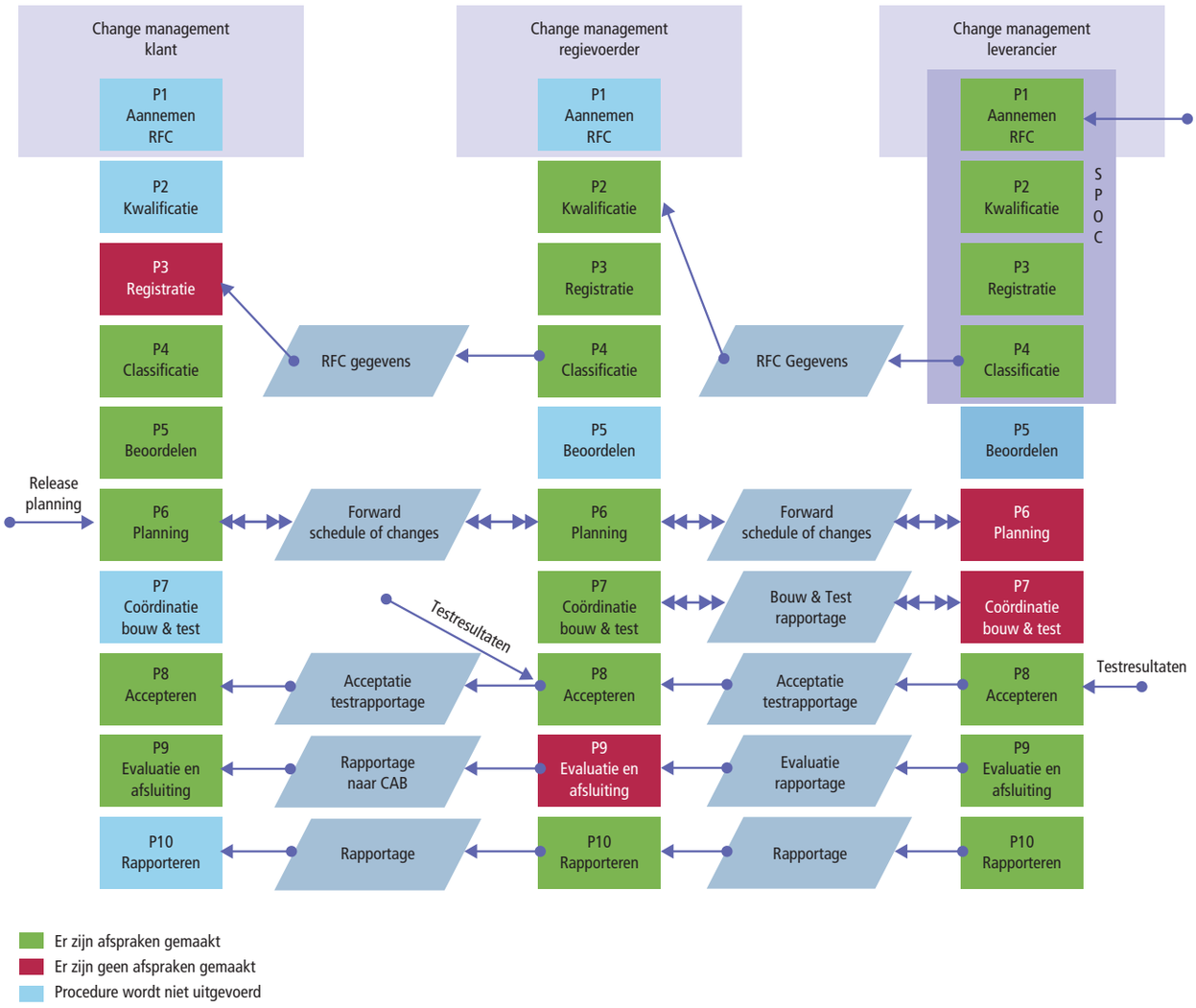
Beheerrequirements voor regievoering

Bij de derde generatie outsourcing besteedt een klant de dienstverlening uit aan verschillende leveranciers. De regievoering over die leveranciers wordt tegenwoordig ook steeds vaker uitbesteed en dan vooral de operationele regievoering. Met zoveel spelers rijst al snel de vraag hoe de beheerprocessen van alle betrokken partijen op elkaar af te stemmen. GlidePath heeft hiertoe invulling gegeven aan het beheerarchitectuurraamwerk, zoals in voorgaande nummers van dit blad is gepubliceerd. Dit artikel beschrijft de door GlidePath gehanteerde werkwijze.
Na een korte beschrijving van de generaties van outsourcing gaat dit artikel eerst in op de problemen die veel organisaties ervaren bij de regievoering over leveranciers aan wie de ICT-dienstverlening is uitbesteed. Daarna wordt de oplossingsrichting besproken.

Bart de Best

De context
Uitbestedingen zijn tegenwoordig een normaal verschijnsel. Toch zijn er in de afgelopen tien jaar grote veranderingen waar te nemen in de wijze waarop dit gebeurt. Er wordt zelfs regelmatig gesproken over generaties van uitbestedingstrategieën.
De eerste generatie van uitbestedingen kenmerkt zich door het afscheid nemen van de gehele ICT-organisatie, aan één partij voor langere tijd. Dit leidde al snel tot het besef dat de flexibiliteit en innovatie die de business vereist, haaks staat op het in beton gieten van de dienstverlening.
De tweede generatie van uitbestedingen gaat dan ook uit van een kortere contractduur waarbij de leverancier zelf gebruikmaakt van de verschillend gespecialiseerde toeleveranciers.
De derde generatie geeft nog meer vrijheidsgraden aan de klant. Hierbij wordt uitgegaan van een uitbesteding aan meer partijen.

Bij de derde generatie van uitbesteding kan ook de regievoering over de leveranciers worden uitbesteed. In het beheerlandschap dat hiermee wordt vormgegeven komt er nu een rol bij en zien we drie prominente rollen naar voren komen: de klant, de regievoerder en de verschillende leveranciers. In dit artikel noemen we de organisaties die deze rollen invullen de beheerpartijen. Het geheel van te beheren ICT-producten



Figuur 1 Beheerprocesketen

en ICT-diensten door één beheerpartij noemen we een beheerdomein. Zo onderkennen we het klantdomein, het regiedomein, en het leveranciersdomein.

Waar in de eerste en tweede generatie outsourcing meestal een beheerproces voor het grootste gedeelte binnen één beheerorganisatie wordt afgehandeld, zien we bij de derde generatie outsourcing dat elk beheerdomein een deel van een beheerproces voor zijn rekening neemt (zie figuur 1).

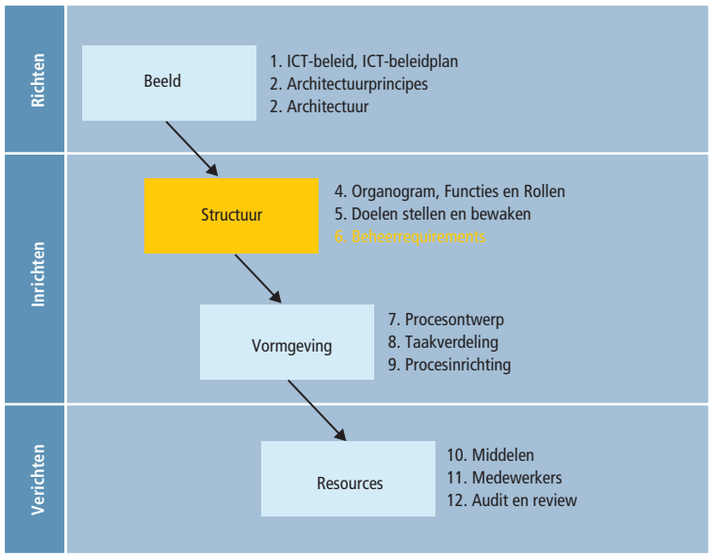
Vooral de operationele beheerprocessen, zoals change management, vormen op deze wijze ketens van beheerprocessen. Belangrijk hierbij is te onderkennen dat elke beheerpartij wel degelijk alle beheerprocessen volledig kan hebben vormgegeven. Tevens passen de leveranciers hun procesinrichting voor diverse klanten toe in wellicht meer dan één keten van beheerprocessen.

Het effectief en efficiënt doorlopen van een keten van aaneengeschakelde beheerprocessen vereist dat elke beheerpartij in de keten actief meedoet om zijn gedeelte af te stemmen op de keten van de klant om de keten SLA-afspraken invulling te kunnen geven. Hiertoe is het noodzakelijk om per keten van beheerprocessen beheerrequirements op te stellen en de naleving te bewaken.

In IT Beheer Magazine nummer 10, 2007, is beschreven hoe regie onder architectuur kan worden vormgegeven aan de hand van het BEA-stappenplan, zoals

GlidePath

GlidePath is een ISO-gecertificeerde service managementorganisatie die operationeel beheer en regievoering diensten levert voor complexe of bedrijfskritische ICT-omgevingen. Het ICT Operations Center van GlidePath biedt haar diensten aan op basis van een geïntegreerd beheermodel dat uniek is in haar soort. Naast dit portfolio van operationele beheerdiensten, heeft het bedrijf een model ontwikkeld waarmee de regie gevoerd wordt over alle betrokken leveranciers die een rol spelen in de infrastructuur van haar klanten. Samen vormen deze diensten de basis voor een betrouwbaar ICT-platform en ICT-operatie. Hiermee speelt GlidePath in op de strikter wordende regelgevingen over de aantoonbare operationele controle bij bedrijven. Om dit te garanderen heeft het bedrijf zich laten certificeren voor de hoogste code van informatiebeveiliging (ISO27001) en worden plannen uitgewerkt om op COBIT-niveau te gaan functioneren.
In totaal werken bij GlidePath 60 mensen die 35 klanten bedienen in Nederland en Duitsland.



Figuur 2 Beheren onder Architectuur (BEA) stappenplan[2,3,4]

afgebeeld in figuur 2. Dit onderhavige artikel zoomt in op stap nummer 6, de beheerrequirements, en laat zien hoe GlidePath hier concreet invulling aan heeft gegeven.

Probleemstelling

Het vormgeven aan een keten van beheerprocessen is in grote lijnen gelijk aan die van een enkelvoudige beheerprocesinrichting. De stappen van het BEA-stappenplan zijn dus ook hier van toepassing. Er is echter een aantal specifieke verschillen te benoemen dat een andere aanpak vereist. De belangrijkste verschillen zijn:

- Elk beheerdomein:
  - heeft een eigen beheerorganisatie en dito procesinrichting;
  - administreert alle informatie voor zijn eigen beheerprocessen;
  - heeft eigen service management en system management tools die gelden als basis voor de eigen procesbesturing;
  - heeft zijn eigen rol in de keten (proceseigenaar, procesmanager, procesuitvoerder). [4]
- De beheerorganisaties gebruiken in de praktijk weliswaar vaak marktstandaarden zoals ITIL, ASL en BiSL, maar:
  - hanteren niet alle daarbinnen onderkende beheerprocessen;
  - hanteren per beheerproces een andere procedure-indeling, afwijkende werkinstructies en rapportages en eigen terminologie;
  - gebruiken geen eenduidig begrippenkader;
  - de beheerprocessen verschillen vaak qua volwassenheid.

De oplossingsrichting

Om de dualiteit van autonomie en ketenoriëntatie het hoofd te bieden is het architectuurdenken een randvoorwaarde. De stappen 1 en 2 van het BEA-stappenplan, zoals afgebeeld in figuur 2, moeten dan ook leiden tot een duidelijk ICT-beleidsplan en architectuurprincipes van de klant. Dit moet gedeeld worden met de regievoerder en de leveranciers. Regievoering vereist ook een duidelijke afbakening van beheerdomeinen, hieraan kan in stap 3 invulling gegeven worden met een beheerprocessenblauwdruk[1]. Door de beeldvorming die verkregen is in stappen 1, 2 en 3 zouden de inrichtingstappen 4 tot en met 9 van het BEA-stappenplan genoeg richting moeten krijgen om een goede samenwerking in de keten tot stand te brengen. Dit blijkt in de praktijk echter niet zo eenvoudig als dit lijkt. 'The devil is in the detail' wordt vaak gesteld en dat geldt ook bij de regievoering.

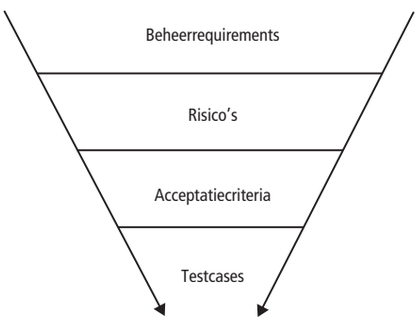
Juist bij de stappen 7, 8 en 9 blijkt vaak dat de afgestemde beeldvorming schipbreuk leidt. Dit komt door tal van factoren, zoals vervanging van mensen tijdens de rit, veranderingen in de organisatiestructuur in de betrokken beheerdomeinen, onvoldoende of slechte communicatie naar de met de inrichting en/of uitvoering belaste personen/afdelingen, en last-but-not-least het feitelijk pas begrijpen van de impact van wat gevraagd wordt bij het concretiseren ervan.

Stap 6 van het BEA-stappenplan moet dit probleem tackelen. Door van meet af aan beheerrequirements op te stellen en af

te stemmen, kunnen beelden sneller worden geconcretiseerd en kunnen vroegtijdig maatregelen worden genomen. En dat is nu precies wat we bij requirement management vanuit systeemontwikkeling ook leren kennen. Wat opgeleverd moet worden is nu alleen geen informatiesysteem, maar een beheerorganisatie.

Deze stap van het BEA-stappenplan kent een tweeledige betekenis toe aan de beheerrequirements. Aan de ene kant zijn beheerrequirements de eisen met betrekking tot de functionaliteit, kwaliteit of beheersbaarheid van een ICT-product en/of ICT-dienst die gesteld worden vanuit de beheerorganisatie om de SLA-normen te borgen. Aan de andere kant omvat het de eisen die gesteld worden aan de beheerprocessen en de daarbij gehanteerde beheermiddelen, om de beheerprocesdoelen te kunnen realiseren. Dit artikel gaat in op dit laatste aandachtsgebied.

Hierbij wordt onderscheid gemaakt tussen beheerrequirements en acceptatiecriteria, zoals gedefinieerd in het begrippenkader aan het einde van dit artikel. Omdat in dit artikel alleen ingegaan wordt op de acceptatiecriteria voor de beheerprocessen, de zogenoemde generieke acceptatiecriteria, worden deze verder kortweg geduid als 'acceptatiecriteria'.



Figuur 3 Relatie tussen beheerrequirements en acceptatiecriteria

De beheerrequirements gelden als ontwerpcriterium voor de inrichting van de beheerorganisatie (processen/middelen). De acceptatiecriteria worden gehanteerd als toetsing van de *deliverables* van de beheerorganisatie-inrichting om vast te stellen of de onderkende risico's afdoende zijn beheerst. Figuur 3 laat de samenhang tussen deze termen zien.

In tabel 1 zijn een aantal voorbeelden opgenomen van beheerrequirements die een proceseigenaar kan hanteren.

De proceseigenaar dient de risico's van constructiefouten, gebreken en andere tekortkomingen in de beheerprocesinrichting te beheersen. Hiertoe organiseert hij een risicoanalyse-bijeenkomst waarin op basis van de beheerrequirements en het procesontwerp de risico's worden bepaald. Deze worden bij oplevering en/of jaarlijks (in een audit) aan de hand van acceptatiecriteria getoetst om vast te stellen dat de onderkende risico's beheerst zijn. Hierbij vormen de acceptatiecriteria in wezen een *subset* van de beheerrequirements op basis van een risicoanalyse. Een aantal voorbeelden hiervan zijn opgenomen in tabel 2.

De Toepassing

De toepassing van beheerrequirements en acceptatiecriteria klinkt eenvoudiger dan het is. Om te komen tot een doelmatige toepassing is het belangrijk om voor elk beheerproces invulling te geven aan het onderstaande stappenplan:

1. Beheerrequirements:
   - 1.1 bepaal de eigenaar, de scope en de bron van de beheerrequirements;
   - 1.2 borg dat alle betrokken partijen akkoord gaan met de beheerrequirements;
   - 1.3 stem af wanneer voldaan is aan de beheerrequirements;
   - 1.4 bepaal binnen welke beheerprocedures er invulling aan gegeven moet worden;
   - 1.5 plan en bewaak de realisatie.
2. Acceptatiecriteria:
   - 2.1 bepaal op basis waarvan risico's voor de beheerprocessen bepaald worden;
   - 2.2 bepaal de risico's;
   - 2.3 bepaal met welke acceptatiecriteria de beheersing van de risico's getoetst kan worden;
   - 2.4 stem af wanneer voldaan is aan een acceptatiecriterium;
   - 2.5 plan wanneer, hoe en door wie een acceptatiecriterium getoetst wordt.

Ter verduidelijking zijn hieronder een aantal best practices opgenomen die toegepast kunnen worden bij het doorlopen van deze stappen.

1. Best practices
Beheerrequirements:

1.1 Zorg ervoor dat er maar één proceseigenaar per beheerproces (keten) onderkend wordt. Deze proceseigenaar moet de beheerrequirements vaststellen.

De scope van de beheerequirements hangt samen met de aard van de relatie. Zo zijn er blackbox-, whitebox- en greybox-benaderingen te onderkennen.

a) Bij een blackbox-benadering hanteert ieder beheerdomein wat hij zelf de beste oplossing acht. De beheerrequirements gelden dan alleen voor de interface, dus de informatie-uitwisseling en de sturing (rapportage).

b) Bij een whitebox-benadering wordt de werking van een beheerproces over de beheerdomeinen heen inhoudelijk geanalyseerd en op elkaar afgestemd. Dit geeft veel meer flexibiliteit, maar is ook veel complexer te realiseren. Zeker als het beheerdomein onderdeel is van meer ketens.

c) De greybox-benadering gaat uit van een aantal eisen, dat gesteld wordt aan de werking van het proces, vooral voor incidenten,

Beheerrequirements voor beheerprocessen:	
ID	Beheerrequirements
SLM-104	**Niet halen normen.** Opdrachtnemer signaleert aan opdrachtgever als het afgesproken serviceniveau niet kan worden nagekomen, en wel bij voorkeur vooraf en anders zo snel als mogelijk.
CHM-112	**Fallback.** Er is ten tijde van implementatie een fallbackscenario beschikbaar om in geval van onvoorziene problemen de wijziging terug te kunnen draaien.
PBM-104	**Known errors.** Structurele oorzaken worden geadministreerd in een lijst met 'bekende fouten'.
ICM-105	**Registratie.** Van elke melding worden de volgende zaken vastgelegd: Call/ITSM nummer, categorie, datum en tijd van aanmelding, datum en tijd van afmelding, naam en organisatie aanmelder, naam service deskmedewerker, aard van de melding, oplossing/afhandeling, urgentiecode en status.
CFM-103	**Statusoverzicht.** In de vastgelegde configuratierecords wordt zowel de actuele status als de geschiedenis van de statuswijzigingen opgenomen.

Tabel 1 Beheerrequirements

Acceptatiecriteria voor beheerprocessen:		
ID	**Risico's**	**Acceptatiecriteria**
SLM-004	**Meetbaarheid** De SLA is niet (economisch) meetbaar. De meetbaarheid betreft hier de Prestatie Indicatoren (PI): – per beheerdomein; – per beheerproces; – per service.	1. Onderken Herkenbare Prestatie Indicatoren (HPE) per PI, bijvoorbeeld de ICT-services per bedrijfsproces. 2. Ken PI's en normen toe per HPE.
CHM012	**Informatievoorziening** De change manager krijgt niet een compleet overzicht van de risico's en de mate waarin deze zijn beheerst, waardoor een GO/NOGO op onvolledige informatie is gebaseerd.	Borg in het Dossier Afspraken en Procedures dat de change manager van alle betrokken beheerpartijen een risicoanalyse ontvangt van alle RFC's waarvan het risico medium of hoog is. Van elk risico is aangegeven hoe wordt vastgesteld dat de risico's adequaat beheerst zijn aan de hand van acceptatiecriteria die voorzien zijn van meetvoorschriften. Een GO/NOGO wordt alleen gegeven op basis van een testrapport van de acceptatiecriteriatoetsingen.
PBM-001	**Jump to conclusions** De probleemanalyse is inefficiënt als gevolg van het onnodig analyseren van mogelijke oorzaken van problemen, omdat van te voren had kunnen worden vastgesteld dat deze oorzaken niet gerelateerd zijn aan de symptomen.	Problemen worden met probleemanalyse methode opgepakt die jump-to-conclusions uitsluiten, zoals Kepner & Tregoe.
ICM-003	**Knowledge base** Het percentage gematchte incidenten is veel te laag als gevolg van een niet adequate knowledge base, waardoor de SLA-oplostijden niet gehaald worden.	Van elk incident wordt achteraf bepaald welke informatie aan de knowledge base moet worden toegevoegd.
CFM-002	**Scope** De scope en het detailleringniveau van de CMDB zijn niet afgestemd op de dienstverlening.	De SLA bepaalt de minimale scope van de CMDB aan de hand van de onderkende Logische Configuratie Items.

Tabel 2 Risico's en acceptatiecriteria

problemen en changes die meer beheerdomeinen raken. Hiervoor worden dan specifieke afspraken gemaakt over hoe te werk wordt gegaan en waar nodig worden beheerprocessen in beheerdomeinen aangepast, zoals een andere of additionele risicoanalysemethode of probleemanalysemethoden.

De bronnen van de beheerrequirements zijn:

a) de verbeterpunten uit de reguliere ketenreviews en ketenaudits;
b) de klachten van betrokken partijen (gebruikers en beheerdomeinen);
c) het niet halen van SLA-normen;
d) de initiatie van een beheerketen (ontwerp in een greenfield-situatie).

Intermezzo I
Afstemming volwassenheid De volwassenheid van de beheerorganisatie en die van de leveranciers moeten op elkaar zijn afgestemd.
Marktconformiteit Door marktconforme beheermodellen toe te passen in architectuurmodellen is het eenvoudiger om ICT-diensten af te stemmen met leveranciers.
Eenheid van bestuur Door maximaal één proceseigenaar en procesmanager te benoemen voor een beheerproces, ongeacht het aantal betrokken beheerdomeinen, ontstaat er een eenduidige inrichting en besturing van het proces.
Extern eigenaarschap Door het eigenaarschap van een volledig uitbesteed beheerproces bij de leverancier te leggen, wordt optimaal gebruikgemaakt van het economics-of-scales-effect.
SMART-doelen Door elk procesdoel (functioneel doel, kwaliteitdoel en volwassenheiddoel) SMART te definiëren neemt de kans dat dit doel gehaald wordt toe.
Doelen afstemmen Door een beheerproces te besturen op zowel een functioneel doel, kwaliteitdoel als volwassenheiddoel is het mogelijk om de werking van het proces af te stemmen op de doelen van het beheerdomein en de relaties met andere (beheer)domeinen.
Interfacebenadering Door de interfacebeschrijving tussen de interne en externe beheerorganisatie te beschrijven op beheerproces- en beheerprocedureniveau, wordt voorkomen dat de afspraken zo gedetailleerd worden dat ze onwerkbaar en/of incompleet worden.
Regelkring Het hanteren van een regelkring (uitvoeren, meten, terugkoppeling besturing) in de procesbesturing verhoogt niet alleen de kwaliteit van het proces, maar geeft tevens aan waar gaten zitten in het kwaliteitsysteem.

1.1 De proceseigenaar stemt de door hem vastgestelde beheerrequirements af met de procesmanagers van de betrokken beheerdomeinen.

1.2 Voor elk beheerrequirement moet gedocumenteerd zijn hoe vast te stellen is of hieraan is voldaan, kortom er moet een meetvoorschrift zijn vastgesteld.

1.3 De blauwdruk definieert de beheerprocesdemarcatie. Deze opdeling van verantwoordelijkheden op procesniveau wordt in het beheerprocesontwerp gedetailleerd naar verantwoordelijkheden per beheerprocedure. Door de beheerrequirements te matchen met de beheerprocedures is ook duidelijk in welke beheerdomeinen de beheerrequirements invulling moet worden gegeven.

1.4 Het is verstandig om de beheerrequirements onderdeel te maken van het Service Quality Plan (procesverbeterplan). Dit SQP wordt normaal gesproken opgesteld op basis van een review of audit. De proceseigenaar kan de bewaking vormgeven aan hand van de volgende punten:

a) regelmatig afstemmingsmomenten inplannen met de procesmanagers; in de praktijk blijkt één dag in de veertien dagen het absolute minimum bij een beperkt aantal deelnemers (één klant, één regievoerder, vijf leveranciers);
b) inplannen van de realisatie van de beheerrequirements;
c) de resultaten in de afstemmingsoverleggen bespreken;
d) formele rapportage van de procesmanagers aan de proceseigenaar laten toesturen;
e) afstemmen van de verbeterplannen om de keten goed te laten verlopen.

2. Best practices acceptatiecriteria

2.1 De risico's van de beheerprocessen kunnen het beste afgeleid worden van de doelen van de beheerprocessen en dan vooral het kwaliteitsdoel. Door vast te stellen wat de Kritieke Succes Factoren (KSF's) zijn voor het halen van de doelen kunnen deze gedefinieerd worden als te beheersen risico's. Een KSF is immers de reden waarom mogelijkerwijs de doelstelling van het beheerproces niet gehaald wordt.

2.2 Laat elke proceseigenaar samen met de procesmanagers uit de verschillende beheerdomeinen de risico's bepalen. Hiertoe dienen de beheerrequirements en de procesontwerpen als basis.

2.3 Voor elk onderkend risico moet bepaald worden wat de beste beheersing is in de zin van één of meer acceptatiecriteria. Feitelijk zijn de acceptatiecriteria dus die subset van de beheerrequirements die risicovol zijn.

2.4 Voor elk acceptatiecriterium moet een meetvoorschrift vastgesteld worden. Hiertoe kan het meetvoorschrift van het beheerrequirement worden overgenomen. Omdat de acceptatie-

Begrippenkader

In de artikelen die in dit blad over beheerarchitectuur zijn verschenen[1,2,3,4,5] is gekeken naar de toepassen van beheerarchitectuur bij diverse organisaties vanuit verschillende hoedanigheden (projecten, regievoering en architectuur). Daarbij zijn dan ook kleine verschillen ontstaan in het begrippenkader. Dit artikel definieert de begrippen in de volledige breedte en geeft tevens de samenhang weer. Als basis is uitgegaan van de definitie van het boek 'acceptatiecriteria' [Best 2006/1]'[6].

Beheerrequirements
Een beheerrequirement is een eis met betrekking tot de functionaliteit, kwaliteit of beheerbaarheid van een ICT-product en/of ICT-dienst die gesteld wordt vanuit de beheerorganisatie teneinde de doelstellingen van de beheerprocessen te borgen. Daarnaast zijn er ook beheerrequirements die eisen stellen aan de producten die voortvloeien uit de beheerprocesinrichting zoals beheerprocesontwerpen, beheerprocedures en beheermiddelen.

Generieke acceptatiecriteria
Generieke acceptatiecriteria zijn de te toetsen beheerrequirements die de beheerorganisatie stelt aan de te gebruiken ICT-producten, ICT-diensten, en de producten die voortvloeien uit de beheerprocesinrichting zoals beheerprocesontwerpen, beheerprocedures en beheermiddelen, om de mate waarin de onderkende risico's zijn beheerst vast te stellen.

De generieke acceptatiecriteria zijn gebaseerd op de kritieke succesfactoren van de beheerprocessen van de beheerorganisatie. Deze acceptatiecriteria heten 'generieke acceptatiecriteria' omdat ze zoveel als mogelijk informatiesysteem onafhankelijk zijn gedefinieerd. Ze kunnen (tot op zekere hoogte) zelfs organisatie onafhankelijk gedefinieerd worden door te kiezen voor een algemeen gangbaar referentiemodel als ITIL [Best 2006/1].

Specifieke acceptatiecriteria
Specifieke acceptatiecriteria zijn de te toetsen requirements die de gebruikersorganisatie stelt aan de te gebruiken ICT-producten en ICT-diensten, om de mate waarin de onderkende risico's zijn beheerst vast te stellen.

De specifieke acceptatiecriteria zijn gebaseerd op de kritieke succesfactoren van de bedrijfsprocessen van de gebruikersorganisatie. Deze acceptatiecriteria heten 'specifieke acceptatiecriteria' omdat ze per organisatie en zelfs per product moeten worden bepaald [Best 2006/1].

criteria onderdeel kunnen zijn van een audit kan het zijn dat het meetvoorschrift aangepast moet worden. Ook kan het risico een aanpassing van het meetvoorschrift vereisen.

2.5 De toetsing van de acceptatiecriteria vindt idealiter plaats op twee momenten, te weten de oplevering door de procesmanager en de jaarlijkse audit.

Rollen
De rolverdeling voor het hanteren van beheerrequirements is als volgt. De **ICT-manager** wordt geïnformeerd over de behaalde resultaten.

De **beheerarchitect** bewaakt dat de beheerrequirements invulling geven aan de beleidsuitgangspunten van het ICT-beleid. Ook bewaakt de beheerarchitect dat de beheerrequirements harmoniëren met de architectuurprincipes voor de beheerorganisatie (zie Intermezzo I).

Daarnaast controleert de beheerarchitect de toepassing van de architectuurmodellen, zoals de blauwdruk. De beheerrequirements moeten overeenkomstig de demarcatielijnen (beheerdomein scheidingslijnen) van de blauwdruk gekozen worden. Hiertoe adviseert de beheerarchitect de service manager en de proceseigenaren. Tot slot controleert de beheerarchitect of de architectuurprincipes afdoende vertaald zijn naar beheerrequirements om de realisatie van de architectuurprincipes te borgen.

De **Service manager** bewaakt dat de beheerprocessen en beheermiddelen harmonieus samenwerken. Vanuit die rol ondersteunt en adviseert hij de proceseigenaren bij het opstellen van de beheerrequirements. Daarnaast adviseert de service manager de proceseigenaren op het gebied van de risicobeheersing en het hanteren van een adequate set van acceptatiecriteria voor de acceptatie van de beheerprocesinrichting. De service manager is het centrale aanspreekpunt voor zowel de business, de IT-manager als de regievoerder en de leveranciers en vice versa.

De **proceseigenaar** stelt het beheerprocesontwerp vast en geeft daarbij invulling aan de beheerrequirements.

De proceseigenaar verricht vervolgens samen met de belanghebbenden een risicoanalyse om de risico's van de doelen van zijn beheerproces in kaart te brengen. Deze risico's kunnen betrekking hebben op zowel mensen, methoden als middelen. Daarnaast stelt hij de proactieve en reactieve tegenmaatregelen vast om de risico's te beheersen. Tot slot selecteert hij op basis van de uitkomst van de risicoanalyse de optimale set van acceptatiecriteria. De acceptatiecriteria dienen om de risico's tijdens de procesimplementatie te beheersen.

De **procesmanager** bewaakt dat invulling wordt geven aan het functionele doel, het kwaliteit doel en het volwassenheidsdoel. Hiertoe richt de procesmanager zijn beheerproces conform het procesontwerp in. Daarbij is hij verantwoordelijk om de door de proceseigenaar opgestelde beheerrequirements invulling te geven en te toetsen. Daarnaast wordt in de jaarlijkse audit getoetst of het beheerproces nog steeds voldoet aan de gestelde eisen aan de hand van de acceptatiecriteria voor het betreffende beheerproces. Op basis van het auditverslag stelt de procesmanager een Service Quality Plan (SQP) op voor de gevonden afwijkingen. Na goedkeuring van het SQP door de proceseigenaar rapporteert de procesmanager maandelijks aan de proceseigenaar over de voortgang van het SQP. De procesmanager kan ter verantwoording worden geroepen door de proceseigenaar voor het niet invulling geven van de acceptatiecriteria.

De **procesuitvoerders** geven advies aan de procesmanager ten aanzien van het realiseren van procesverbeterpunten. Hierdoor wordt borging verkregen voor het daadwerkelijk invulling geven aan, en nakomen van de verbeteringen. Zodra het SQP is goedgekeurd door de proceseigenaar zijn de procesuitvoerders degenen die de wijzigingen onder aansturing van de procesmanager doorvoeren.

Conclusie

Bij het uitbesteden van ICT-diensten aan meer leveranciers ontstaan ketens van beheerprocessen. In de praktijk geeft elke leverancier een eigen invulling aan de beheerprocessen binnen zijn eigen beheerdomein. Om de SLA-normen te kunnen realiseren kan een regievoerder aangesteld worden die de beheerprocessen in de ketens op elkaar afstemt. De toegepaste werkwijze van Glidepath is hierbij zeer succesvol gebleken. Het blijkt dat de beheerrequirements een belangrijk hulpmiddel zijn, omdat hierdoor vroegtijdig concreet gemaakt wordt hoe de eindsituatie eruit moet zien. Naast beheerrequirements is het belangrijk om acceptatiecriteria op te stellen waarmee de belangrijkste risico's van een falende beheervoorziening zijn geborgd. Deze kunnen ook periodiek getoetst worden, bijvoorbeeld in een jaarlijkse audit.

Drs. ing. Bart de Best RI (e-mail: bartb@dbmetrics.nl).

Dankwoord

Hierbij dank ik Louis van Hemmen, Said El Aoufi, Fred Ros, Maarten As, Erwin Winkel, Frans Wessels en Thijs van Hofwegen voor hun bijdrage van dit artikel en GlidePath voor het verlenen van hun toestemming tot publicatie van dit artikel.

Noten/literatuur

1. *Drievoudig demand/supply*, IT Beheer Magazine, nr. 10, 2006.
2. *Beheren onder architectuur*, IT Beheer Magazine, nr. 5, 2007.
3. *Beheerarchitectuur in projecten*, IT Beheer Magazine, nr. 8, 2007.
4. *Regie onder beheerarchitectuur*, IT Beheer Magazine, nr. 10, 2007.
5. *Beheerarchitectuur heeft nog een lange weg te gaan*, IT Beheer Magazine, nr. 10, 2007.
6. De Best, Bart, *Acceptatiecriteria*, 2006 ISBN 90 395 2499 8.
7. De Best, Bart, *Ketenbeheer in de praktijk*, 2006 ISBN 9789012116633.