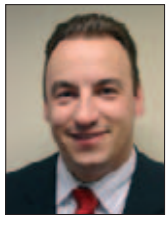
Vrijwillig aan de slag met CobiT

Ondoenlijk of nuttige exercitie?

Leon Dirks, Daniel van Burk, Rocco Jacobs

Over CobiT is sinds de introductie van CobiT 4.0[1] veel geschreven. Het raamwerk, van oorsprong afkomstig uit de auditorswereld, is dankzij Sarbanes-Oxley de laatste jaren flink in populariteit gegroeid. Maar hoe zit het met de toepasbaarheid van CobiT in de praktijk bij een IT-governance verbetertraject? Aan de hand van een casus van het ministerie van VROM gaan we in op de ervaringen die zijn opgedaan met betrekking tot het verbeteren van IT-governance en het gebruik van CobiT hierbij als raamwerk.

Drs. L.G. (Leon) Dirks RE EMIA, Auditor IT bij de Auditdienst van het Ministerie van VROM. Vanuit zijn functie is Dirks als projectleider verantwoordelijk voor de uitvoering van IT audits en adviesopdrachten in multidisciplinaire teams binnen het ministerie van VROM.



Drs. D.E. (Daniel) van Burk CISA, Executive Business Consultant Information Risk Management bij Atos Consulting. Vanuit zijn functie adviseert Van Burk over onderwerpen als IT governance, compliance, security, business continuity management.

Drs. C.L.J.C. (Rocco) Jacobs RE, Senior auditor IT bij de Auditdienst van het Ministerie van VROM. Als senior auditor is Rocco verantwoordelijk voor de coördinatie en de aansturing van het IT audit cluster van de departementale auditdienst van het Ministerie van VROM. Daarnaast is hij als projectleider verantwoordelijk voor de uitvoering van IT audits en adviesopdrachten in multidisciplinaire teams.

De drie auteurs vormden het projectmanagement van het IT-governance project bij het Ministerie van VROM. Zij hebben dit artikel op persoonlijke titel geschreven.

Tot 2004 beschikten de Diensten[2] van VROM elk over een eigen IT-afdeling. Een gezamenlijk IT-beleid ontbrak feitelijk en een CIO-rol was niet onderkend. Binnen *het Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer* (VROM) was een wildgroei aan applicaties ontstaan. Het was zelfs voor de individuele gebruiker mogelijk een applicatie aan te schaffen en deze 'stand alone' te gebruiken. Dit leidde tot een portfolio van meer dan 1.400 applicaties, zo bleek na een inventarisatie. Het behoeft geen nadere uitleg dat deze situatie ongewenst was en een sanering werd ingezet. Na de saneringsslag in 2003 waren er nog zo'n 500 applicaties. Voorts besloot VROM in de periode 2003/2004 een groot deel van haar IT-functie uit te besteden. Het ging hierbij om de uitbesteding van de exploitatie, het technische systeembeheer en het applicatiebeheer. Het functioneel beheer bleef bij VROM. Deze ontwikkelingen gingen gepaard met het reorganisatietraject ZEUS (Zeer Excellente Uitvoering Secundaire processen) dat VROM in 2004 heeft uitgevoerd. Onderdeel van dit reorganisatietraject was een herinrichting van de IT-functie. In figuur 1 wordt het besturingsmodel van de IT-functie na de herinrichting van ZEUS schematisch weergegeven. Hierna zullen we de reorganisatie van de IT-functie kort samenvatten.

Na ZEUS wordt de kaderstelling van IT voortaan centraal geformuleerd door de stafafdeling Personeel, Organisatie en Informatie (POI) en vastgesteld door de plaatsvervangend Secretaris-Generaal in zijn rol als CIO. Binnen de gestelde kaders bepalen de Diensten het informatiebeleid van hun dienst.
Verder beschikken de Diensten op een enkele uitzondering na niet meer zelf over een eigen IT-afdeling en zijn de IT-beheertaken gecentraliseerd in een gemeenschappelijke dienst IT-beheer. IT-advies taken zijn ondergebracht in de VROM Advies- en Expert Dienst (VAED) als onderdeel van de Gemeenschappelijke Dienst.
Een dienst kan IT-expertise inhuren van de VAED om een IT-project, bijvoorbeeld het vervangen van een applicatie, uit te voeren. Elke dienst heeft een informatiemanager die de 'linking pin' vormt met de IT-beheerders, de IT-kaderstellers en de IT-dienstverleners. De I-controller functie is zowel centraal binnen POI als decentraal in de Diensten belegd.

Kortom, ingrijpende veranderingen bij VROM in een periode van twee jaar. De veranderingen grepen fundamenteel in op de IT-governance van VROM. Dit vormde voor de interne Auditdienst van VROM aanleiding om een jaar later de stand van zaken op te nemen. In hoeverre functioneert nu IT-governance als onderdeel van het Management Control Systeem (MCS) uit het oogpunt van beheersing van bedrijfs- en beleidsprocessen? Waar hadden die ingrijpende veranderingen nu in geresulteerd? Was dit nog in lijn met de gedachten van het reorganisatietraject ZEUS? Waren er nog verbeteringen of veranderingen nodig om de IT goed te kunnen beheersen? De Auditdienst begon met het maken van een foto van de beheersing van de IT-functie om de stand van zaken te bepalen.

Gezien de zwaarte van de nog maar recent doorgevoerde veranderingen besloot de Auditdienst niet een audit uit te voeren en een oordeel af te geven maar een onderzoek te doen waarin suggesties tot verbetering of verandering konden worden gedaan. Als referentiekader diende niet alleen het reorganisatiemodel ZEUS maar koos de Auditdienst ook voor CobiT als internationaal geaccepteerd raamwerk voor IT-governance.

Indien de eerste fase van het onderzoek, het maken van een foto, daartoe aanleiding zou geven, zou de tweede fase van het onderzoek worden gestart waarin een gapanalyse wordt uitgevoerd om de verbeteringen in kaart te brengen. Het onderzoek zou dan vervolgens eindigen met een implementatievoorstel voor deze verbeteringen. Op voorhand wist de Auditdienst niet of fase twee en drie überhaupt zouden worden uitgevoerd en in welke vorm.

In het onderstaande wordt het verloop van het onderzoek toegelicht en worden de belangrijkste resultaten samengevat.

Verloop van het onderzoek

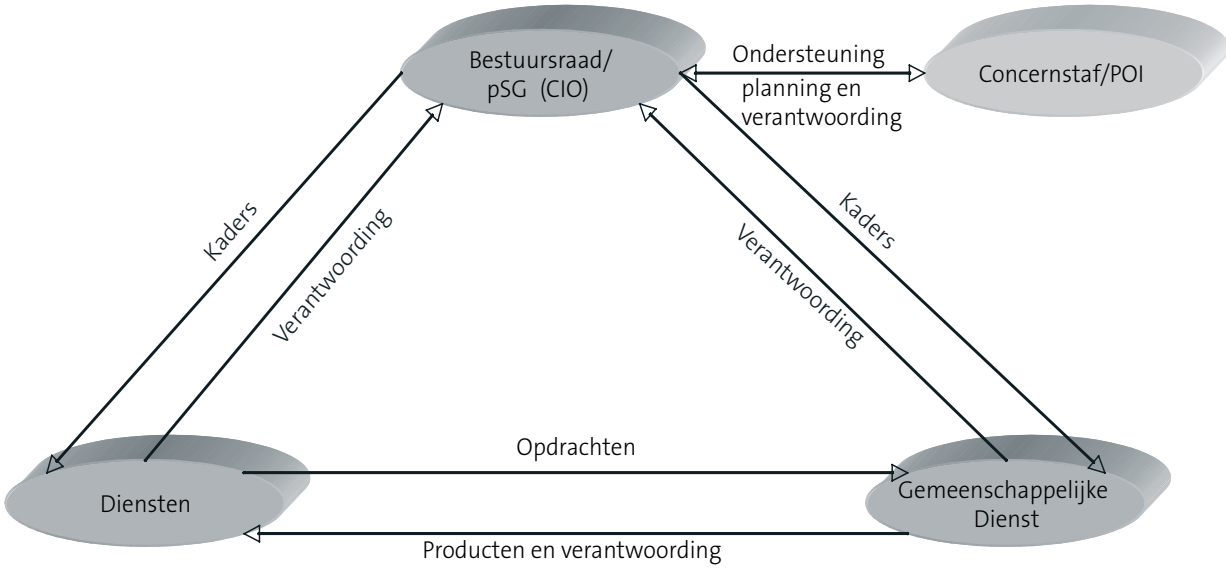
In dit hoofdstuk worden de verschillende fasen van het onderzoek van de Auditdienst nader toegelicht.

Fase 1: Foto

De foto werd gemaakt door alle direct betrokkenen in de I-kolom te interviewen. Dit betrof vertegenwoordigers van de vraagzijde (de Diensten), de aanbodzijde (IT-beheer) en de directie POI als kadersteller. Ook vertegenwoordigers van de financiële kaderstellers Financieel Economische Zaken (FEZ) werden geïnterviewd. Afbeelding 2 van het speelveld van de IT-functie bij VROM na het ZEUS-traject vormde het uitgangspunt voor het vaststellen van de te interviewen personen. In principe is van iedere actor (in het figuur een bol) minimaal één persoon geïnterviewd. Figuur 2 geeft tegelijkertijd een indicatie van de complexiteit van het samenspel van actoren in het beheer van de IT-functie bij VROM.

Basis voor de vragenlijst die bij de interviews werd gehanteerd, vormden de organisatieopzet van de IT-functie na ZEUS (zoals weergegeven in figuur 2) en de vier CobiT-domeinen met de bijbehorende 34 processen. Deze vier CobiT-domeinen zijn door middel van verschillende kleuren ook zichtbaar gemaakt in figuur 2.

De vragenlijst werd bij de interviews niet altijd strikt toegepast. De Auditdienst speelde in op de informatie die in het



Figuur 1 IT-functie VROM en CobiT na ZEUS

interview werd ontvangen en paste vervolgens de vragenlijst aan. Van ieder gesprek is een verslag gemaakt en afgestemd met de geïnterviewde. Indien de geïnterviewde dat wenste, vond nog een gesprek plaats. Daarnaast werd documentatie (bijvoorbeeld de IT-visie van VROM) onderzocht.
Op zich is de aanpak van deze eerste fase niet bijzonder maar in de uitvoering vergde het wel een flexibele opstelling van de onderzoekers zonder de uitgangspunten van het onderzoek geweld aan te doen.
De bevindingen zijn aan het einde van de fase geclusterd naar de vier CobiT kwadranten en grafisch weergegeven in het IT-besturingsmodel van VROM na ZEUS. De aanbevelingen, verdeeld over de korte en de lange termijn, zijn tot stand gekomen door de bevindingen te evalueren ten opzichte van CobiT en het reorganisatiemodel ZEUS. Eén van de aanbevelingen is het advies geweest om CobiT als referentiemodel binnen VROM in te voeren.

Ter afronding van de eerste fase van het onderzoek zijn de resultaten in de vorm van power point slides in concept gepresenteerd aan de plaatsvervangend Secretaris Generaal als CIO van VROM en vertegenwoordigers van POI, FEZ, VAED, IT beheer en de Diensten. De slides van deze presentatie vormden het definitieve rapport dat hierna werd uitgebracht.

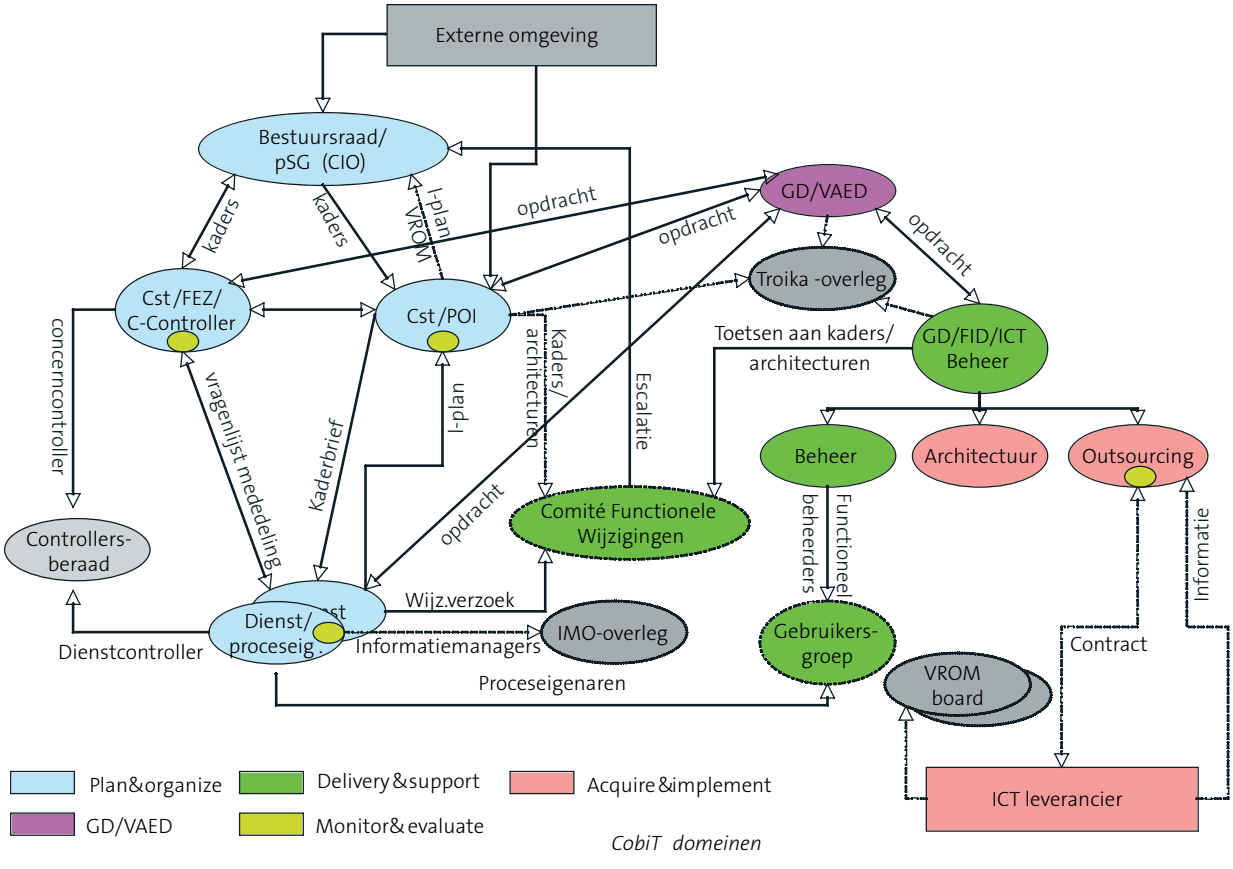
In zijn reactie op de bevindingen, koos de plaatsvervangend Secretaris Generaal voor de invoering van CobiT binnen VROM. De resultaten van het onderzoek werden als afsluiting van deze fase in een breed verband aan VROM gepresenteerd. In deze presentatie zijn tevens de belangrijkste kenmerken van het CobiT-model toegelicht.

Fase 2: Gap-analyse

Beslispunten

De tweede fase bestond uit het in kaart brengen van de IST en de SOLL situatie van de IT-governance binnen VROM voor een beperkt en select aantal IT-processen uit CobiT. In termen van CobiT: door het huidige en gewenste volwassenheidsniveau van een proces te bepalen op een schaal van vijf, ontstaat zicht op de benodigde verbeteringen. De start van de gap-analyse leverde twee beslispunten op:
- De selectie van CobiT-processen.
- Het bepalen van het gewenste volwassenheidsniveau.

Het is natuurlijk een utopie om alle 34 CobiT-processen tegelijkertijd erbij te betrekken. Maar hoe maak je nu een selectie uit 34 IT-processen? Dat vergt een solide afweging want een onterecht geselecteerd proces draagt niet bij aan het realiseren van de projectdoelstellingen. In een workshop met vertegenwoordigers van de Diensten, IT-beheer en POI is een gezamenlijke top-vijf van de grootste ambities en knelpunten van VROM met betrekking tot IT vastgesteld. Op basis van deze informatie deed de Auditdienst in overleg



Figuur 2 Actoren IT-governance VROM

met de VAED een voorstel voor negen CobiT processen die als eerste zouden moeten worden aangepakt. De deelnemers aan de workshop en de CIO bekrachtigden de selectie waaraan de CIO nog een proces toevoegde dat als doel had de communicatie op het gebied van IT te verbeteren.

In figuur 3 staan de CobiT processen vermeld, waarop wij ons binnen VROM hebben gericht.

AI6	Manage changes
PO10	Manage projects
PO1	Define a strategic IT plan
PO2	Define the information architecture
PO5	Manage the IT investment
PO6	Communicate management aims and direction
DS6	Identify and allocate costs
DS1	Define and manage service levels
ME1	Monitor and evaluate IT performance
AI1	Identify automated solutions

Figuur 3: Selectie IT-processen

Het tweede beslispunt was het gewenste volwassenheidsniveau van de geselecteerde processen. De CIO besloot dat het volwassenheidsniveau van de geselecteerde processen binnen anderhalf jaar één niveau hoger moest zijn, ongeacht het huidige volwassenheidsniveau. Het lijkt een kleine stap, 'slechts' één stap hoger, maar het kan een forse inspanning betekenen. Veelal betekent het dat bestaande processen moeten worden aangepast en dat vergt de nodige moeite. Het invoeren van een standaard projectenmethodiek zoals Prince2 betekent dat medewerkers een cursus moeten volgen, een andere werkwijze moeten aanleren, dat een projectenbureau moet worden geïnstalleerd, et cetera. Figuur 4 geeft een impressie van de volwassenheidsniveaus.

Uitvoeren gap-analyse

Workshops waarvoor de al eerder in dit artikel genoemde betrokkenen werden uitgenodigd, speelden een belangrijke rol bij de vaststelling van de gaps. Om de workshops goed voor te bereiden, is telkens aan de hand van een zelf ontwikkelde MS Acces tool het CobiT proces aan elke individuele deelnemer toegelicht. Ook heeft iedere deelnemer door het 'scoren' van volwassenheidskenmerken met behulp van de genoemde MS-Acces tool individueel een volwassenheidsniveau voor het onderhavige CobiT proces vastgesteld.

Vervolgens is in een workshop waarin alle betrokkenen werden uitgenodigd het individuele volwassenheidsniveau veralgemeend zodat een VROM volwassenheidsniveau voor een proces ontstond. In dezelfde workshop is, na de vaststelling van het huidige volwassenheidsniveau, gezamenlijk bepaald welke maatregelen additioneel zouden moeten worden getroffen, danwel zouden moeten worden aangepast om aan de gewenste mate van volwassenheid te kunnen voldoen. De CIO heeft de resultaten van deze tweede fase bekrachtigd.

Fase 3: GRIP

Fase 3 was bedoeld om de verbeterpunten uit fase 2 te realiseren. Feitelijk was dit een separaat project met de naam GRIP: Gemeenschappelijke Realisatie I-Professionalisering. Door de realisatie van de verbeterpunten bereiken de tien geselecteerde processen het volgende volwassenheidsniveau. Figuur 5 toont de verdeling van de tien processen over vier aandachtsgebieden. De verbeteringen zouden fasegewijs worden gerealiseerd.

Inmiddels had de Bestuursraad van VROM besloten om Prince2 als standaard voor projecten binnen VROM toe te passen. De idee daarbij was meteen praktijkervaring op te doen met de toepassing van Prince2. GRIP was in die zin een ervaringsproject. Daarom is voor de start van GRIP een Project Initiatie Document (PID) opgesteld en is conform Prince2 een projectorganisatie opgezet met een stuurgroep waarin zowel de vraagkant (klant) als de aanbodzijde (leverancier) was vertegenwoordigd.

Het voornemen de I-kolom binnen VROM te reorganiseren, deed de CIO besluiten halverwege het eerste deelgebied pas op de plaats te maken met GRIP. Proceseigenaren zijn aangesteld die de resterende activiteiten van het eerste aandachtsgebied moeten realiseren. De acties voor de overige processen werden belegd in de lijn of geparkeerd totdat de ontwikkelingen in de I-kolom zijn afgerond. POI is verantwoordelijk gesteld voor de monitoring van de opvolging van de acties. Begin september 2007 heeft POI voor de eerste keer de verantwoordelijke proceseigenaren aangeschreven om de voortgang inzake de verbeteringen van het eerste aandachtsgebied te melden. Daarnaast heeft POI voor de overige zeven CobiT-processen een voorstel gedaan hoe daarmee moet worden omgegaan in het reorganisatieproces van de I-kolom.

Leerervaringen

Elk van de drie fasen heeft leerervaringen opgeleverd. Deze leerervaringen kunnen we verdelen in ervaringen over het IT-governance traject en het toepassen van CobiT. Deze paragraaf bevat de leerervaringen uit het IT-governance traject. De leerervaringen met CobiT worden uitgewerkt in de paragraaf 'Meerwaarde en valkuilen bij het gebruik van CobiT'.

Hoe pak je het aan?

IT-governance traject

Het traject begon als een IT-governance onderzoek dat werd geïnitieerd door de interne Auditdienst in samenwerking met de stafdirectie POI. Voor de Auditdienst was dit een niet alledaags onderzoek omdat de werkzaamheden normaliter vooral bestaan uit het uitvoeren van audits in het kader van de wettelijke controletaak en op verzoek van het

Maturity level for process XXX IT process	Understanding & Awareness	Training & Communication	Process & Practices	Techniques & Automation	Compliance	Expertise
1. Initial/ad hoc	Recognition	Sporadic communication on issues	Ad hoc approach to process& practice			
2. Repeatable but intuitive	Awareness	Communication on the overall issues and needs	Similar/common but intuitive process emerges	Common tools are appearing	Inconsistent monitoring on isolated issues	
3. Defined process	Understanding of need to act	Informal training supports individual initiatives	Practices are defined, standardized and documented, sharing of better practice begins	Tool set is standardized, currently available practices are used and enforced	Inconsistent monitoring, measurement emerges, balanced scorecard adopted occasionally; root cause analysis is intuitive	Involvement of IT specialists in business processes
4. Managed and measurable	Understand full requirements	Formal training supports a managed programme	Process ownership and responsibilities are set, process is sound and complete, internal best practices are applied	Mature techniques are used, standard tools are enforced, limited tactical use of technology	Balanced score cards are used in some areas, exceptions are noted, root cause analysis is standardised	Involvement of all internal domain experts
5. Optimised	Advanced, forwardlooking understanding	Training and communications support external best practices and use leading edge concepts	Best external practices are applied	Sophisticated techniques are deployed, extensive optimised use of technology	Balanced scorecard is globally applied, exceptions are consistently noted and acted upon, root cause analysis is always applied	Use of external experts and industry leaders for guidance

Figuur 4 Impressie van CobiT volwassenheidsniveaus

management. Nu was er sprake van een onderzoek waarin geen oordeel 'goed' of 'slecht' werd afgegeven maar waarin een 'foto' werd gemaakt van de stand van zaken op basis van CobiT en het reorganisatiemodel dat in 2004 werd gerealiseerd. Op deze wijze werd de CobiT-kennis van de Auditdienst in een adviesrol aangewend ten gunste van de organisatie. Dit bood de Auditdienst de mogelijkheid om zich nog meer als adviseur van het management te profileren en de organisatie maakte kennis met een ongebruikelijke rol van de Auditdienst.

Gewoon beginnen

In de eerste fase van het project zijn we gewoonweg begonnen. We kozen een algemeen bekende IT-beheersingsmethodiek en namen het reorganisatiemodel als tweede referentiekader. Door niet te kiezen voor een selectietraject naar een model boekten we tijdwinst en voorkwamen we een discussie over de geschiktheid van allerlei modellen.
Tijdens het onderzoek stonden we wel open voor eventuele andere modellen die door betrokkenen bij IT-governance konden worden voorgesteld. Dat kon omdat we CobiT niet op een strikte wijze als normenkader hanteerden.

Breed onderzoek

Om een scherpe foto te maken zijn een groot aantal interviews uitgevoerd met VROM functionarissen van zowel de vraagzijde als de aanbodzijde van IT. Op deze wijze ontstaat meer draagvlak voor het onderwerp IT-governance en de methode die in het onderzoek werd toegepast. Nut en noodzaak worden helder voor zover dat nog niet het geval was bij controllers, (informatie-) managers, IT-cluster coördinatoren en projectleiders.

Routebepaling

Selectie van processen

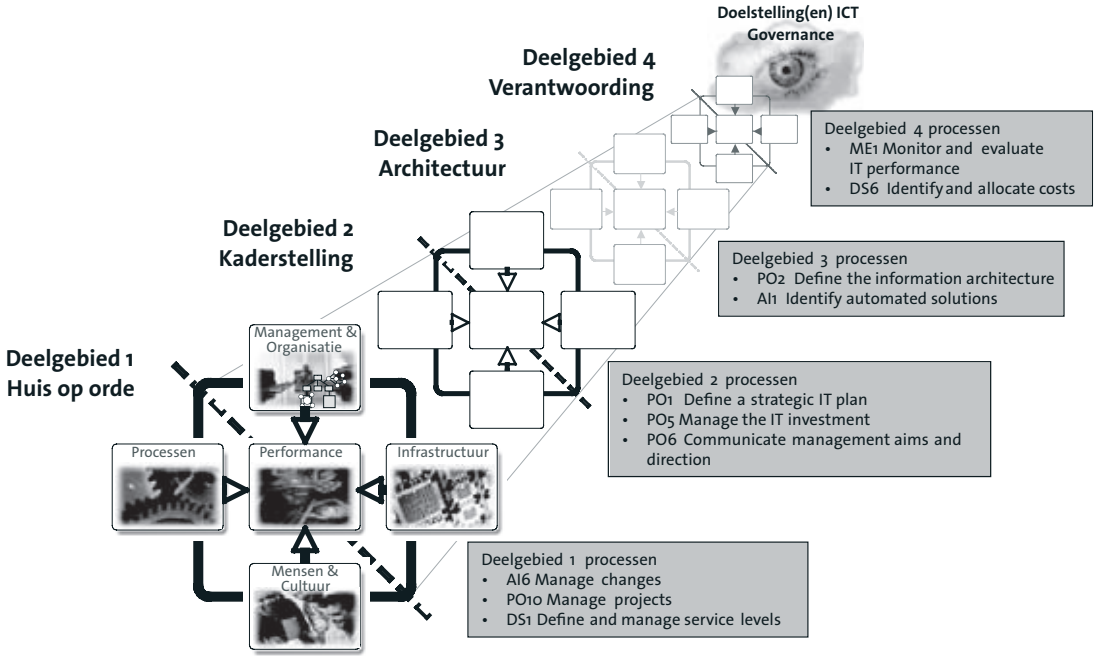
Ook de selectie van IT (CobiT-) processen deden we in samenspraak met een brede VROM-vertegenwoordiging. Door de VROM-medewerkers leading te maken in de processelectie ontstond een breed draagvlak in de organisatie om deze processen te verbeteren.

Complexe materie

Het vaststellen van volwassenheidsniveaus is niet eenvoudig. Enerzijds is het scoren van de volwassenheid op basis van stellingen een kwalitatieve beoordeling, anderzijds streefden we wel naar onderlinge vergelijkbaarheid. We hebben gebruik gemaakt van de wegingen van stellingen die door de vakorganisatie ISACA zijn opgesteld om de resultaten van de interviews onderling vergelijkbaar te maken, terwijl we ervoor waakten om niet te vervallen in mathematische gemiddelden, dit zou enkel schijnzekerheid opgeleverd hebben. Scores werden dus 'slechts' als een indicatie van het volwassenheidsniveau gezien. De echte vaststelling van het volwassenheidsniveau vond plaats door de VROM vertegenwoordigers in de eerdergenoemde workshop over een proces.

Samenwerking tussen vraagzijde en aanbodzijde IT

Zowel de vraagzijde als de aanbodzijde van IT waren in de workshops vertegenwoordigd. Dit had een positieve impact op de samenwerking en de communicatie tussen deze twee zijden van IT. De gebruikers kwamen in gesprek met de IT-ers.



Figuur 5 Vier aandachtsgebieden

De organisatie staat niet stil

Open oog voor veranderingen

In de derde fase moesten de acties worden uitgevoerd om een volgend volwassenheidsniveau te bereiken. Al vrij snel bleek echter dat ontwikkelingen in de I-kolom binnen VROM ertoe leidden dat het nodig was om de acties uit het GRIP project anders te beleggen. Een reorganisatie binnen de I-kolom van VROM was namelijk op komst. Voor een deel van de acties was het mogelijk of nodig deze alsnog uit te voeren dan wel te beleggen bij andere projecten. Een ander deel van de acties kon pas worden uitgevoerd nadat het stof in de I-kolom was neergedaald. Het is van belang dergelijke ontwikkelingen tijdig te onderkennen en de impact hiervan op een IT governance project vast te stellen.

Prince2

VROM besloot de methodiek Prince2 als standaard in te voeren voor de organisatie en aansturing van haar projecten. Daarom diende het GRIP project in lijn met de Prince2 standaard opgezet te worden. Dat betekende ook dat de Stuurgroep niet alleen kennis diende te hebben van CobiT maar ook van Prince2. En dat bleek in de praktijk een lastige combinatie. Het onderwerp IT governance was beter behapbaar geweest voor de Stuurgroep als we niet voor deze combinatie hadden gekozen.

Samenstelling stuurgroep

De stuurgroep bestond uit twee vertegenwoordigers van de IT-organisatie en twee vertegenwoordigers uit de Diensten, naast een voorzitter en een secretaris. De twee vertegenwoordigers uit de Diensten gaven aan IT-governance en CobiT vooral te zien als onderwerpen die behoorden bij de IT-organisatie. Dat betekent dat de gebruikers een andere rol wilden vervullen dan als lid van de stuurgroep. De vertegenwoordigers van de Diensten voelden zich meer thuis in een klankbordgroep.

Meerwaarde en valkuilen bij het gebruik van CobiT

Bij het doen van het onderzoek naar IT-governance binnen VROM is zoals aangegeven gebruik gemaakt van CobiT 4.0. Tijdens dit traject hebben we in de praktijk een aantal meerwaarden en valkuilen van CobiT onderkend.

Meerwaarde van CobiT

Paraplufunctie

CobiT kent als een van de weinige modellen een scope waarbinnen elementen als strategie, ontwikkeling, beheer en beveiliging opgenomen zijn, zij het op een redelijk hoog (abstractie)niveau. Dit in tegenstelling tot modellen als ITIL, ASL en BiSL die zich meer op beheer richten, CMM dat zich meer op ontwikkeling richt en de Code voor Informatiebeveiliging die, zoals de naam al aangeeft, primair gericht is op beveiliging. Door deze brede scope en het hoge abstractieniveau leent CobiT zich uitstekend om als een soort paraplu te dienen waarmee de samenhang gezocht kan worden en het totaalbeeld gevormd kan worden ten aanzien van modellen die reeds bij een organisatie in gebruik zijn. Daarbij moet soms wel een vertaling worden gemaakt van bijvoorbeeld ITIL-processen naar processen binnen CobiT. Bij VROM werd al gebruik gemaakt van modellen als ITIL, ISPL, BiSL en Prince2. Het gebruik van CobiT voor het in kaart brengen van de IST en SOLL situatie voor verschillende processen gaf het voordeel dat de diverse processen op

een uniforme manier benaderd konden worden in de workshops.

Gemeenschappelijk begrippenkader

Door de steeds bredere acceptatie van CobiT (zowel binnen als buiten de audit-wereld) heeft CobiT de potentie om als gemeenschappelijk begrippenkader te dienen dat de organisatie kan gebruiken in de communicatie over IT gerelateerde processen in een organisatie. Dit voorkomt veel begripsverwarring. Binnen het project bij VROM hebben we gemerkt dat het consequent vasthouden aan het CobiT begrippenkader goed werkte om snel tot inzicht en resultaten te komen. Ook het feit dat betrokkenen bij de vraag- en aanbodzijde van de informatievoorziening binnen hetzelfde begrippenkader met elkaar praten was directe winst.

Volwassenheidsniveaus

Om een goed beeld te krijgen van de huidige situatie ten aanzien van processen en een groeipad te kunnen definiëren is het prettig dat CobiT 4.0 per proces volwassenheidsniveaus heeft gedefinieerd met stellingen die ieder volwassenheidsniveau beschrijven. Hierbij moeten meteen wel een paar kanttekeningen worden geplaatst.

Bij methodieken, waarmee je kunt scoren, ligt altijd het risico van een al te mathematische benadering op de loer. De scores moeten geen eigen leven gaan leiden, zeker niet als er gemiddelden berekend gaan worden van de scores die verschillende stakeholders aan het proces hebben toegekend. Het blijft een kwalitatieve benadering.

Ook is het onze ervaring dat de eisen die aan processen worden gesteld voor bepaalde volwassenheidsniveaus nog al eens uit elkaar lijken te lopen. Voor het ene proces haal je veel makkelijker volwassenheidsniveau 3 dan voor een ander proces. Het is weliswaar appels met peren vergelijken, maar het geeft wel aan dat de volwassenheidsniveaus niet al te absoluut kunnen worden beschouwd.

Valkuilen bij het gebruik van CobiT

Het is slechts een model

Modellen zijn vereenvoudigde weergaven van de werkelijkheid en zijn geldig onder bepaalde condities. Daarom moet je uitkijken voor het dogmatisch toepassen van een model en dit geldt ook voor CobiT. Dit lijkt een open deur, maar het gebeurt nog steeds dat een model gebruikt wordt als argument om iets wel of niet te doen. In het project hebben we scherp gekeken naar de achterliggende doelstellingen van het professionaliseren van de informatievoorziening op basis van de belangrijkste ambities en issues die er waren. Dit heeft erg geholpen om met de juiste focus naar processen te kijken en ook bewust elementen eruit weg te laten die niet dienstbaar waren aan de doelstellingen van het project. Het proces PO6 Communicate Management Aims and Direction bijvoorbeeld was in de scope geplaatst om te borgen dat de communicatie ten aanzien van IT governance voldoende aandacht kreeg in het project en daarna in de staande organisatie. We hebben daarom vooral gekeken naar de Key Performance Indicators / Key Goal Indicators en detailed control objectives die gericht waren op het verhogen van bewustzijn van en draagvlak voor IT-governance, en niet zozeer naar de detailed control objectives die betrekking hebben op de beheersing van de communicatie.

Hoogste volwassenheidsniveau is niet zaligmakend

Volwassenheidsniveaus en groeimodellen kunnen impliciet leiden tot een houding waarbij automatisch naar het hoogste volwassenheidsniveau wordt gestreefd. De vraag is echter of dit altijd gewenst en bedrijfseconomisch verantwoord is. Er moet vooral gekeken worden naar de eisen die aan het proces worden gesteld vanuit de omgeving en het daarbij behorende volwassenheidsniveau. Tevens moet goed rekening worden gehouden met wat de organisatie aankan qua veranderingen en in relatie tot de volwassenheid op andere onderdelen. In ons project is ervoor gekozen om te streven naar een verhoging van de volwassenheid met 1 niveau en om daarna, gegeven de situatie op dat moment, te evalueren of verder groei in volwassenheid noodzakelijk is. Dit heeft geholpen om de ambities tot een realistisch niveau te beperken.

Gebruik van CobiT is niet geïntegreerd in organisatie

De meerwaarde van CobiT zoals eerder beschreven kan alleen ten volle worden uitgebaat als de hele organisatie ermee gaat werken. Wanneer het binnen het domein van bijvoorbeeld de Auditdienst blijft zal er geen gemeenschappelijk begrippenkader ontstaan en kan er niet over meer processen op een eenduidige wijze een verbeterplan worden opgesteld. Het intensief betrekken van zowel de aanbodzijde, de beleidsmakers als de vraagzijde van IT heeft ertoe geleid dat er op het juiste niveau en met de juiste gezichtspunten naar de professionalisering kon worden gekeken en heeft bijgedragen aan het creëren van draagvlak voor het realiseren van verbeteringen.

Conclusies

In de VROM casus is CobiT als hulpmiddel toegepast in een IT governance traject. Hierbij is gebleken dat CobiT door zijn brede scope goed hanteerbaar is om de IT-governance in kaart te brengen. De relatief beperkte diepgang van CobiT (er wordt vooral aangegeven wat er geregeld moet zijn, niet zozeer hoe dit geregeld moet worden) biedt tevens de mogelijkheid om aan te sluiten op (reeds in gebruik zijnde) modellen als ITIL en Prince2. Het feit dat CobiT niet van buitenaf of van bovenaf is opgelegd (dit traject is niet geïnitieerd omdat wet- en regelgeving het departement hiertoe verplichtte) heeft in dit project positief uitgewerkt. VROM wenste zelf meer zicht te krijgen op de stand van zaken betreffende de beheersing van IT. Dit vormde de startpositie om vast te stellen of verbeteringen nodig waren gelet op ontwikkelingen in de nabije toekomst en geconstateerde knelpunten.

Om meer redenen is het gebruik van CobiT een nuttige exercitie geweest. Het is een alom geaccepteerd raamwerk dat houvast bood aan de deelnemers aan het project. Wel vergt het toepassen van CobiT een kritische houding. Niet alle stellingen en control objectives bijvoorbeeld zijn van toepassing op VROM. Ook zijn niet alle CobiT processen even goed uitgekristalliseerd.

CobiT wordt door veel organisaties gebruikt. Dat heeft als voordeel dat veel kennis en ervaring in het toepassen van het raamwerk in het bedrijfsleven beschikbaar is. ISACA heeft een actieve CobiT community. Deze kennis en ervaring zijn ook nuttig gebleken voor de Rijksoverheid.

Toch kan het toepassen van CobiT ook zomaar ondoenlijk worden. Indien alle CobiT-processen tegelijkertijd worden aangepakt is het risico groot dat de organisatie het overzicht verliest. Ook het te strikt hanteren van het raamwerk en het niet voldoende vertalen van de methode naar de situatie van een organisatie kan leiden tot een mislukking van een IT governance traject. Pas daarom CobiT toe met de nodige voorzichtigheid en benader de methode voldoende kritisch. Het is slechts een methode, die je als hulpmiddel kan gebruiken om je ICT op een hoger plan te brengen. CobiT moet niet als een doel op zich worden gehanteerd. ■

Noten

1 Inmiddels is CobiT 4.1 verschenen

2 Een dienst is een zelfstandige organisatorische eenheid binnen het ministerie, te vergelijken met een divisie binnen een grote onderneming