Aan: Stuurgroep Operatie BRP
Van: Cor Franke (gedelegeerd opdrachtgever)
Datum: 30 april 2015
Onderwerp: Rapportage KPMG "Herhaling onderzoek broncode" dd. 15 april 2015
Kopie aan: -

1. Inleiding

KPMG is verantwoordelijk voor de QA op de kwaliteit van de broncode. KPMG heeft de gedelegeerd opdrachtgever op 15 april een concept rapportage gestuurd naar aanleiding van de door KPMG uitgevoerde tweede toets op de broncode. De definitieve rapportage is op 30 april ontvangen.

In de rapportage doet KPMG een aantal aanbevelingen. Door middel van deze notitie adviseer ik de stuurgroep ten aanzien van de opvolging van deze aanbevelingen.

2. Algemene reactie gedelegeerd opdrachtgever

De rapportage van KPMG laat zien dat het project de aanbevelingen uit de vorige toets goed (heeft) op(ge)pakt. Het project heeft een kwaliteitsraamwerk opgesteld (normenkader codekwaliteit) dat is vastgesteld door de stuurgroep , de regels uit dat raamwerk zijn opgenomen in de controleprogrammatuur en het project volgt actief de signalen uit die programmatuur op. In de woorden van KPMG: "Uit het onderzoek blijkt dat er, mede naar aanleiding van eerdere aanbevelingen, duidelijke stappen zijn gezet om de kwaliteit van de software te waarborgen.". Verder geeft KPMG aan dat er goede progressie te zien is in de beschikbare documentatie, wat de onderhoudbaarheid van de software ten goede komt.

KPMG merkt daarnaast op dat het project niet alle kwaliteitsdoelen uit het normenkader realiseert. Het programma is zich hiervan bewust en werkt hieraan. Tenslotte hebben KPMG en het project overleg gevoerd over een formulering in het normenkader die tot onverwacht hoge bevindingen leidt. Dat overleg heeft tot een gemeenschappelijk voorstel voor aanpassing van het normenkader geleid.

Het geheel overziend trek ik de conclusie dat het project de juiste en voldoende aandacht geeft aan het aspect codekwaliteit.

3. Aanbevelingen KPMG

KPMG doet in zijn adviesbrief de volgende aanbevelingen:

a. **Aanbeveling 1: Maak uitzonderingen op de gestelde kwaliteitsdoelen inzichtelijk**

Tekst KPMG:
"*Delen van de code waarvoor is bepaald dat deze niet aan de kwaliteitsdoelen hoeven te voldoen worden buiten de monitoring geplaatst middels markeringen in de broncode. Deze markeringen missen veelal een gedocumenteerde toelichting. Daarbij is het aantal markeringen erg groot en is niet altijd gespecificeerd om welke codeerregels het gaat.*

Ons advies is op een eenduidige manier toelichting te documenteren voor de markeringen. 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'.".

Reactie gedelegeerd opdrachtgever:
Dit is een goed voorstel van KPMG, want deze werkwijze voorkomt een grote hoeveelheid uitleg in de code zelf. Voor de precieze wijze van vastlegging zal het project een nader voorstel doen (mogelijk gebeurt dit door middel van een document, maar andere oplossingen zijn ook mogelijk).

b. **Aanbeveling 2: Herformuleer de gestelde kwaliteitsdoelen en overweeg aanvullende codeerregels op te nemen in de regelset**

Tekst KPMG:
"*De formulering van de kwaliteitsdoelen zorgt voor enige verwarring. Wij adviseren deze doelen iets anders te formuleren zodat duidelijk is dat goed gemotiveerde uitzonderingen ook mogelijk zijn rond Veiligheid en Betrouwbaarheid (kwaliteitsdoel 2) en dat (alle) uitzonderingen niet meetellen in de RCI berekening (kwaliteitsdoel 7).*

De voorgestelde herformulering van de tekst op pagina 5 van de kwaliteitsdoelen luidt: "Explains" maken geen deel uit van de telling ten behoeve van de normen 1 tot en met 6. Ten aanzien van norm 7 wordt de specifieke bijdrage van de issues die de "Explains" veroorzaken in de berekening van de Rule Compliance Index in kaart gebracht, de berekening van de index wordt voor deze bijdrage gecorrigeerd door de door "Explains" veroorzaakte bevindingen niet in de telling mee te nemen.

Tevens zijn sinds de vaststelling van de kwaliteitsdoelen een aantal aanvullende codeerregels opgenomen in de "de facto" industriestandaard. Deze regels leveren aanvullende bevindingen op, ook op de aspecten Veiligheid en Betrouwbaarheid. Wij adviseren deze aanvullende regels na te lopen en zo nodig in de kwaliteitsdoelen op te nemen.".

Reactie gedelegeerd opdrachtgever:
De door KPMG voorgestelde herformulering van de kwaliteitsdoelen lost het probleem op van de onverwachte zeer hoge aantallen bevindingen rond de normen 2 en 7. De oorzaak hiervan bleek, zoals al werd vermoed, de definitie van de betreffende normen te zijn, en met name de afbakening van de code waarop de normen betrekking hebben. Ik stel voor het normenkader op dit punt aan te passen, gebruikmakend van het tekstvoorstel van KPMG.

Waar het gaat om de ontwikkelingen in de "de facto" industriestandaard is helder dat KPMG hier (in zijn rol van expert) goed zicht op heeft. Ik zal KPMG daarom vragen aan te geven welke nieuwe codeerregels voor het project relevant (kunnen) zijn. Het project zal op basis daarvan analyseren of de huidige set codeerregels aanvulling behoeft en wat de "impact" van deze aanvulling is.

c. **Aanbeveling 3: Richt een proces in voor het borgen van de veiligheid van standaard componenten**

Tekst KPMG:
" *Naar 'good practice' wordt veelal gebruik gemaakt van standaard (externe) componenten. Een groeiend aantal componenten bevatten echter zwakheden ten aanzien van de Veiligheid. Gezien deze bevinding ook terugkwam in september 2014, adviseren wij wederom een periodiek en controleerbaar proces in te richten waarin wordt onderzocht of er nieuwe zwakheden zijn ontstaan of ontdekt in de externe componenten. Hierbij kan tevens een check naar nieuwere versies worden meegenomen.*".

Reactie gedelegeerd opdrachtgever:
Deze aanbeveling is eerder door mij onderschreven. Het project heeft deze aanbeveling nog niet geïmplementeerd, maar heeft prioriteit gegeven aan de oplevering van BOP-stap 3.1a en de actualisatie van planning en begroting. Ik stel voor dat het project deze aanbeveling in de komende maanden implementeert.

d. **Aanbeveling 4: Blijf documentatie uitbreiden**

Tekst KPMG:
" *In het BRP-project is veel vooruitgang te zien in de beschikbare (technische) documentatie. Vanuit deze documenten zou nog explicieter opgenomen kunnen worden welke requirements worden vervuld met de beschreven componenten. Daarnaast is het een 'work in progress' en adviseren wij de beschikbare documentatie te blijven uitbreiden.*

Het SAD van het Migratie project had in september 2014 een aantal openstaande TODO's, deze zijn sindsdien nog niet opgepakt. Wij adviseren de documentatie te updaten naar de huidige stand van zaken.

Door RvIGzijn NFR's opgesteld naar de categorieën zoals beschreven in ISO25010. De NFR's in de categorie Beveiligbaarheid geven voornamelijk de praktische invulling voor dit onderwerp. Wij adviseren het programma de herformulering van deze doelen tot verifieerbare requirements te bespreken met RvIG. De huidige requirements kunnen dienen als de praktische invulling van de categorie Beveiligbaarheid.".

Reactie gedelegeerd opdrachtgever:
De uitbreiding van de documentatie die KPMG vaststelt is het gevolg van de opvolging van de aanbeveling van KPMG op dit punt uit de vorige toets. Het project heeft eerder al voorzien de documentatie verder uit te breiden. Daarmee vereist deze aanbeveling geen verdere aandacht. Wel zal ik het project opdracht geven bij de acties rond documentatie ook de afhandeling van de openstaande TODO's in het SAD van het Migratieproject te betrekken. Dit laatste heeft geen hoge prioriteit, in die zin dat het SAD pas op een later moment gereed hoeft te zijn. Het project zal de aanpassing van het SAD in zijn planning opnemen.

Waar het gaat om de NFR's heeft het project al eerder in de richting van de stuurgroep aangegeven de (formulering van de) NFR's met RvIG te zullen bespreken. Daarmee geeft het project naar mijn mening voldoende invulling aan de aanbeveling van KPMG.

e. **Aanbeveling 5: Maak broncode gereed voor eerste publieke inzage**

Tekst KPMG:
" *De broncode bevat in-line commentaar wat in een aantal gevallen duidt op het niet volledig afronden van een taak. Wij adviseren voor de eerste publieke inzage een kritische blik te werpen op deze (reeds met de ontwikkelteams gedeelde) commentaren en bijbehorende stukken code. Tevens adviseren wij het uitvoeren van een volgende review op de kwaliteit van de broncode tegelijk te laten plaatsvinden met de eerste inzage in de broncode zodat bekend is wat het publiek te zien krijgt.*".

Reactie gedelegeerd opdrachtgever:
De aanbeveling van KPMG met betrekking tot het "in line commentaar" voorkomt onnodige reacties van partijen die de broncode inzien. Ik zal het project O&R opdracht geven de bedoelde commentaren nog een keer op noodzaak na te lopen.

Het uitvoeren van een "review" voor het bieden van de mogelijkheid tot inzage in de broncode is een goed idee, het doel daarvan zou zijn de (eventuele) risico's in de voorliggende versie van de broncode die verband houden met de inzage in de broncode te signaleren (daarmee is de toets minder breed dan een reguliere toets die KPMG uitvoert). Dit heb ik ook al aan KPMG gecommuniceerd (zodat KPMG de benodigde capaciteit beschikbaar kan maken).

4. <u>Volgende toets</u>

In mijn algemene reactie gaf ik aan dat ik, het geheel overziend, de conclusie trek dat het project de juiste en voldoende aandacht geeft aan het aspect codekwaliteit. In het verlengde daarvan stel ik ook vast dat de kwaliteit van de code en documentatie in de afgelopen maanden aanzienlijk verbeterd is. De maatregelen die het project in dit kader genomen heeft blijven onverkort van kracht, daarom is mijn verwachting dat de kwaliteit van de broncode in de komende maanden verder zal toenemen.

In het licht hiervan is mijn voorstel om KPMG te vragen over zes maanden een volgende "review" uit te voeren.