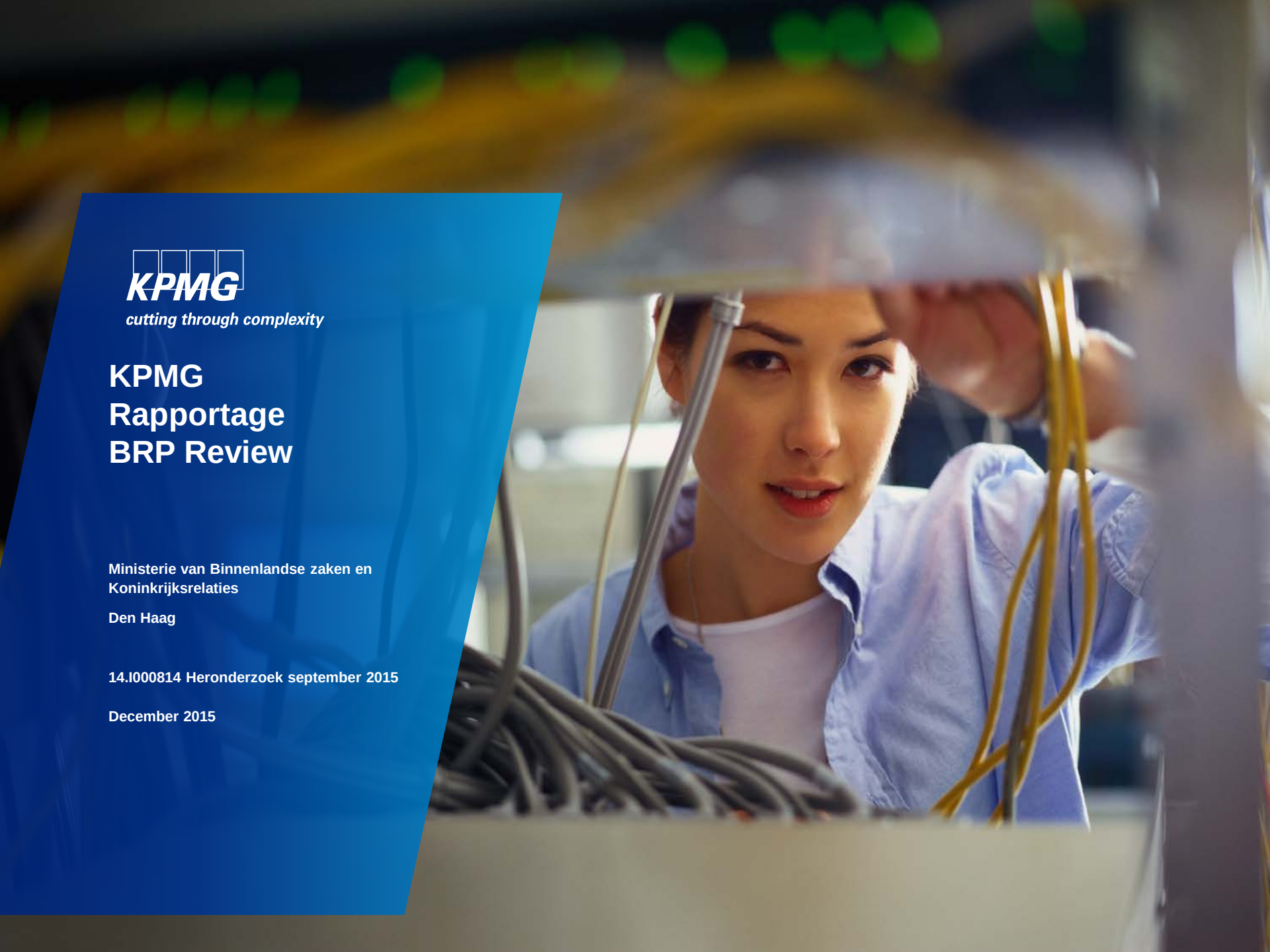

KPMG
cutting through complexity

KPMG Rapportage BRP Review

Ministerie van Binnenlandse zaken en Koninkrijksrelaties

Den Haag

14.I000814 Heronderzoek september 2015

December 2015

KPMG Advisory
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Phone +31 (0)20 656 8251
Fax +31 (0)20 656 8125

Persoonlijk en Vertrouwelijk
Gedelegeerd opdrachtgever Operatie BRP
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Operatie BRP

Amstelveen, 2 december 2015

Onderwerp: Onderzoek broncode BRP versie 19 augustus 2015

Onze referentie: 14.I000814 Heronderzoek september 2015

Geachte heer Franke,

Met deze rapportage willen wij u informeren over de resultaten van de tweede herhaling van ons onderzoek naar de kwaliteitsborging in het programma BRP (voorheen mGBA) voor zover het kwaliteit van de software betreft. Op uw verzoek heeft KPMG Advisory N.V. (hierna: KPMG) dit onderzoek uitgevoerd in overeenstemming met de uitgebrachte offerte met referentie "14.I000814 heronderzoek september 1.0" d.d. 25 augustus 2015.

Deze rapportage vormt de afsluiting van onze werkzaamheden en bevat een managementsamenvatting met de context van het onderzoek, alsmede de belangrijkste bevindingen en aanbevelingen. In het vervolg van het rapport zijn de bevindingen in detail uitgewerkt. Wij wijzen erop dat deze managementsamenvatting en factoren niet als zelfstandig stuk moeten worden gezien, doch in samenhang met het gehele rapport dienen te worden beoordeeld.

Dit rapport is bedoeld voor de operatie BRP om inzicht te krijgen in de software kwaliteitsbeheersing. Het is niet bedoeld voor andere partijen en het gebruik van dit rapport door andere partijen is dan ook voor eigen risico.

KPMG aanvaardt geen aansprakelijkheid voor het gebruik van dit rapport anders dan waarvoor het is opgesteld en aanvaardt geen aansprakelijkheid jegens andere partijen dan het ministerie van Binnenlandse zaken en Koninkrijksrelaties.

Hoogachtend,

KPMG Advisory N.V.

drs. J.M.A. (Joost) Koedijk CISA CISM
Partner

Inhoudsopgave

Uw KPMG-contactpersonen:

Joost Koedijk
Partner
KPMG Advisory N.V.
koedijk.joost@kpmg.nl

Deborah Hofland
Senior Manager
KPMG Advisory N.V.
hofland.deborah@kpmg.nl

KPMG

cutting through complexity

Management-samenvatting

Managementsamenvatting

Door KPMG is een onderzoek herhaald naar de kwaliteitsmaatregelen binnen Operatie BRP ten aanzien van de ontwikkelde software waarbij wederom kwaliteitskarakteristieken van de software op 19 augustus 2015 in kaart zijn gebracht.

Het verbeteren van de softwarekwaliteit wordt gezien als een taak die naast het ontwikkelen van functionaliteit moet worden uitgevoerd.

Uit het onderzoek komt, conform de verwachting, een met het onderzoek van maart 2015 vergelijkbaar beeld naar voren.

Inleiding

Voor u ligt de rapportage van het onderzoek naar de kwaliteitsmaatregelen binnen Operatie BRP ten behoeve van de ontwikkelde software. Doel van dit onderzoek is om, vanuit een onafhankelijke positie, invulling te geven aan een tweede herhaling van het onderzoek naar de kwaliteitsmaatregelen binnen Operatie BRP. Het programma Operatie BRP heeft in de notitie 'Normenkader codekwaliteit Centrale BRP-voorzieningen' d.d. 13 januari 2015 een zevental kwaliteitsdoelen opgesteld. In dit onderzoek is wederom in kaart gebracht in welke mate de software reeds aan deze kwaliteitsdoelen voldoet.

KPMG heeft dit onderzoek in september 2015 uitgevoerd op basis van analyse van kwaliteitsmaatregelen, broncode (versie van 19 augustus 2015), documentatiestudie en gesprekken met de ontwikkelaars. Het betreft derhalve de software die onderdeel 3.1b (mutatielevering in BRP-formaat) bevat en op 19 augustus tevens is opgeleverd voor integratietesten. Deze managementsamenvatting bevat de belangrijkste bevindingen.

Dit onderzoek heeft zich wederom geconcentreerd op de beantwoording van een viertal onderzoeksvragen en de mate waarin opvolging is gegeven aan aanbevelingen uit eerdere onderzoeken.

Algemeen beeld

Het programma Operatie BRP bouwt aan een centraal onderdeel van het Nederlandse stelsel van basisregistraties. Dat brengt met zich mee dat er hoge eisen worden gesteld aan de kwaliteit en architectuur van de software. In de voortbrengingsprocessen heeft het programma maatregelen getroffen om deze kwaliteit te borgen. Zo maakt de softwareontwikkelorganisatie gebruik van kwaliteitsdashboards zoals deze door het product SonarQube worden geleverd. Deze zijn ingericht conform gestelde kwaliteitsdoelen, wat sturing op deze doelen mogelijk maakt.

KPMG heeft de eerdere onderzoeken van september 2014 en maart 2015 herhaald om vast te stellen of de kwaliteitsmaatregelen juist zijn geïmplementeerd en of de kwaliteit van de software over de assen Onderhoudbaarheid, Betrouwbaarheid en Veiligheid voldoet om in productie te gaan.

Het is daarbij belangrijk op te merken dat het programma het verbeteren van de softwarekwaliteit ziet als een taak die naast het ontwikkelen van functionaliteit moet worden uitgevoerd. Door goede dagelijkse monitoring van de code kwaliteit beoogd men geen nieuwe problemen te introduceren. De in het verleden ontstane problemen, die de door KPMG in eerdere onderzoeken gegeven bevindingen omvatten, worden gedurende de programmalooptijd weggewerkt.

Uit het onderzoek komt, conform de verwachting. een met het onderzoek van maart 2015 vergelijkbaar beeld naar voren waarbij met betrekking tot software-kwaliteit wederom vooruitgang is geboekt.

De monitoring van de softwarekwaliteit binnen de teams functioneert en er wordt duidelijk op gestuurd dat er, met name ten opzichte van de gestelde kwaliteitsdoelen, geen nieuwe issues worden geïntroduceerd. De toename van het aantal regels code, voor met name het project BRP, leidt tot iets betere 'kwaliteitscijfers' ten opzichte van de vorige meting. Wel is er, nu er veel verschillende versies en deelwaarnemingen binnen de monitoring bestaan, aandacht nodig voor het beheer van de monitoringomgeving; deze omgeving dient zo eenvoudig en begrijpelijk mogelijk te zijn.

Voor het project BRP is de documentatie verder verbeterd, hoewel er nog enkele delen zijn die niet zijn ingevuld. Voor beide projecten is bruikbare documentatie aangetroffen omtrent de binnen de projecten uitgevoerde (opleverings)testen. Het beschikbaar zijn van testcases voor deze testen bevordert de onderhoudbaarheid van het systeem. Bij een wijziging kan overall systeemfunctionaliteit snel worden getoetst.

Volgend uit de door de ontwikkelteams gekozen graduele verbeterstrategie blijven er punten waarop de softwarekwaliteit verder kan worden verbeterd. Details zijn ook dit keer met de ontwikkelteams gedeeld. Wij adviseren op basis van de ingerichte kwaliteitsmaatregelen te blijven sturen op verbetering van de codekwaliteit en de documentatie.

Wij hebben begrepen dat het programma voornemens is deze versie van de software begin 2016 ter inzage te geven aan het publiek. Voor een volgende externe review zou het goed zijn als deze wederom vooruitloopt op een volgende openbare inzage in de broncode.

Managementsamenvatting

De monitoring van de softwarekwaliteit werkt conform verwachting. Er worden geen nieuwe problemen geïntroduceerd.

Ten op zichtte van bevindingen uit eerdere onderzoeken zijn verbeteringen van de softwarekwaliteit geïdentificeerd.

Onderzoeksvragen

Hieronder is beknopt de beantwoording van de vier onderzoeksvragen opgenomen.

1. Hoe zijn de kwaliteitsmaatregelen rond de softwareontwikkeling ingericht?

Voor de monitoring van de softwarekwaliteit wordt SonarQube gebruikt. Hierin zijn dashboards ingericht voor zowel BRP als Migratie conform de in de stuurgroep vastgelegde kwaliteitsdoelen (januari 2015) inclusief de codeerregels.

De twee aanvullende codeerregels waartoe de stuurgroep op 20 augustus 2015 heeft besloten zijn, gezien het tijdschema, begrijpelijkerwijs niet in de dashboards opgenomen. Onderzocht moet nog worden of opname mogelijk is of dat op andere wijze controle plaats moet vinden.

Het aantal markeringen is in het project Migratie afgenomen, maar blijft desondanks bij beide projecten nog erg groot. De markeringen worden daarbij niet altijd op een eenduidige wijze toegepast. Ook missen de markeringen nog regelmatig een gedocumenteerde verantwoording.

In de projecten BRP en Migratie wordt anders omgegaan met uitzonderingen op de codeerregels. Het gemixte gebruik van de twee methoden heeft beperkte impact op de in het dashboard getoonde Rule Compliance Index, welke tevens onderdeel is van de gestelde kwaliteitsdoelen (kwaliteitsdoel 7).

2. Wat is de Onderhoudbaarheid van de software?

In het BRP-project zijn zichtbare vorderingen gemaakt met betrekking tot de documentatie. Binnen enkele documenten ontbreken paragrafen of hoofdstukken die nog ingevuld dienen te worden. In de vergelijking met het project Migratie valt met name op dat er op onderwerpen verschillen van diepgang zijn waarvoor soms wel, en soms niet, een verklaring voor is te geven.

Ook is er testdocumentatie aangetroffen voor de door de projecten voor oplevering uitgevoerde testen. Met name voor het project Migratie is deze documentatie uitgebreid te noemen. Het beschikbaar zijn van testcases voor deze testen bevordert de onderhoudbaarheid van het systeem.

In de afbakening van de kwaliteitsdoelen is aangegeven dat ook gegenereerde code moet voldoen aan de kwaliteitsdoelen. Zoals bekend, uit onze softwarekwaliteitsrapportage van maart 2015, zit in de thans gegenereerde code (onveranderd) een herhaling van een afwijking ten aanzien van cyclische afhankelijkheden. Dit leidt tot een hoog aantal uitzonderingen met betrekking tot deze cyclische afhankelijkheden (kwaliteitsdoel 6) waardoor de Onderhoudbaarheid van deze gegenereerde code in beperkte mate is gewaarborgd. Wij hebben begrepen dat het programma voornemens is om voor de definitieve oplevering de generatoren te verbeteren zodat daarna opnieuw de code wordt gegenereerd die dan aan de kwaliteitsdoelen voldoet.

3. Is de software inherent betrouwbaar?

Ten aanzien van de kwaliteitsdoelen op het gebied van Veiligheid en Betrouwbaarheid (kwaliteitsdoel 2) is geconstateerd dat de onderzochte code niet geheel aan deze doelen voldoet. Afwijkingen betreffen voornamelijk de foutafhandeling en logging.

Wij hebben wederom vooruitgang geconstateerd ten aanzien van de testdekking bij beide projecten. Het kwaliteitsdoel rond testdekking (kwaliteitsdoel 3) is echter nog niet behaald. Ten behoeve van het gelijktijdig omgaan met verschillende schrijf- en leesoperaties zijn transactiemechanismen nodig om de integriteit van de gegevens te borgen. Over de afgelopen periode is geen aantoonbare vooruitgang waargenomen in de beschrijving van dit mechanisme zodat onduidelijk blijft hoe dit mechanisme na versie 3.1 dient te functioneren.

4. Is de software inherent veilig?

In het onderzoek van maart 2015 zijn zwakheden in gebruikte (externe) componenten aangetroffen. Deze zijn sindsdien deels opgepakt. Echter, nog niet alle componenten met zwakheden zijn vervangen, wat de Veiligheid niet ten goede komt. Tijdens gesprekken met de ontwikkelaars is wel aangegeven dat hierop spoedig actie genomen zal worden. Zo is vlak na de oplevering voor deze review (19 augustus 2015) gestart met de vervanging van de verouderde JBoss-versie.

Managementsamenvatting

Hoewel er voortgang is geboekt wordt niet aan alle zeven door Operatie BRP opgestelde kwaliteitsdoelen voldaan.

Wij adviseren op basis van de ingerichte kwaliteitsmaatregelen te blijven sturen op verbetering van de codekwaliteit.

Kwaliteitsdoelen

Hoewel er voortgang is geboekt ten opzichte van het eerdere onderzoek, wordt niet aan alle zeven door Operatie BRP opgestelde kwaliteitsdoelen voldaan: voor ‘blocking’ en ‘critical’ issues (kwaliteitsdoel 1), inline documentatie (kwaliteitsdoel 4) en code duplicatie (kwaliteitsdoel 5) zijn de doelen door BRP gehaald. Voor Migratie wordt aanvullend ook aan ‘issues’ ten aanzien van Veiligheid en Betrouwbaarheid (kwaliteitsdoel 2), cyclische afhankelijkheden (kwaliteitsdoel 6) en Rule Compliance Index (kwaliteitsdoel 7) voldaan.

Sinds onze vorige rapportage zijn er, door voortschrijdend inzicht en doorontwikkeling, codeerregels toegevoegd aan de standaardinstallatie van de softwarekwaliteitsbeheersing-tooling. Ook na onze verschilinventarisatie, die in augustus 2015 met het programma is gedeeld, stond de ontwikkeling van de codeerregels voor de tooling niet stil. Enkele bevindingen naar aanleiding van deze aanvullende codeerregels zijn ter illustratie (en eventueel verdere analyse) met de ontwikkelteams gedeeld. Wij hebben begrepen dat het programma voornemens is om op een later moment, als (nagenoeg) aan de gestelde kwaliteitsdoelen wordt voldaan, de verschillen tussen de kwaliteitsdoelen en de doorontwikkelde ‘de facto’ industriestandaard te beoordelen en eventueel aanvullingen in de kwaliteitsdoelen op te nemen en de software daarop aan te passen. Wij ondersteunen dat graag met een dan actuele verschilinventarisatie.

Aanbevelingen

Wij hebben de volgende aanbevelingen, welke in dit rapport in meer detail zijn uitgewerkt:

- Voer beheer uit op de omgeving voor kwaliteitsmonitoring zodat deze inzichtelijk en eenvoudig in gebruik blijft.
- Maak de ontbrekende documentatieonderdelen inzichtelijk en plan de invulling.
- Blijf werken aan het inzichtelijk maken van de uitzonderingen op de gestelde kwaliteitsdoelen.

De opdracht

De gedelegeerd opdrachtgever van Operatie BRP wil inzicht in de wijze waarop de kwaliteit van de ontwikkelde software wordt beheerst. De kwaliteitsbeheersing moet daarbij worden getoetst vanuit het perspectief van het goed en voldoende betrouwbaar in gebruik nemen van de software. Deze opdracht is een vervolg op de eerdere analyses en brengt in kaart wat de vooruitgang is in de kwaliteitsbeheersing.

Uit het onderzoek komen pragmatische verbeteradviezen om de kwaliteit en de kwaliteitsbeheersing van de software te verbeteren.

Achtergrond

Na een heroriëntatie zet het programma Operatie BRP de bouw van de Basis Registratie Personen (hierna: BRP) voort. Als aanvullende Quality Assurance (QA)-maatregel heeft het programma aan KPMG gevraagd een review uit te voeren op de kwaliteitsmaatregelen rond de softwareontwikkeling die binnen het programma plaatsvindt. Een eerste review hierop heeft rond de zomer van 2014 plaatsgevonden.

Naar aanleiding van dit eerste kwaliteitsonderzoek heeft KPMG geadviseerd enerzijds kwaliteitsdoelen voor de software op te stellen, hetgeen in een adviesbrief van KPMG nader is geformuleerd. Anderzijds is het advies periodiek een onderzoek naar de kwaliteit van de broncode te laten uitvoeren door een onafhankelijke partij.

Operatie BRP heeft in de notitie ‘Normenkader codekwaliteit Centrale BRP-voorzieningen’ d.d. 13 januari 2015 kwaliteitsdoelen geformuleerd, welke in januari 2015 door KPMG zijn gereviewd. Deze kwaliteitsdoelen zijn daarna door de stuurgroep vastgelegd. In maart 2015 heeft KPMG, in een eerste herhaling van het onderzoek naar de kwaliteitsmaatregelen, onderzocht in welke mate de software reeds aan de opgestelde kwaliteitsdoelen voldeed.

Doel van het onderzoek

Doel van het onderzoek is om, vanuit een onafhankelijke positie, invulling te geven aan een tweede herhaling van het onderzoek naar de kwaliteitsmaatregelen conform ons onderzoeksplan ‘Software en architectuur review mGBA’ van 21 maart 2014 met kenmerk 14.I000814 v2. Hierbij is wederom in kaart gebracht in welke mate de software reeds aan de opgestelde kwaliteitsdoelen voldoet.

Scope

De scope van het onderzoek beperkt zich tot de broncode, documentatie en kwaliteitsdashboards van de software zoals die door het programma Operatie BRP wordt ontwikkeld. Wanneer gerefereerd wordt aan ‘de kwaliteitsdoelen’ worden hiermee de kwaliteitsdoelen uit het document ‘Normenkader codekwaliteit Centrale BRP-voorzieningen’ d.d. 13 januari 2015 bedoeld.

Aanpak

Het onderzoek richt zicht op vier deelonderwerpen:

- Hoe zijn de kwaliteitsmaatregelen rond de softwareontwikkeling ingericht?
- Wat is de Onderhoudbaarheid van de software?
- Is de software inherent betrouwbaar?
- Is de software inherent veilig?

De toetsing van de vier deelonderwerpen heeft op dezelfde wijze plaatsgevonden als is beschreven in het genoemde onderzoeksplan dat ook aan de basis stond van de eerdere onderzoeken. In de rapportage wordt daarbij tevens in kaart gebracht in welke mate de software reeds aan de gestelde kwaliteitsdoelen voldoet.

Allereerst is in dit onderzoek een inventarisatie gemaakt van de informatie die uit dashboards, documentatie en broncode-onderzoek te verkrijgen is.

Waar mogelijk is, vanuit de onderzoeksvragen, de verkregen informatie direct vergeleken met van toepassing zijnde kwaliteitsstandaarden en ‘good practices’ uit ‘de facto’ industriestandaarden, specifieke KPMG-checklists en de ervaring van het onderzoeksteam.

Deze bevindingen, gegroepeerd naar onderzoeksvraag, zijn besproken en afgestemd in het kader van hoor en wederhoor.

Er heeft een centrale meeting plaatsgevonden om bevindingen aan te scherpen en aanbevelingen op te stellen. Hierna is, met afstemming tussen partijen, de rapportage vormgegeven.

Resultaat

Het resultaat van het onderzoek is deze geschreven rapportage. De bijlagen van deze rapportage omvatten de gedetailleerde beantwoordingen van de onderzoeksvragen, bevindingen en overzichten.

De rapportage is bedoeld de gedelegeerd opdrachtgever inzicht te geven in de kwaliteit van de software, de kwaliteitsmaatregelen rond de ontwikkeling en de mate waarin thans aan de gestelde kwaliteitsdoelen wordt voldaan. Daarnaast zijn voor het project (zo mogelijk) aanbevelingen opgenomen voor verbeteringen in de software en de kwaliteitsmaatregelen.

Aanbevelingen

1. Voer beheer uit op de omgeving voor kwaliteitsmonitoring zodat deze inzichtelijk en eenvoudig in gebruik blijft

De huidige omgeving voor kwaliteitsmonitoring kent 10 dashboards waarin gegevens met betrekking tot kwaliteitsmonitoring zijn opgenomen. Hieronder valt bijvoorbeeld het dashboard 'BRP Normenkader Oud'. Wij adviseren dashboards die niet (meer) gebruikt worden of niet meer relevant zijn te verwijderen.

Behalve de dashboards zijn er 43 projecten opgenomen in de omgeving voor kwaliteitsmonitoring. Een dashboard is opgebouwd uit meerdere projecten, dus er is reden om meerdere projecten bij te houden. Echter, de functie van veel van deze projecten is niet duidelijk, en het hoge aantal projecten maakt de herleidbaarheid van de dashboards en daarmee de gehele SonarQube-omgeving, ook voor dagelijkse gebruikers, onoverzichtelijk.

2. Maak de ontbrekende documentatieonderdelen inzichtelijk en plan de invulling

Binnen het project zijn, sinds de vorige review, zichtbare vorderingen gemaakt met betrekking tot de documentatie. Echter, er ontbreken binnen enkele documenten paragrafen of hoofdstukken die nog ingevuld dienen te worden. Wij hebben begrepen dat de aanvulling van deze ontbrekende hoofdstukken in de nabije toekomst gepland staat.

Ook is er testdocumentatie aangetroffen (voor de door de projecten uitgevoerde testen voor oplevering), die met name in het project Migratie uitgebreid is. Voor zowel Migratie als BRP zou de testdocumentatie nog verder uitgebreid kunnen worden, denk hierbij bijvoorbeeld aan het aanbrengen van een directe traceerbaarheid tussen de requirements en de testcases die eraan gekoppeld zijn. Dit maakt het eenvoudiger om aan het eind van de testfase na te gaan of alle gewenste functionaliteit in de applicatie is gerealiseerd. Daarnaast bevordert deze documentatie op lange termijn de onderhoudbaarheid van het systeem.

Ook is het raadzaam om een meer eenduidige lijn te trekken in welke vorm van documentatie er per project wordt aangeleverd; momenteel is er verschil in de omvang en diepgang van de documentatie tussen BRP en Migratie.

Dit verschil is deels te verklaren door het verschil in omvang en scope van de twee onderdelen. Zo heeft BRP haar eigen gegevensmodel en is dit voor Migratie niet van toepassing. Dit geldt in mindere mate voor documenten die door beide projecten worden geleverd zoals releasenotes.

3. Blijf werken aan het inzichtelijk maken van de uitzonderingen op de gestelde kwaliteitsdoelen

Deze aanbeveling is reeds tijdens de review van maart aangedragen, maar er is op dit gebied geen zichtbare verbetering waargenomen.

Binnen het project zijn er delen van de code waarvoor is bepaald dat deze niet aan de kwaliteitsdoelen hoeven te voldoen. Deze blokken code worden buiten de monitoring geplaatst middels markeringen in de broncode. Deze markeringen missen echter veelal een gedocumenteerde toelichting. Daarnaast is het aantal markeringen vrij hoog en wordt niet altijd gespecificeerd om welke codeerregels het gaat.

Ons advies blijft daarom op een eenduidige manier toelichting te documenteren voor deze markeringen. Ons voorstel is deze te categoriseren en in een document aan te geven waarom verschillende categorieën buiten beschouwing worden gelaten voor de kwaliteitsdoelen.
Dit verbetert het inzicht in de omvang en redenen voor het niet voldoen aan de kwaliteitsdoelen. De categorieën zouden bijvoorbeeld kunnen zijn: 'Third-party libraries', 'JBoss-code', 'Hergebruikte GBA-V-code', 'BRP-generatoren' en 'Uitgesloten voor controle op cyclische afhankelijkheid'.

Door doorontwikkeling (en voortschrijdend inzicht) van de softwarekwaliteitsbeheersing-tooling groeit het verschil tussen de vastgestelde kwaliteitsdoelen en de standaardinstallatie van de SonarQube-tooling. Het voornemen van het programma om onze eerdere aanbeveling, om op een goed moment de verschillen tussen de kwaliteitsdoelen en de doorontwikkelde 'de facto' industriestandaard te beoordelen en eventueel aanvullingen in de kwaliteitsdoelen op te nemen, uit te voeren blijft belangrijk. Voor een recent overzicht van deze verschillen verwijzen wij u door naar de brief '*Ontwikkeling codeerregels in 'de facto' standaard*' – d.d. 5 augustus 2015.