

Aan: Stuurgroep Operatie BRP
Van: Erik Ruijs
Datum: 11 september 2014
Onderwerp: Reactie op aanbevelingen KPMG
Kopie aan: -

KPMG heeft in de afgelopen periode een toets uitgevoerd op de kwaliteit van de code die Operatie BRP ontwikkelt. KPMG heeft in zijn rapportage een aantal aanbevelingen opgenomen. In deze notitie geef ik aan op welke manier ik de aanbevelingen van KPMG zal implementeren. De aanbevelingen zullen worden opgenomen in het Register aanbevelingen QA.

1. Aanbeveling 1: Maak gebruik van de genomen kwaliteitsmaatregelen, stuur op verbetering van de codekwaliteit

Aanbeveling KPMG:

"De ontwikkelomgeving omvat met o.a. SonarQube en Jenkins, faciliteiten om de kwaliteit van de ontwikkelde code te monitoren. Door gebruik te maken van een uitgebreide set regels in SonarQube is het mogelijk om verschillende kwaliteitsaspecten van de code te monitoren. Hoewel subtiele stijlverschillen mogelijk zijn, adviseren wij om zowel BRP als migratie gebruik te maken van eenzelfde set regels. Deze set kan gebaseerd zijn op de huidige set van migratie aangevuld met de additionele squidmetriekeken. Hiermee wordt aangesloten op "goodpractices" uit de industrie. Wij adviseren om continue te sturen op verbetering van de codekwaliteit, waarbij weloverwogen keuzes worden gemaakt. Concreet kunnen hiervoor de volgende maatregelen worden genomen:

- *Stel kwaliteitsdoelstellingen op ten aanzien van de codekwaliteit en neem deze op in het Sonar dashboard. Wij zijn graag bereid binnen deze opdracht over beide systemen passende kwaliteitsdoelstellingen te adviseren.*
- *Stem de kwaliteitsdoelstellingen af met de beheerorganisatie.*
- *Monitor de codekwaliteit door middel van periodieke rapportages uit SonarQube, bijvoorbeeld aan het eind van iedere sprint.*
- *Herhaal over 3 maanden een extern softwarekwaliteitsonderzoek. Afhankelijk van de resultaten is daarna herhaling iedere 6 maanden opportuun."*

Reactie PL O & R:

Operatie BRP zal samen met KPMG de kwaliteitsdoelstellingen ("normenkader") opstellen en zal dit normenkader daarna met Agentschap BPR afstemmen.

Het project heeft de monitoring door rapportages uit SonarQube al eerder ingericht, dit vindt wekelijks plaats.

Met KPMG is afgesproken dat de volgende toets over drie maanden plaatsvindt. Als de uitkomst daarvan positief is vindt de daaropvolgende toets over zes maanden plaats. Als er nog bevindingen zijn verkorten we die termijn tot drie maanden.

2. Aanbeveling 2: Ontwikkel documentatie, voornamelijk voor BRP

Aanbeveling KPMG:

"Ten tijde van dit onderzoek bleek de beschikbare documentatie voor BRP zeer beperkt. Van de migratie is een uitgebreid architectuurdokument aanwezig. Wel ontbreken nog aspecten rondom transacties en beveiliging. Wij adviseren om te investeren in het ontwikkelen van (technische) documentatie, waarbij wij alvast aandacht willen geven aan:

- *Technische architectuur van de applicatie;*
- *Transactie-en lockingmechanismen;*
- *Web services en hieraan gerelateerde berichtdefinities, inclusief foutberichten;*
- *Documentatie met betrekking tot veiligheidsmechanismen, waaronder authenticatie en sessiemanagement."*

Reactie PL O & R:

Het project zal de hier bedoelde documentatie opleveren. De daarmee gemoeide inspanningen zijn in kaart gebracht en zijn opgenomen in de voortgangsrapportage.

3. Aanbeveling 3: Verbeter de codekwaliteit BRP datamodel

Tekst KPMG:

"Het datamodel is gegenereerd met behulp van zelfgeschreven generatoren. Het uitgangspunt ten tijde van dit onderzoek is dat de generatoren niet worden opgeleverd en dat daarmee wijzigingen na oplevering handmatig in de code gemaakt moeten worden.

Dit betekent dat de onderhoudbaarheid van de gegenereerde code voldoende moet zijn. Gezien de hoeveelheid bevindingen rondom complexiteit, code duplicatie en cyclische afhankelijkheden adviseren wij om de codekwaliteit van de gegenereerde code te verbeteren zodat deze gaat voldoen aan de kwaliteitsdoelstellingen.

Indien er alsnog besloten wordt om de generatoren op te leveren, dient er:

- *Aanvullend onderzoek gedaan te worden naar de codekwaliteit van de generatoren, waarbij ook strenge eisen ten aanzien van onderhoudbaarheid moeten gelden;*
- *Duidelijk onderscheid gemaakt te worden tussen gegenereerde code en code die aan te passen is door de ontwikkelaar."*

Reactie PL O & R:

Het project zal een afweging maken tussen aanpassing van de generatoren (zodat die code voor het data model opleveren die aan de eisen uit het normenkader voldoet) en handmatige aanpassing van de code voor het data model. De uitkomst daarvan zal het project vastleggen in de volgende voortgangsrapportage.

Als het project besluit de generatoren aan te passen zal overleg plaatsvinden met Agentschap BPR over de wenselijkheid de generatoren over te dragen aan beheer. Als dat niet wenselijk is zal het project alleen de code van het data model overdragen. In beide gevallen voldoet de code aan het voornoemde normenkader.

4. Aanbeveling 4: Werk het transactie- en locking model verder uit en implementeer en test dit

Tekst KPMG:

"Een robuust transactie- en lockingmechanisme is noodzakelijk om onder andere in geval van gelijktijdige schrijf en leesoperaties en foutsituaties de integriteit van gegevens te borgen.

- *Werk het voorgestelde transactiemechanisme verder uit op basis van de functionele en niet-functionele eisen, waarbij de integriteit van gegevens geborgd kan worden.*
- *Implementeer, documenteer en test dit mechanisme uitvoerig."*

Reactie PL O & R:

Het, voor de huidige fase adequate locking- en transactiemechanisme, wordt als onderdeel van de normale ontwikkeling van de software verder doorontwikkeld. Het documenteren en testen maakt daar onderdeel van uit.