Acceptatieprocedure bij agentschap BPR bewijst zich in de praktijk

Risicobeheersing bij nieuwe functionaliteit

Het in productie nemen van nieuwe of gewijzigde informatiesystemen door beheerorganisaties vereist een goede risicoanalyse en risicobeheersing. Als daarvan geen sprake is, kan het gevolg zijn dat informatiesystemen niet aan de functionele eisen, kwaliteitseisen en beheereisen voldoen. Het agentschap BPR (Basisadministratie Persoonsgegevens en Reisdocumenten) heeft een acceptatieprocedure opgesteld die invulling geeft aan het analyseren en beheersen van deze risico's. BPR heeft deze procedure inmiddels met succes toegepast.

Bart de Best

Veel beheerorganisaties hanteren nauwelijks of geen acceptatiecriteria om nieuwe of gewijzigde informatiesystemen te accepteren. Als er al acceptatiecriteria zijn, dan zijn die zo generiek dat er geen risicobeheersing van uitgaat. Aan de andere kant zijn er ook organisaties die wel acceptatiecriteria gebruiken in het Change Managementproces. Dit zijn er echter meer dan eens zoveel dat er geen tijd in projecten vrijgemaakt kan worden om ze toe te passen.

De crux is dan ook om alleen die acceptatiecriteria te hanteren die gebaseerd zijn op een risicoanalyse, waarbij de faalfactoren van functionaliteit, kwaliteit en beheerbaarheid duidelijk worden. De acceptatiecriteria moeten worden gehanteerd als meetinstrument om vast te stellen of de risico's beheerst zijn. Op basis daarvan kan Change Management wel of niet het groene licht geven voor het in productie nemen van de nieuwe of gewijzigde functionaliteit. Het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) heeft invulling gegeven aan zo'n risicoanalyse in de vorm van een acceptatieprocedure.

Achtergrond

BPR hecht veel waarde aan het beheersen van de risico's van nieuwe of gewijzigde informatiesystemen. Het agentschap is er namelijk verantwoordelijk voor te schouwen en toetsen of de in beheer zijnde informatiesystemen voldoen aan de gerelateerde wetgeving. Daarnaast zijn de informatiesystemen van groot maatschappelijk belang, omdat veel overheidsinstanties afhankelijk zijn van de beschikbaarheid en betrouwbaarheid van de informatievoorziening door BPR.
Verstoringen aan applicaties, zoals de BV BSN en GBA-V (zie kader 'BPR-organisatie'), of erger nog, corruptie van de gegevensbanken waarvan het berichtenverkeer gebruikmaakt, heeft dan ook een directe impact op vele overheidsprocessen. Als acceptant van de nieuwe of aangepaste informatiesystemen hanteert BPR dan ook een stringente acceptatieprocedure, waarbij invulling wordt gegeven aan het beheersen van de risico's qua functionaliteit, kwaliteit en beheerbaarheid.

Acceptatieprocedure

De acceptatie van nieuwe of gewijzigde informatiesystemen geschiedt volgens het zogenaamde GSA-stappenplan, zoals afgebeeld in figuur 1. *GSA* staat voor 'Generieke en Specifieke Acceptatiecriteria'. Het GSA-stappenplan is erop gericht om acceptatiecriteria

BPR-organisatie

BPR (Basisadministratie Persoonsgegevens en Reisdocumenten) is een agentschap van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Het agentschap is eindverantwoordelijk voor de jaarlijkse uitwisseling van ongeveer zestig miljoen berichten met algemene persoonsgegevens en de productie en distributie van jaarlijks 1,2 miljoen paspoorten en 900.000 Europese identiteitskaarten. De eerste opdracht van BPR is ervoor te zorgen dat de infrastructurele functie van de gemeentelijke basisadministratie en de reisdocumenten naar behoren functioneert. Daarnaast beheert BPR verschillende registers en informatiesystemen, waaronder het Basisregister Reisdocumenten, het register van burgerservicenummers (BV BSN) en de centrale component(en) van de moderne GBA (GBA-V). BPR verricht zelf het functioneel beheer (waaronder gegevensbeheer) en voert de regie over de leveranciers die het applicatiebeheer en technisch beheer uitvoeren voor deze informatiesystemen. Het functioneel beheer is dus het primaire bedrijfsproces van BPR; de core business.

te bepalen voor nieuw te ontwikkelen informatiesystemen of wijziging van bestaande informatiesystemen. Er worden zeven stappen doorlopen.

Stap 1: beeld. De eerste stap is het bepalen van het beeld van de bedrijfsprocessen waarvoor het informatiesysteem wordt gebouwd of veranderd. Hierbij wordt naast de functionaliteit vooral gekeken naar de SMART-doelen van deze processen, om de kwaliteitseisen zoals de beschikbaarheid, beveiliging, capaciteit, performance en continuïteit te bepalen. Tevens wordt bepaald welke impact dit informatiesysteem heeft op het beheer (specifiek het functioneel beheer). Vervolgens wordt een plaat gemaakt van de applicatie en de omgeving waarmee de applicatie communiceert. Als derde onderdeel van de beeldvorming wordt een plaat gemaakt van de infrastructurele services waarvan het informatiesysteem gebruikmaakt. Deze platen zijn niet bedoeld als ontwerpdocumenten, maar alleen ter beeldvorming voor de beheerorganisatie van wat er nu eigenlijk geaccepteerd moet gaan worden.

Stap 2: scope. In deze stap wordt een decompositie gemaakt van de applicatieplaat en de infrastructuurplaat in de vorm van bouwstenen (*system building blocks*). Hierdoor wordt het complexe geheel opgedeeld in eenduidig beheerbare eenheden. Van deze bouwstenen wordt bepaald welke wijzigingen ze vereisen ten opzichte van de bestaande infrastructuur en beheerprocessen. Voor bestaande informatiesystemen dienen de platen om vast te stellen welke onderdelen van de applicatie en de infrastructuur door de wijziging worden getroffen. Deze system building blocks (SBB's) worden uniek genummerd. De verkregen SBB-nummers worden gebruikt in de volgende stappen van het GSA-stappenplan, zoals het identificeren van risico's, acceptatiecriteria en testcases.

Naast de decompositie van de infrastructuur en de applicatie worden ook de bedrijfsprocessen uiteengerafeld in de betrokken *use cases* (functionaliteit) en de *supplementary specs* (kwaliteit). De eisen die in stap 1 aan het informatiesysteem zijn gesteld, worden in deze stap per use case uitgewerkt. Ten slotte worden de use cases afgebeeld op de SBB's van de infrastructuur en de applicatie.

Stap 3: risico. De risico's worden bepaald door per SBB-plaat met materiedeskundigen de mogelijke faalfactoren te onderzoeken. Daarna worden de risico's geclassificeerd. Zo worden per risico de kans en de impact bepaald, die samen het belang vormen van beheersing van het risico. De risicobeheersing bestaat uit het definiëren van tegenmaatregelen. Hoe groter het risico, des te belangrijker het is om de tegenmaatregelen toe te passen en te toetsen of ze effectief zijn. Hiertoe worden acceptatiecriteria opgesteld die de basis vormen voor de acceptatietestplannen. Tevens worden de risico's geclassificeerd per SBB, use case en ISO 9126-kwaliteitsattribuut[1]. Deze classificatie van risico's is de basis voor stap 4.

Stap 4: focus. BPR hanteert voor elk project een *master testplan*, waarin het testdomein, de testbasis, de testfocus en de teststrategie worden bepaald. Het testdomein wordt bepaald door de SBB's en de use cases die in stap 2 zijn vastgesteld als scope. De testbasis bestaat uit het benoemen van de testobjecten en de bijbehorende documentatie. Deze informatie komt uit stap 2 en uit het Project Initiation Document van het project. De testfocus geeft aan welke risico's in ieder geval beheerst moeten worden. Deze focus wordt bepaald door de classificatie van de risico's zoals in stap 3 is verricht. Zo kan de nadruk liggen op een bepaalde set van SBB's en use cases, en binnen deze set op het ISO 9126-kwaliteitattribuut beveiliging of beschikbaarheid. De richtlijn is dat de meerderheid van de testcases (bijvoorbeeld tachtig procent) binnen de testfocus moet vallen. Dit zijn immers de risico's die vooral beheerst moeten worden. De overige twintig procent van de risico's worden dus niet beheerst door middel van testcases.

Stap 5: GSA. Deze stap is bedoeld om vast te stellen wanneer de geïdentificeerde risico's worden beheerst. Dit gebeurt door functionaliteiteisen, kwaliteitseisen en beheereisen te formuleren in de vorm van zowel generieke als specifieke acceptatiecriteria. De generieke acceptatiecriteria vormen een basisset van acceptatiecriteria waaruit per project een selectie wordt gemaakt. De specifieke acceptatiecriteria zijn uniek per project en moeten specifiek voor dat project onderkende risico's borgen.

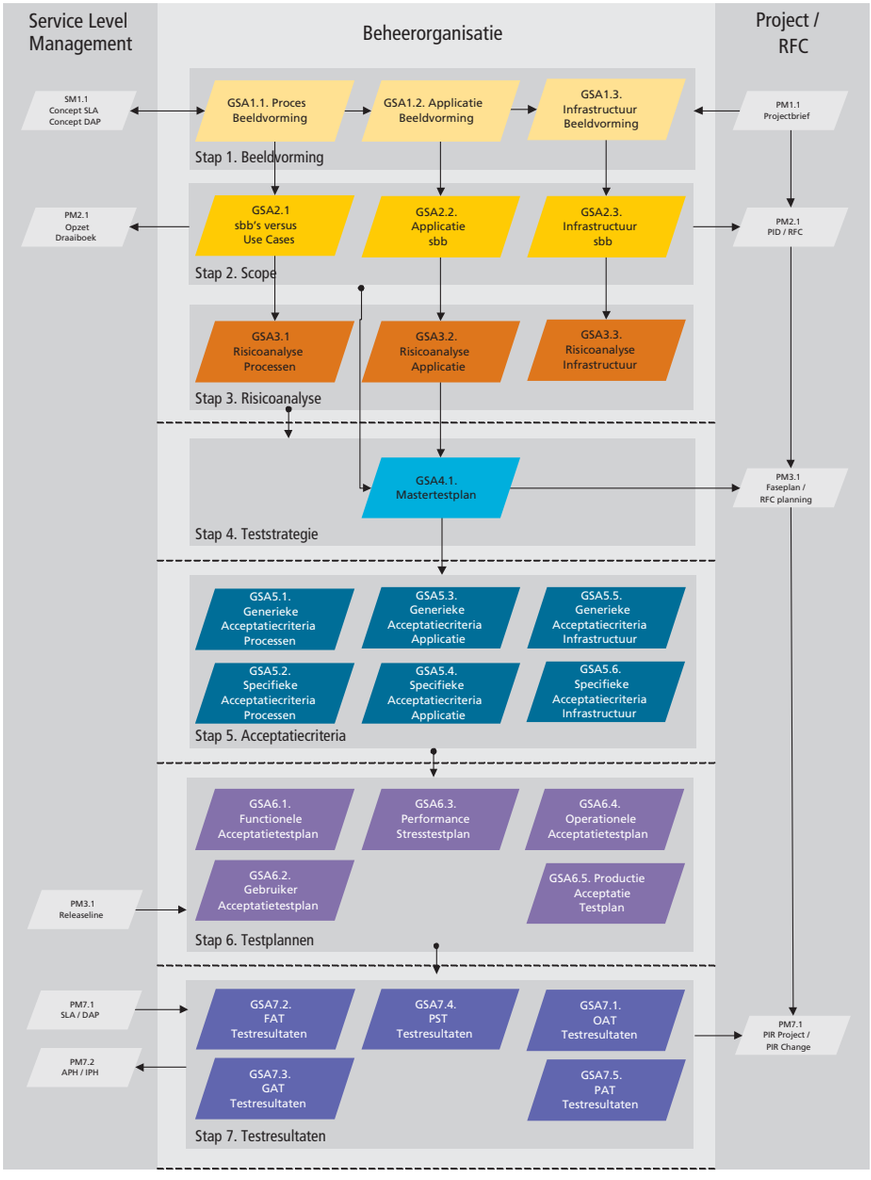
Stap 6: plan. De acceptatietestplannen beschrijven de testscenario's/testcases om vast te stellen of aan de acceptatiecriteria wordt voldaan. Het Operationele Acceptatie Testplan (OAT) omvat ener-

Figuur 1 GSA-stappenplan

zijds de testcases voor de individuele applicatie-SBB's en de infrastructuur-SBB's, en anderzijds de testcases om de juiste samenwerking van deze SBB's te toetsen. Het OAT wordt alleen in de acceptatieomgeving uitgevoerd. Het Productie Acceptatie Testplan (PAT) is een selectie van de OAT-testcases die in de productieomgeving wordt uitgevoerd nadat het informatiesysteem daar is geïnstalleerd en geconfigureerd. Het Functionele Acceptatie Testplan (FAT) wordt gebruikt om vast te stellen of het informatiesysteem de gespecificeerde functionaliteit biedt. Het Gebruiker Acceptatie Testplan (GAT) is bedoeld om vast te stellen of de beheerfunctionaliteit van het informatiesysteem voldoet aan de eisen van de functioneel beheerder en gegevensbeheerder. Het Performance Stress Testplan (PST) ten slotte is bedoeld om het gedrag van het informatiesysteem te testen op aspecten als beschikbaarheid, capaciteit en performance.

Stap 7: test. Dit is de laatste stap in het GSA-stappenplan, waarin de acceptatietestplannen worden uitgevoerd. Ondersteund door de testresultaten wordt aan de CAB een advies over de inproductiename voorgelegd.

Bij elke stap wordt de verkregen informatie vastgelegd in specifiek hiertoe ontworpen documenten. Deze documenten vormen een belangrijke basis voor het beheer van de applicatie en de betrokken infrastructuur. Ze zijn dan ook niet voor eenmalig gebruik, maar dienen als uitgangspunt voor de risico- en impactanalyse ingeval van wijzigingen en onderhoudsprojecten. De documenten en de onderlinge samenhang zijn afgebeeld in figuur 2.

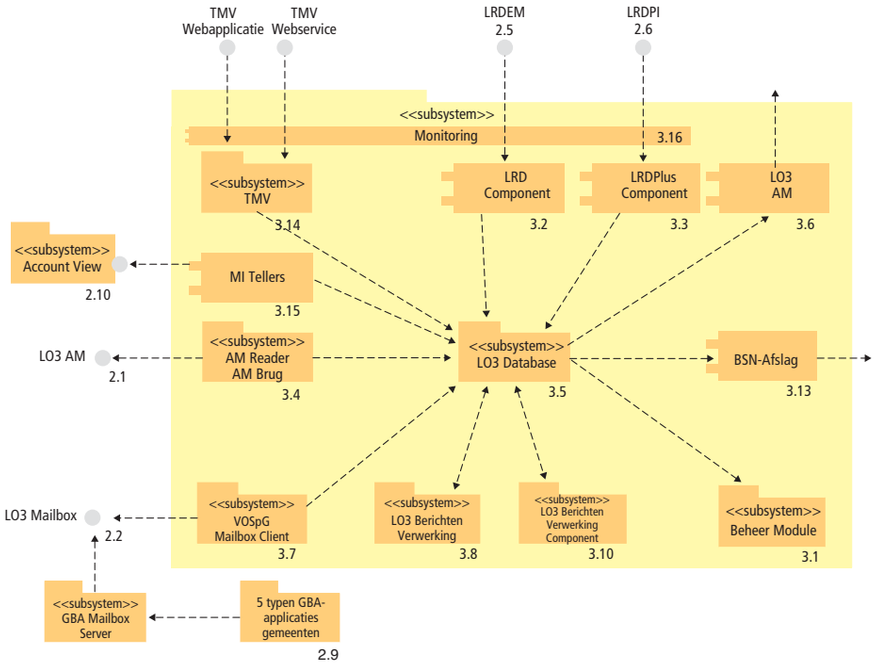


Figuur 2 GSA-stappenplan-documentenflow

Toelichting

Stap 1: beeld. Een voorbeeld van een applicatieplaat (GSA-stap 1.2) is weergegeven in figuur 3. Dit is een eerste oriëntatie op wat gerealiseerd wordt. Deze plaat wordt of opgesteld in een definitiestudie, projectstartarchitectuur, functioneel ontwerp of wordt in samenwerking met het ontwikkelteam opgesteld. Belangrijk is dat deze stap zo vroeg mogelijk in het acceptatietraject wordt verricht.

Voor de infrastructuur wordt een technisch schema (GSA-stap 1.3) gebruikt en voor het procesmodel bijvoorbeeld een *data flow diagram* (GSA-stap 1.1). De drie platen geven een goed beeld van wat opgeleverd gaat worden. Elke plaat wordt door de betrokken stakeholder in een beeldvormingssessie gepresenteerd aan de beheerorganisatie in de volgorde bedrijfsprocesmodel/beheerprocesmodel - applicatieplaat - infrastructuurplaat. Na afstemming van de beeldvorming tussen de ontwikkelorganisatie en de beheerorganisatie worden deze documenten vastgesteld.



Figuur 3 GSA-stap 1.2, applicatiebeeldvorming

Stap 2: scope. De tweede stap is het afbeelden van de infrastructuurplaat op een system building block-plaat (GSA-stap 2.3, zie figuur 4). BPR hanteert voor alle projecten dezelfde SBB-plaat en bepaalt vervolgens welke bouwstenen zijn geraakt.

De infrastructuur-SBB-plaat is opgebouwd uit infrastructurele servicelagen. Elke laag is weer opgebouwd uit een aantal SBB's. De onderste laag is een verzamellaag van infrastructuurbeheerservices. De toegevoegde waarde van de SBB's is velerlei. BPR hanteert de platen voor de volgende zaken:

- overzicht van betrokken beheerpartijen door kleuring van de SBB-i's;
- overzicht van binnen of buiten scope zijn van SBB-i's;
- kleuren van risico's: rood (groot) – geel (middel) – groen (klein);
- stuurgroeppresentaties voor de go/no-gobeslissingen;
- identificatie van risico's, acceptatiecriteria en testgevallen;
- configuratie-items voor ITIL-beheerprocessen.

Analoog aan de infrastructuur-SBB-plaat wordt ook voor de applicatie een SBB-plaat gemaakt (GSA-stap 2.2, zie figuur 5). Ook die is ingedeeld in lagen met daarbinnen de bouwstenen, en ook hier is de onderste laag gericht op het beheer. De laag daarboven bevat de applicatie-interfaces met andere informatiesystemen, de derde laag de applicatieprocesverwerkende modulen, en ten slotte komen de rapportage en de gebruikersinterfaces.

Stap 3: risico. BPR hanteert voor zowel het proces, de applicatie als de infrastructuur een risicoanalyse. Hierbij worden drie groepen gevormd. De applicatie- en de infrastructuurgroep duiden de risico's die alleen aan één SBB toe te kennen zijn. Hierbij wordt bijvoorbeeld de A&K-analyse (afhankelijkheden & kwetsbaarheden) gehanteerd. De derde groep bepaalt de procesgerelateerde risico's. Hiertoe worden de risico's per use case bepaald op basis van de afbeelding van de use case op de betrokken infrastructuur en applicatie-SBB's (zie figuur 6).

Op basis van de initiële risico's wordt bepaald of een risico groot, middel of klein is door te bepalen wat de kans en de impact ervan is. Alle onderkende risico's worden voorzien van tegenmaatregelen. De risico's inclusief tegenmaatregelen zijn de basis voor de acceptatiecriteria.

Stap 4: focus. Behalve voor het bepalen van het testdomein en de testbasis is het master testplan ook bedoeld om een testfocus te bepalen voor de onderkende risico's en vervolgens de teststrategie (zie tabel 1). Hierbij worden de producten uit stap 2 en stap 3 gecombineerd. Tevens wordt de dekkingsgraad van de testcases vastgelegd in het master testplan door per SBB de testcases te tellen en te vergelijken met de risicokleuring.

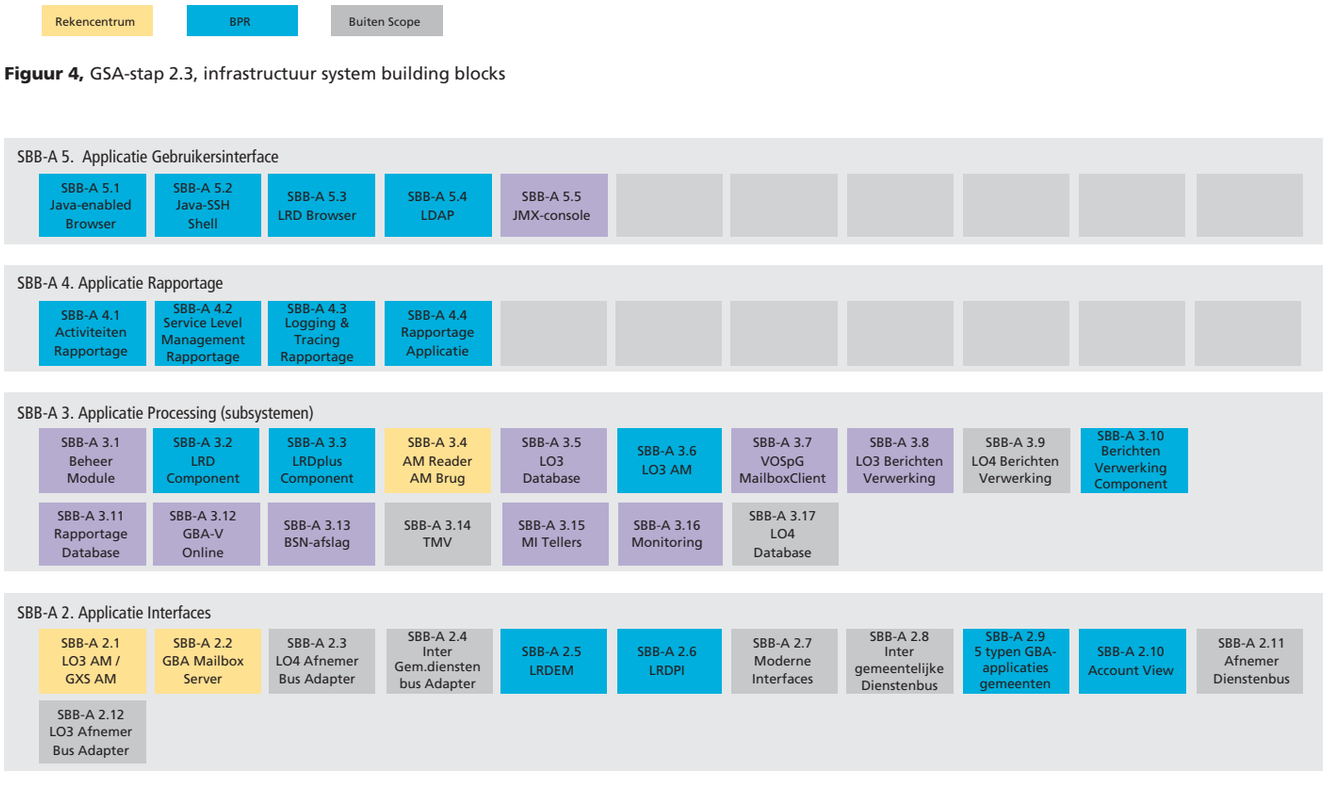
Stap 5: acceptatiecriteria. De acceptatiecriteria zijn bedoeld om vast te stellen of de risico's effectief worden beheerst (zie een voorbeeld in tabel 2).

Praktijkervaring

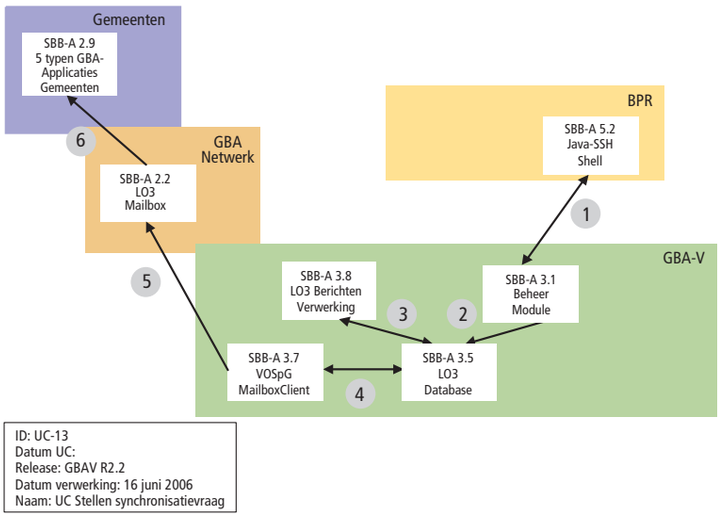
De belangrijkste best practices voor het toepassen van het GSA-stappenplan zijn:

- Begin in een project van meet af aan met het volgen van het stappenplan. De acceptatiecriteria moeten vaststaan voordat aan de bouw wordt begonnen.
- Acceptatiecriteria en servicenormen (in een sla) gaan hand in hand. Stel beide gelijktijdig op en relateer ze aan elkaar.
- Het beheersen van risico's vereist beeldvorming (stap 1) en afbakening (stap 2) op zowel proces-, applicatie- als infrastructuurniveau.
- Een risicosessie levert meer relevante risico's op door:
  - de drie aspectgebieden infrastructuur, applicatie en processen te scheiden. Wel moet minimaal één persoon alle drie de sessies bijwonen;
  - een grondiger voorbereiding door bijvoorbeeld een beeldvormingssessie, waarin de platen uit de documenten van stap 1 en stap 2 worden doorgenomen en gecontroleerd. Ook moeten de betrokkenen tijdig de relevante projectdocumentatie krijgen en hebben gelezen;

Figuur 4, GSA-stap 2.3, infrastructuur system building blocks



Figuur 5 GSA-stap 2.2, applicatie system building blocks



Figuur 6 GSA-stap 2.1, use cases versus system building blocks

  - meer domeinkennis aanwezig te laten zijn. Het verdient de voorkeur om in ieder geval de betrokken beheerders (waaronder leveranciers) uit te nodigen; zij hebben het grootste belang bij het onderkennen en beheersen van de risico's.
- Het verdient aanbeveling om de betrokken beheerders zelf de risicolijsten in te laten vullen (inclusief kans en impact). Deze risicolijsten moeten van tevoren aan de risicosessiedeelnemers worden gestuurd. Zij kunnen dan vooraf hun eigen risico's noteren.
- Eenduidige id's van SBB's maken de risicobeheersing makkelijker te traceren over acceptatiecriteria, testcases en testresultaten.
- Voorkom dubbelingen van risico's door eerst de SBB-gerelateerde risico's te bepalen en pas daarna de use case-gerelateerde risico's (die door de samenwerking van SBB's worden bepaald).
- Acceptatiecriteria moeten voorafgaand aan de bouw met de betrokken bouwers worden doorgenomen. Per acceptatiecriterium moet vastgesteld worden op welke wijze invulling gegeven gaat worden aan de gestelde eis.

		TESTSOORT				
SBB	Gerelateerde service	OAT	FAT	GAT	PST	PAT
SBB-I 3.1	Webserver Communicatie					
SBB-I 3.2	Reverse Proxy					
SBB-I 3.3	Firewall					
SBB-I 3.4	Routers					
SBB-I 3.5	Applicatie Communicatie					
SBB-I 3.6	Database Communicatie					

Tabel 1 Onderdeel van master testplan

ID	TCR	ISO9126	Acceptatiecriterium	Meetvoorschrift
A1.3-05	T	Analyseerbaarheid	HERLEIDBAARHEID Elke foutboodschap moet refereren naar het onderdeel van de applicatie waar de fout is opgetreden.	Controleer de foutenlijst, verifieer dit bij het steekproefsgewijs veroorzaken van fouten.

Tabel 2 Voorbeeld acceptatiecriterium

- Het vertalen van acceptatiecriteria naar standaards en richtlijnen voor het bouwteam is een prima borging voor de kwaliteit, mits die standaards en richtlijnen worden bewaakt.
- De A&K-analyse en het stappenplan blijken goed samen te gaan, maar hiertoe moet wel een afstemming plaatsvinden tussen SBB's en de in de A&K-analyse onderkende objecten.
- RUP (Rational Unified Process) en het GSA-stappenplan zijn goed integreerbaar. Belangrijk is wel om onderscheid te maken tussen drie stromen: processen, applicatie en infrastructuur. De snelheden van het doorlopen van het stappenplan zijn namelijk niet evenredig aan elkaar. De infrastructurele GSA-stappen lopen in de fasen van RUP achter op de processen en de applicatieve GSA-stappen. Het uiteenlopen van de stappen moet echter beperkt blijven. Voor de bouwfase moeten de acceptatiecriteria vastgesteld zijn en omgezet zijn in standaards en richtlijnen.
- De generieke acceptatiecriteria kunnen prima hergebruikt worden. Het is wel belangrijk om per project een selectie te maken. Ook moeten die acceptatiecriteria techniekonafhankelijk geschreven worden.

Hierbij dank ik de vele reviewers van dit artikel en het agentschap BPR voor hun medewerking aan dit artikel, met name drs. ing. P. (Peter) de Jong, coördinator service management. Verder dank aan ing. P.P.M. (Pascal) Huijbers voor zijn toestemming om de SBB- infrastructuurplaat bij BPR te gebruiken.

Drs. ing. B. de Best RI, E-mail: bartb@qforce.nl

Noten/literatuur

1 ISO 9126 is een kwaliteitsmodel van ISO waarbinnen kwaliteit van informatiesystemen is gedefinieerd aan de hand van een aantal kwaliteitsattributen, zoals beschikbaarheid, onderhoudbaarheid, et cetera.

De Best, B., 'Gebrek aan kwaliteitsbeheersing pragmatisch aanpakken', in: *IT Beheer Magazine* 7/2005

De Best, B., 'Acceptatiecriteria in de praktijk', in: *IT Beheer Magazine* 1/2006

B. de Best, *Acceptatiecriteria*, Sdu Uitgevers, 2006. ISBN 9039524998