezig om op korte termijn (relevant voor 1/1/2015) de ontwikkelcapaciteit te vergroten. Er moet rekening worden gehouden met inleertijd voor de PGB omgevingen en scrumervaring. Grootschalige uitbreiding wordt op korte termijn niet als realistisch gezien. De capaciteit van de scrum teams is de laatste maanden nog geleidelijk uitgebreid. In raming van juli is de capaciteit ca 2870 uren/maand, in de actuele raming van september is de capaciteit ca 3650 uren/maand. In het teamoverzicht zijn 7 nieuwe resources zichtbaar.

Appendix B Geraadpleegde Personen

Conrad Huisden	projectleider
Rob van der Pouw Kraan	scrummaster, testcoördinator, QA
André Boeters	QA functionaris Programma Trekkingsrechten Ministerie van VWS
Menno Gmelig Meijling	Hoofd architectuur SVB
Evert Dekkers	programmamanager
Alfred v.d. Berg	senior user, Directeur SSP
Niek Pool	functioneel beheerder, gedelegeerd productowner
Marco van Wanrooij	sectiemanager ITB infrastructuur en beheer
Peter De Witte	security officer ITB
Bram Sonneveld	teamlead, senior ontwikkelaar
Jan Leenders	beheerder netwerkinfrastructuur
Gerard Albertsboer	beheerder webtechnologie infrastructuur
Erik Pepping	senior supplier, Hoofd Ontwikkeling IT-Bedrijf
Thijs Bazuin	functioneel beheerder, gedelegeerd productowner
Rob Henzen	teamlid, testengineer
Marc van Dijk	procescoördinator ITB/BSI/regie
Bas Auer	beheerder webapplicatieomgevingen
Robin Riemersma	scrummaster
Emiel van der Linden	dotNet consultant, senior ontwikkelaar
Nora Nijsten	procescoördinator ITB/BSI/Regie

Appendix C Geraadpleegde documentatie

1. Memo “IT-audit SVB TR-SVB”, Ministerie van VWS, d.d. 31 juli
2. Programmaplan van aanpak PGB Trekkingsrecht 2014 definitief 01072014
3. ICT deelproject PGB trekkingsrechten Project Initiatie Document PGB 10.0 V1.0
4. Project Start Architectuur PGB 10.0 v0.3
5. SVB Handboek Projectmethodiek Prince2 v06
6. Projecten in een gecontroleerde & wendbare omgeving definitief 1.0
7. Issue log ICT deelproject PGB Trekkingsrechten 10.0
8. Risk register SSP PGB 10.0
9. Verslag SIB PGB10 DEF.DOCX d.d. 22 juli 2014
10. Verslag SIB PGB10 CONCEPT.DOCX d.d. 02 september 2014
11. Verslag Bestuurlijk Overleg 9 juli trekkingsrecht concept d.d 9 juli 2014
12. R5033 End Project Report PGB 9.0 Trekkingrecht en Sepa 1.0
13. R36490 Voortgangsrapport PGB 10.0 Trekkingsrecht 07 2014
14. Overzicht onderwerpen per container d.d. 20-07-2014
15. Overzicht onderwepen per container dd 24-09-2014-2
16. Product Backlog versie 11.4 (Juli 2014)
17. Productbacklog versie 11.7 d.d. 26/09/2014
18. Planningsdocumenten:
    - Raming SSP Wensen 2014 juli 2014
    - Raming SSP Wensen 2014 eind september 2014
    - Voortgang pijlen planning / SSP mijlpalen (juli 2014)
    - Voortgang pijlen planning / SSP mijlpalen augustus 2014
    - Voortgang pijlen planning / SSP mijlpalen september 2014
    - Burndown PGB mijlpaal 1-10 Groen 23-09
    - Burndown PGB mijlpaal 1-10 paars 26-09
19. Draaiboek R38657 PGB 10.0_Nestor_1.1
20. Mastertestplan ICT deelproject PGB Trekkingsrechten v05
21. Detail Testplan Performance PGB 10.0 v05
22. Functioneel ontwerp Use Case 008 Beheren budget-v0.8
23. Product risico analyse PGB10.0
24. Regressietest TSC 008 Beheren budget v0.8
25. Evaluatiedocument Retrospective Sprint 9
26. Sprint- versus Releaseplanning (SSP) v0.4
27. Review procedure Testdocumentatie
28. Service Level Agreement SSP 2014 versie 1.2
29. Document met procesbeschrijving: Van idee naar backlog 25-5
30. Documenten van SVB Auditdienst:
    - ADU13 0112a SVB DigiD - Interne rapportage DigiD-assessment 2013 v10
    - ADU13 0112b bijlage 2 SVB DigiD-assurancerapport 2013 - v10
    - Auditdienst Basisdocument Testmanagement SVB v0.8
    - Rapportage IT audits 2013 V1.0