Beheer van IT vergt discipline

Mw. J.A.M. Holla RE en drs. M.T.J.M. Piels

Het beheer van IT wordt voor steeds meer organisaties een vitale rol als het gaat om de continuïteit van de bedrijfsvoering en het verkrijgen van concurrentievoordeel. In het algemeen wordt ingeschat dat ongeveer tachtig procent van de kosten van informatiesystemen niet meer in systeemontwikkeling zit maar in beheer en exploitatie. Toch blijkt uit de praktijk dat het beheer nog steeds onderbelicht is. In dit artikel wordt een benadering voor het verbeteren en optimaliseren van het beheer van IT beschreven, waardoor IT inderdaad door organisaties als strategisch wapen kan worden ingezet.

Inleiding

Al jaren wordt er, in de diverse literatuur, gesproken over de toenemende mate van automatisering binnen organisaties. Hierbij gaat het niet meer alleen om het (deels) automatiseren van de ondersteunende bedrijfsprocessen in organisaties, maar om het automatiseren van de primaire bedrijfsprocessen. Voorbeelden hiervan zijn de talloze ERP-projecten (Enterprise Resource Planning) waardoor het primaire bedrijfsproces grotendeels afhankelijk is geworden van de geautomatiseerde gegevensverwerking, kortweg IT (informatietechnologie).

De toenemende afhankelijkheid van IT is een ontwikkeling die niet meer valt terug te draaien. Deze afhankelijkheid vraagt om adequate (aan)sturing van het management over de toe te passen automatiseringsvormen. Tevens wil het management gerust worden gesteld over het beheer van de aanwezige IT. De mate van professionaliteit van het beheer van de IT bepaalt namelijk in grote mate de toepasbaarheid van IT als strategisch wapen.

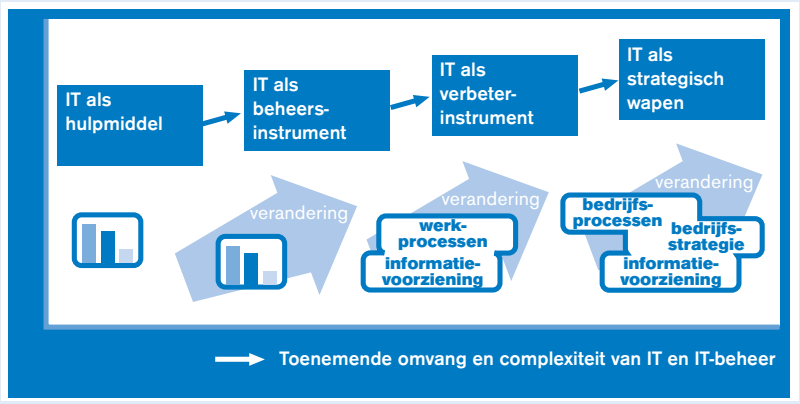
In dit artikel wordt op dit laatste aspect nader ingegaan, waarbij zal worden aangetoond dat het periodiek uitvoeren van een technical audit een positieve bijdrage levert aan het verbeteren van het beheer van de IT, met als gevolg dat het primaire bedrijfsproces in organisaties eveneens stabieler wordt uitgevoerd. Daarnaast zal het werk van de accountant enigszins worden vereenvoudigd, doordat tevens met deze benadering de general IT controls grondig worden onderzocht. Technical auditing op basis van beheerdisciplines omvat namelijk audits waardoor de factor tijd (werking) aan het oordeel kan worden toegevoegd.

Om bovenstaande stelling te onderbouwen is gekozen voor de volgende indeling van het artikel. Eerst wordt stilgestaan bij het toenemende belang van IT voor organisaties. Vervolgens wordt beschreven waarom het toenemende belang van IT leidt tot een toenemend belang van beheer van IT. Om het auditen van het beheer van IT in een context te plaatsen wordt de positie aangegeven die technical auditing inneemt in het vakgebied van IT-auditing. De kern van dit artikel bestaat uit de beschrijving van de auditaanpak die KPMG EDP Auditors (KEA) hanteert bij het uitvoeren van technical audits, waarbij wordt gesteund op een procesgerichte benadering. Daarna worden aan deze benadering handen en voeten gegeven met een aantal, uit de praktijk, aansprekende voorbeelden van technical audits. Ten slotte wordt beschreven op welke wijze de KEA-benadering van technical auditing een positieve bijdrage kan leveren aan het verbeteren (professionaliseren) van het beheer van IT. Doordat een effectievere en efficiëntere invulling aan het beheer van de IT kan worden gegeven, kunnen de primaire bedrijfsprocessen ongestoord hun voortgang hebben, ondersteund met behulp van een stabiele IT-omgeving.

Belang van IT voor een organisatie

IT is een niet meer weg te denken fenomeen in onze samenleving. We begeven ons in een turbulent tijdperk, waarbij markten in beweging zijn en IT zich in een hoog tempo ontwikkelt. De ontwikkelingen op het gebied van de IT hebben gezorgd voor een groot aantal veranderingen. IT is een onmisbaar hulpmiddel bij de informatieverzorging binnen en tussen organisaties. Bij het toepassen van IT werd al snel gedacht aan IT als hulpmiddel bij de uitvoering van routinematige en arbeidsintensieve productieprocessen. Met de automatisering daarvan kunnen de grootste besparingen worden gerealiseerd. Daarnaast wordt IT al geruime tijd als beheerinstrument gebruikt. Ondersteunende bedrijfsprocessen (financiële administratie en personeelszaken) zijn in de meeste organisaties als eerste geautomatiseerd.

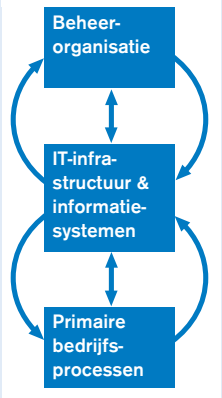
Echter, IT wordt tegenwoordig steeds meer gebruikt om de primaire bedrijfsprocessen en besturende processen te verbeteren. Het verbeteren van de ondersteuning aan afnemers, leveranciers en medewerkers staat hierbij voorop. IT wordt steeds vaker gebruikt om de organisatie in staat te stellen flexibel te kunnen reageren op veranderende (markt)omstandigheden. Door de kansen te benutten die door IT worden aangereikt, kan een organisatie de concurrentie een stap voor blijven. Daarmee is de IT in toenemende mate van invloed op het bedrijfsresultaat. Met andere woorden, IT biedt de organisatie kansen om innovatiever te worden. IT is daarmee een strategisch wapen geworden.



Figuur 1. Groeifasenmodel.

Het op meerdere gebieden inzetten van IT kan worden gezien als een groeiproces met een toenemende omvang en complexiteit. Door de enorme snelheid waarmee de ontwikkelingen in de IT plaatsvinden, is het juiste gebruik hiervan voor veel organisaties geen gemakkelijke taak. De combinatie van het groeiproces met een toenemende omvang en complexiteit met het strategisch belang voor de organisatie rechtvaardigt de aandacht van het management voor de kwaliteit van de informatievoorziening op de korte én de lange termijn. Alleen aandacht besteden indien zich problemen aandienen, is niet meer toereikend; een vaak onoverkomelijke achterstand is dan opgelopen. Daarnaast vraagt iedere wijze van inzet van IT om haar eigen sturingsmethoden. Management en beheersing van IT worden van essentieel belang voor de effectiviteit en slagvaardigheid van een organisatie.

Kortom, voordat een organisatie IT wil inzetten als strategisch wapen en het gebruik van IT derhalve laat groeien, dient de organisatie zorg te dragen voor een stabiele IT-omgeving. Dit kan worden bereikt door het adequaat inrichten van het beheer van de IT-omgeving. Het belang van de professionalisering van het beheer van de IT neemt toe naarmate een organisatie afhankelijker wordt van de IT.



Figuur 2. Samenhang beheer IT en primaire bedrijfs-processen.

Belang van adequaat beheer van IT

Om IT als strategisch wapen te kunnen inzetten moet de organisatie bepaalde doelstellingen hebben. Om deze te verwezenlijken zal de organisatie een aantal (bedrijfs-) activiteiten uitvoeren. Ter ondersteuning van deze activiteiten zal gebruik worden gemaakt van één of meer informatiesystemen. De onderliggende componenten waarop deze informatiesystemen draaien wordt de IT-infrastructuur genoemd. De IT-infrastructuur kan worden gezien als opgebouwd uit technologische componenten, systeem- en toepassingssoftware, procedures en documentatie. Om de IT-infrastructuur te beheren en daarmee de bedrijfsactiviteiten te ondersteunen is een adequate beheerorganisatie noodzakelijk. In figuur 2 is het verband tussen deze componenten weergegeven.

Ofwel, indien een organisatie IT als strategisch wapen wil inzetten, neemt het belang van het beheer van de IT steeds meer toe.

Bedrijven worden steeds meer afhankelijk van automatisering en veranderingstrajecten met betrekking tot de automatisering kennen een steeds snellere levenscyclus. Hierdoor is het van belang dat de organisatie kan steunen op adequate procedures en richtlijnen voor het beheren van de reeds aanwezige IT. Indien de aanwezige IT op een zorgvuldige manier in de hand kan worden gehouden, is de kans groot dat nieuwe componenten (hardware, software en informatiesystemen) gemakkelijker worden geïntegreerd. Daarnaast is het met een, steeds verdergaande, 7×24-uurssamenleving van belang dat de IT te allen tijde beschikbaar is.

Genoemde ontwikkelingen onderschrijven het belang van het beheer van IT en het is dan ook begrijpelijk dat de laatste jaren steeds meer tijd en moeite worden besteed aan het zo effectief en efficiënt mogelijk beheren van de aanwezige IT. Deze IT bestaat bij de meeste organisaties uit diverse platformen (mainframe, midrange en desktop) en IT-componenten (netwerk, hardware, software, etc.) van diverse leveranciers, waarbij bewezen technologie vaak samen wordt gebruikt met allerlei nieuwe ontwikkelingen. De vraag die bij veel organisaties leeft, is: 'Hoe kan zo effectief en efficiënt mogelijk worden omgegaan met het beheer van de multivendor, multiplatform automatisering?'

In een artikel ([Vogd98]) van de voorzitter van de belangenvereniging IT Service Management Forum (itSMF) staat beschreven dat het leeuwendeel van de kosten van IT in beheer en exploitatie zit. Daarnaast worden zowel kleine als grote ondernemingen zo afhankelijk van IT dat adequaat beheer en exploitatie van IT primaire voorwaarden zijn om te overleven. De komende drie jaar zullen de investeringen in IT-beheer minstens verdubbelen. Ongeveer tachtig procent van de kosten van IT zit niet meer in systeemontwikkeling (SO), maar in beheer en exploitatie.

Om bovenstaande problemen te kunnen ondervangen dient aan het beheer van de IT een professionele invulling te worden gegeven. Een professionele invulling zodat IT uiteindelijk kan worden ingezet als strategisch wapen in de toenemende concurrentiestrijd op de diverse afzetmarkten. Daarnaast kan door gestructureerd en permanent invulling te geven aan beheer van IT op de middellange termijn kostenvoordeel worden behaald, doordat niet continu achter de feiten wordt aangelopen (ofwel geen onvoorziene situaties ontstaan) en in plaats van correctieve (veelal op ad-hocbasis, snel en ondoordacht inpassen van meestal duurdere oplossingen) preventieve beheermaatregelen kunnen worden genomen.

Deze doorvoering van gestructureerd en gestandaardiseerd beheer van IT kan zelfs leiden tot een voordeel ten opzichte van de concurrenten in de branche waarin de organisatie actief is. Een geslaagde introductie van veel nieuwe producten en/of diensten wordt (met name in de dienstverlenende branches) veelal bepaald door een goede ondersteuning van de automatisering, daar de bedrijfsprocessen en ondersteunende automatisering veelal één geïntegreerd geheel vormen. Om als management te kunnen rekenen op de ondersteuning van een adequate automatisering is het van belang het beheer optimaal in te richten zodat voor nieuwe automatise-

ringsdeelgebieden reeds een stevige beheerbasis aanwezig is. Zolang de beheerorganisatie zelf nog niet in een stabiele situatie is terechtgekomen, zullen de noodzakelijke wijzigingen in de IT niet probleemloos kunnen worden ingevoerd.

De IT-beheerorganisaties zijn derhalve in een continu proces verwikkeld van het optimaliseren en perfectioneren van het beheer van de IT. Veelal zullen deze organisaties hun activiteiten proberen onder te brengen in een algemeen geaccepteerd denkkader zoals ITIL (Information Technology Infrastructure Library), of een soortgelijk implementatiemodel van IT-beheerprocessen. Het management van de organisatie heeft echter vaak geen idee van de mate van professionaliteit van het beheer en het groeipad van de IT-beheerorganisatie naar een toegevoegde waarde in de toenemende concurrentiestrijd.

Plaats van technical auditing in het vakgebied IT-auditing

Het belang van adequaat beheer van IT neemt, zoals gezegd, voortdurend toe en daarom zal en moet het management op de hoogte blijven van de kwaliteit van het beheer. Het is derhalve gewenst om vanuit een onafhankelijk oogpunt te kijken naar de ontwikkelingen van het beheer. Door te laten beoordelen hoever de IT-beheerorganisatie nog is verwijderd van het gewenste niveau van beheer, kan het management van een organisatie bijvoorbeeld bepalen of IT inderdaad als strategisch wapen kan worden ingezet.

Om informatie te kunnen leveren over de kwaliteit van de beheerorganisatie biedt technical auditing het management de mogelijkheid een vinger aan de pols te houden. Dit wordt mogelijk gemaakt door het uitvoeren van audits naar de inrichting en werking van de aanwezige beheerdisciplines aangevuld met audits op de technische implementaties. De doelstelling van de beoordeling van de technische implementaties is vast te stellen of de aanwezige beheerdisciplines juist zijn vertaald in de techniek. Onderstaand zal worden beschreven welke positie dit soort onderzoeken inneemt in het brede IT-auditvakgebied.

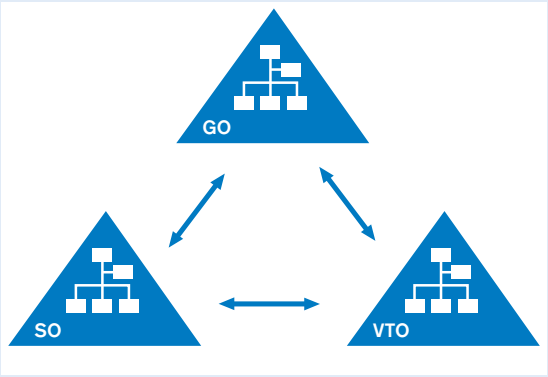
Het vakgebied IT-auditing behelst het door een onpartijdige deskundige kritisch beoordelen van (en adviseren over) de kwaliteit van de organisatie van de automatisering. Met andere woorden, het betreft een breed scala van onderwerpen die zijn gerelateerd aan de kwaliteit van het beheer van de IT. Om de onderzoeken van dit brede vakgebied enigszins te kunnen classificeren kan onderscheid worden gemaakt in drie typen functionele organisaties, die onderstaand worden beschreven.

Als eerste functionele organisatie is te onderkennen de zogenaamde gebruikersorganisatie (GO). Deze organisatie wordt gezien als de afnemer van de automatisering. Alle automatiseringsactiviteiten worden voor deze functionele groep uitgevoerd. Zij werken met de eindproducten van de automatisering ter ondersteuning (of deels vervanging) van de primaire bedrijfsprocessen. Vaak wordt de term eindgebruikersorganisatie als synoniem gehanteerd. De gebruikersorganisatie geeft door middel van functionele eisen aan de automatisering (in)direct sturing aan de beide andere functionele organisaties.

Door het gebruik van automatisering binnen de GO ontstaat een tweede functionele organisatie om de gegevensverwerking alsmede de informatieverstrekking te verzorgen (de verwerkende en transporterende organisatie: VTO). De VTO heeft naast haar gegevensverwerkende en informatieverstrekkende taak tevens een bewarende taak en een taak ten aanzien van datacommunicatie. De data (opgenomen in bestanden/files) van de gebruikers worden bij de VTO in bewaring gegeven. Het is een organisatie met eigen verantwoordelijkheden en bevoegdheden. Aan deze organisatie worden vanuit de GO eisen gesteld waaraan ze dient te voldoen. Daarnaast stelt de VTO zelf eisen aan haar organisatie (ze heeft immers eigen bedrijfsdoelstellingen).

De derde functionele organisatie die bij gebruik van automatisering/informatietechnologie ontstaat is de organisatie voor systeemontwikkeling (applicatieontwikkeling) en systeemonderhoud (SO). Een organisatie die in opdracht van de GO applicaties ontwikkelt en onderhoudt. Ook dit is een organisatie met eigen verantwoordelijkheden en bevoegdheden. In veel gevallen bestaat deze organisatie uit een zogenaamde projectorganisatie.

De VTO- en SO-organisatie zijn al dan niet geïntegreerd met (delen van) de GO-organisatie zowel op het strategische, tactische als het operationele niveau. In een kleinschalige organisatie zal meestal sprake zijn van volledige integratie. Uit het oogpunt van beheersing is het echter noodzakelijk inzicht te hebben in de scheiding van taken, bevoegdheden en verantwoordelijkheden tussen de drie beschreven functionele organisaties. In figuur 3 worden de relaties tussen deze functionele organisaties weergegeven.



Figuur 3. Relaties tussen de functionele organisaties.

Samengevat kan het volgende worden gesteld:
* In geval van automatisering is sprake van minimaal drie functionele organisaties, de gebruikersorganisatie (GO), de systeemontwikkelings- en onderhoudsorganisatie (SO) alsmede de gegevensverwerkende, informatieverstrekkende en gegevenstransporterende organisatie (VTO).
* De VTO verwerkt, transporteert en bewaart gegevens en verstrekt informatie ten behoeve van de GO, de SO en de VTO.

* De SO ontwikkelt en onderhoudt geautomatiseerde toepassingen ten behoeve van de GO, de SO en de VTO.
* De drie organisaties stellen eisen aan de eigen interne organisatie.
* Elk van de drie organisaties stelt eisen aan de andere twee organisaties.

Technical auditing richt zich op de VTO-organisatie. Dit betekent dat de kwaliteit van de VTO-beheerorganisatie, de relaties tussen de VTO- en GO-organisatie, de relatie tussen de VTO- en SO-organisatie en de door de VTO-organisatie beheerde technische objecten/implementaties worden beoordeeld.

Technical auditing KPMG EDP Auditors

Zoals in de inleiding staat vermeld, zal worden aangetoond waarom technical auditing een positieve bijdrage kan leveren aan het optimaliseren van het beheer van IT. Daarvoor is door KEA een auditaanpak ontwikkeld, gebaseerd op beheerdisciplines, die binnen KEA bekend staat onder de naam piramidemodel. Met dit model kan ondersteuning worden geleverd bij het professionaliseren van het beheer van IT. Deze aanpak wordt onderstaand uiteengezet.

Piramidemodel

Het piramidemodel is gedurende de afgelopen twee jaar ontwikkeld door medewerkers van KEA en wordt op basis van voortschrijdend inzicht continu onderhouden. Op dit moment wordt het model bij een toenemend aantal klanten toegepast bij het uitvoeren van onderzoeken, maar ook voor het opstellen van normen, procedures en standaarden voor het inrichten van IT-beheerorganisaties.

In het model is gebruikgemaakt van bestaande modellen, raamwerken en standaarden in het vakgebied, zoals de IT Infrastructure Library ([ITIL90]), het CobIT-raamwerk en de Code voor Informatiebeveiliging.

Doel van het piramidemodel is een overzicht te geven van een groepering van beheeractiviteiten die bij een beheerorganisatie moeten zijn ingericht.

De beheerdisciplines in het piramidemodel beschrijven beheerprocessen en -activiteiten die op een of andere manier binnen iedere IT-organisatie moeten worden onderkend, onafhankelijk van de grootte van de organisatie, de klantenkring of de gehanteerde werkwijze binnen de organisatie. De beheerdisciplines worden daarom onafhankelijk van de personele en organisatorische invulling behandeld. Dit betekent niet dat bij het uitvoeren van een audit geen rekening wordt gehouden met de minimaal benodigde controletechnische functiescheiding.

Doel van het raamwerk is een overzicht te geven van een groepering van beheeractiviteiten die bij een beheerorganisatie moeten zijn ingericht, zodat bij juiste uitvoering van de activiteiten daadwerkelijk sprake kan zijn van professioneel IT-beheer. Hiervoor is een indeling in twaalf beheerdisciplines gekozen waarmee de EDP-auditor tot een evenwichtig onderzoek met voldoende breedte en diepgang kan komen.

Het raamwerk van beheerdisciplines mag niet worden gezien als een strak keurslijf. Het is een flexibel raamwerk waarbij, indien gewenst, beheerdisciplines kunnen opgaan in andere beheerdisciplines of de naamgeving van de beheerdisciplines anders kan luiden. Het is bijvoorbeeld mogelijk tien beheerdisciplines aan te treffen indien een organisatie ervoor heeft gekozen de beheerdisciplines capacity, workload en performance gemeenschappelijk te zien als ‘efficiënt systeemgebruik’.

Een valkuil bij het gebruik van het model is dat de organisatie een proces kan hebben ingericht met een gelijke naamgeving aan één van de twaalf beheerdisciplines maar met een andere scope. Om spraakverwarring te voorkomen dient bij ieder onderzoek aandacht te worden besteed aan de afbakening van de beheerdisciplines en de opsplitsing van het beheer in de organisatie.

Kortom, de piramide is een hulpmiddel waarmee alle beheeractiviteiten van de beheerorganisatie met een in verhouding gelijke diepgang worden beoordeeld. Niet de twaalf disciplines moeten in een organisatie herkenbaar zijn maar wel alle in het piramidemodel onderkende beheeractiviteiten dienen in de organisatie te zijn ingericht.

De beschrijving van de beheerdisciplines

Een korte beschrijving van elke beheerdiscipline en de daarmee samenhangende beheeractiviteiten alsmede de formele definities die worden gehanteerd, volgt hieronder.

IT Policy and Organisation

Alvorens een beheerorganisatie (VTO) op te zetten en te starten met het uitvoeren van IT-beheeractiviteiten zal het doel (het missiestatement) van de organisatie moeten worden bepaald. Dit doel wordt in het beleid vertaald naar een verzameling (deel)doelstellingen, waarin het management enerzijds aangeeft wat het wil bereiken en anderzijds de uitgangspunten en richtlijnen aangeeft die daarbij in acht moeten worden genomen. Alle activiteiten binnen de beheerorganisatie zullen op zodanige wijze moeten worden uitgevoerd dat het doel zo optimaal mogelijk wordt bereikt.

Door het opstellen van een beleid voor elk van de afzonderlijke beheerdisciplines (clustering van een aantal beheeractiviteiten) zal de IT-policy verder worden uitgewerkt. Het is van groot belang dat het beleid op schrift wordt gesteld en dat dit document wordt verstrekt aan alle belanghebbende onderdelen van het bedrijf. Bovendien moet het beleid up-to-date worden gehouden en het document regelmatig worden bijgewerkt. Merk op dat IT Policy and Organisation een overkoepelende beheerdiscipline van alle andere beheerdisciplines is. Het geeft

richting aan, en heeft dus ook een relatie met de overige (elf) beheerdisciplines.

Kortom, IT Policy and Organisation is de beheerdiscipline van het vormen van het beleid voor het beheer van de IT-infrastructuur door middel van het opstellen van doelstellingen, kaders, richtlijnen en reikwijdte om richting en sturing te verlenen ten behoeve van het realiseren van de doelstellingen geldend voor de gehele organisatie.

Service Level Management

De IT-beheerorganisatie zal veel aandacht en inspanning moeten richten op het verkrijgen van inzicht in en het realiseren en verhogen van de klanttevredenheid over de services die zij levert. Hierbij wordt de beheerorganisatie in toenemende mate geconfronteerd met de verwachtingen van afnemers van IT-services. In het nabije verleden was het zo dat de services voornamelijk door de aanbodzijde werden uitgemaakt (technology-push), tegenwoordig dient een rekencentrum zich meer en meer te richten op de informatiebehoeften van de klanten (information-pull).

De activiteiten van een beheerorganisatie worden uitgevoerd ten behoeve van de afnemers van de IT-services (interne of externe klanten). Het is voor zowel de beheerorganisatie als de klant van groot belang dat de kwaliteit van de IT-services optimaal is. Optimaal wil zeggen dat wordt voorzien in de wensen en eisen van de afdelingen over de vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van de IT-services gedurende een overeengekomen periode. Daarom zullen beide partijen formele afspraken (vaak verwoord in service level agreements (SLA's)) moeten maken omtrent de aard, omvang en kosten van de IT-services, inclusief de wijze waarop de services worden geleverd en de eisen die de klant daaraan stelt.

De afspraken die binnen de beheerdiscipline Service Level Management worden gemaakt, worden afgestemd met de andere beheerdisciplines. Elke beheerdiscipline is verantwoordelijk voor één of meer kwaliteitseigenschappen vastgelegd in de service level agreements.

Kortom, Service Level Management is de beheerdiscipline die verantwoordelijk is voor het maken van duidelijke, reële afspraken met de klanten, de controle uitoefent over de naleving van de gemaakte afspraken en de communicatie over de service met de klanten verzorgt.

Configuration Management

Om de afgesproken IT-services aan de (interne) klanten te kunnen leveren en om zodoende aan de gemaakte afspraken te kunnen voldoen, is een bepaalde configuratie van de IT vereist. Deze configuratie bestaat uit een aantal componenten, zogenaamde Configuration Items (CI's), waarbij alle initiële waarden en alle daarop volgende verwijderingen en aanpassingen van CI's worden geregistreerd, zodat de actuele status van een CI te allen tijde is gewaarborgd. Duidelijk is dat de configuratie zodanig moet worden gekozen dat de IT-services op een zo doelmatig mogelijke wijze aan de klant kunnen worden aangeboden, zodat aan alle afspraken wordt voldaan. Hierbij dient de beheerorganisatie nog voldoende flexibel te zijn om te kunnen inspringen op veranderingen in de markt of veranderende behoeften van de klant.

Configuration Management zorgt dus voor een actuele weergave van alle apparatuur, programmatuur met bijbehorende documenten, telecommunicatiefaciliteiten en allerlei andere faciliteiten die een organisatie wenst te beheren. Hiertoe wordt een overzicht bijgehouden waarin alle relevante informatie wordt opgeslagen, zoals de versie en status van de afzonderlijke CI's.

Van groot belang is om actuele informatie van alle CI's bij te houden daar deze gegevens veelvuldig door andere beheerdisciplines worden gebruikt. Bij het verlenen van hulp of het identificeren van een probleem moet de juiste informatie over de CI's snel kunnen worden opgevraagd. Om de informatie op efficiënte wijze op te slaan is het wenselijk de CI's in klassen in te delen. Per klasse kunnen dan weer subklassen worden onderscheiden. De wijze waarop deze indeling in klassen plaatsvindt is per organisatie verschillend.

Kortom, Configuration Management is de discipline van het identificeren van de configuratie-items (CI's), het registreren van de CI's inclusief de status en het verifiëren van de volledigheid en juistheid van de CI's.

Capacity Management

De afspraken die met de afdelingen van de afnemers zijn gemaakt, zullen een bepaalde capaciteit vereisen. Deze capaciteit moet van voldoende niveau zijn om aan de afspraken betreffende de kwaliteit van de dienstverlening te kunnen voldoen. Het is van belang dat niet alleen op dit moment de capaciteit van voldoende niveau is; over een paar jaar dient de capaciteit van de beheerorganisatie nog steeds toereikend te zijn. Dit impliceert dat niet alleen aandacht moet worden besteed aan de benodigde capaciteit op dit moment, maar dat er tevens aandacht moet zijn voor de (middel)lange termijn. De aanpassingen van de capaciteit van de diverse IT-resources moeten bewust en gepland worden uitgevoerd. Hiervoor moet een beheerdiscipline zijn ingevuld waardoor informatie over verwerkingscapaciteit en capaciteitsbehoeften kan worden verzameld. Voor het bepalen van de benodigde capaciteit op (middel)lange termijn moet gebruik worden gemaakt van schattingen, verwachtingen, groeimodellen en verwachtingsformules ten aanzien van de technische ontwikkelingen en ontwikkelingen in de markt.

Kortom, Capacity Management is de beheerdiscipline die zorg draagt voor de registratie van de beschikbare, de huidig gebruikte en de maximaal toelaatbare capaciteit en het waarborgen van voldoende (verwerkings-) capaciteit van de IT-resources op de korte, middellange en lange termijn.

Change Management

Als gevolg van technologische ontwikkelingen, een veranderend klantenbestand, veranderde wensen en behoeften van afdelingen, fouten of storingen in de IT-infrastructuur of op initiatief van het 'eigen' personeel van de beheerorganisatie zullen wijzigingen in de IT-infrastructuur noodzakelijk zijn. Het is van groot belang om het doorvoeren van deze wijzigingen te beheersen, teneinde inzicht te houden in wat de wijziging inhoudt, welke

redenen hiervoor zijn, door wie en wanneer dit gebeurt en wat de eventuele consequenties ervan zijn.

Er dient rekening mee te worden gehouden dat tijdens het uitvoeren van de wijzigingen, verstoringen en afwijkingen van het dienstenniveau zo min mogelijk voorkomen. Hiertoe moet erop worden toegezien dat beproefde methoden en technieken worden gebruikt voor de voorbereiding, bouw, test en implementatie van de nieuwe of gewijzigde componenten.

Een belangrijke rol in deze beheerdiscipline is weggelegd voor de behandeling van een wijziging (de zogenaamde RFC, Request For Change) die (onder andere) kan voortkomen uit het Problem Management. Een wijzigingsvoorstel moet eerst worden geautoriseerd waarna de wijziging een prioriteit krijgt afhankelijk van de urgentie van de wijziging en van de afspraken in het service level agreement. Voor uitvoering van de wijziging kunnen meerdere afdelingen en soms eindgebruikers worden aangewezen.

Kortom, Change Management is de discipline van het controleren en beheren van wijzigingsvoorstellen en de eventuele doorvoering van wijzigingen met betrekking tot alle CI's van de IT-infrastructuur.

Problem Management

De beheerorganisatie wordt gevormd door een samenspel van apparatuur, programmatuur, gegevens en mensen, waarbij problemen (fouten en storingen) kunnen optreden bij elk van deze componenten. Daarnaast kunnen problemen optreden bij de GO of de SO. Deze problemen kunnen kleine incidenten zijn die voor de gebruiker nauwelijks merkbaar zijn, maar ook grote storingen die de dienstverlening gedurende een bepaalde tijd verstoren. De storingen kunnen worden opgemerkt door de gebruikersorganisatie, de 'eigen' medewerkers van de beheerorganisatie of automatische monitorhulpmiddelen op de diverse platformen. Om de kwaliteit van de dienstverlening te garanderen, is het van belang om voorkomende problemen zo snel mogelijk op te lossen. Daarom moet het rekencentrum beschikken over een 'meldpunt' voor problemen, waar bekwame en technisch onderlegde medewerkers direct oplossingen kunnen aandragen, of de problemen kunnen doorverwijzen naar een desbetreffende specialist.

Problemen dienen zo snel mogelijk te worden opgelost.

Kortom, Problem Management is de beheerdiscipline die zich richt op het registreren van de probleemmeldingen, het aandragen van oplossingen en het indienen van een RFC indien noodzakelijk.

Workload Management

De afdelingen in de organisatie zullen werk in de vorm van printopdrachten, verwerkingsopdrachten of rekenopdrachten aan het systeem aanbieden. Hierbij kunnen zij geen rekening houden met het werk dat andere afdelingen aanbieden, hetgeen kan resulteren in grote pieken (met als gevolg langere verwerkingstijden) en dalen (met als gevolg systemen die zonder 'werk' zitten) in het aanbod van werk. Hiertoe moet het werk worden ingepland voor verwerking waardoor de hoeveelheid werk beter wordt gespreid over de beschikbare capaciteit. Daarnaast dient een verdeling van de beschikbare resources over de interactieve gebruikers te worden verzorgd, zodat de eisen verwoord in SLA's kunnen worden gerealiseerd.

Een belangrijke taak van Workload Management is het toewijzen van processortijd aan de verschillende batch jobs (scheduling). Hierbij moet niet alleen rekening worden gehouden met de grootte van de job maar ook met de volgorde waarin de jobs moeten worden verwerkt. In de praktijk wordt alleen aandacht besteed aan grote jobs daar de kleinere jobs wel tussendoor kunnen worden verwerkt (ze gebruiken slechts een fractie van de totale processortijd). Hieruit blijkt dat er een nauwe samenhang is met de beheerdiscipline Operations Management. Daarnaast is het verdelen van het interactieve werk over de aanwezige configuratie eveneens van groot belang.

Kortom, Workload Management is de beheerdiscipline die zich bezighoudt met het groeperen en het verdelen van het te verrichten werk en de planning ervan over de beschikbare IT-resources.

Performance Management

De afnemers verlangen een zekere performance (zoals responstijden en verwerkingstijden) van de IT-infrastructuur. Deze performance-eisen kunnen zijn vastgelegd in SLA's of andere afspraken. Om aan deze afspraken te kunnen voldoen, dienen de systemen optimaal op elkaar te worden afgestemd en moet de performance continu worden bewaakt (meten, monitoren en finetunen), zodat kan worden ingegrepen bij afwijkingen.

Bij respons- en verwerkingstijden gaat het om het meten van de tijdsduur van een proces of handeling. Van belang is dat de capaciteit zodanig is dat er vanuit het gebruik geen klachten zijn betreffende de snelheid van verwerking en respons. Door het afstellen (tuning), wat onder de verantwoordelijkheid van het Performance Management valt, kan de snelheid worden verbeterd. Het is duidelijk dat veelvuldig afstemming met Capacity Management nodig is.

Kortom, Performance Management is de beheerdiscipline die zich richt op monitoring en tuning van de actieve systemen ter waarborging van de gemaakte performanceafspraken.

Security Management

Het management van een organisatie wil zekerheid hebben dat de gegevens in het systeem, maar ook de omliggende apparatuur en programmatuur, op vertrouwelijke en integere wijze worden behandeld. In verband met de vertrouwelijkheid en integriteit van de gegevens dient het rekencentrum zekerheid te bieden dat ongeautoriseerde personen op geen enkele wijze toegang kunnen krijgen tot de apparatuur en de programmatuur en (daarmee tot) de gegevens. Deze beveiliging heeft daarom betrekking op zowel fysieke aspecten (zoals toegang tot gebou-

wen en ruimten) als logische aspecten (zoals wachtwoorden en beperking van functionaliteiten). Daarnaast moet het mogelijk zijn om het verkrijgen van toegang (zowel fysiek als logisch) en de uitgevoerde (kritische) activiteiten achteraf te controleren aan de hand van een audit trail.

Onder de fysieke beveiliging worden verstaan alle maatregelen voor het veiligstellen van gebouwen, computerruimten, kluizen en apparatuur die zowel onopzettelijk als opzettelijk kunnen worden beschadigd. Maatregelen als fysieke toegangscontrole, brandbeveiliging, clear desk policy en beveiliging van kabels zijn voorbeelden om de fysieke beveiliging te waarborgen. Maatregelen als noodstroomvoorzieningen, die dienen om de robuustheid van de informatievoorziening te vergroten (en dus ook beveiliging bieden bij het uitvallen van de stroom), worden tot het Availability Management gerekend.

De maatregelen voor de logische beveiliging moeten een bescherming bieden tegen het onbevoegd kennisnemen van en/of aanbrengen van veranderingen in gevoelige informatie. Hierbij moet gedacht worden aan maatregelen voor de beheersing van gebruikerstoegang en gebruikersbevoegdheden, toegangsbeveiliging voor netwerken, computers en toepassingen en maatregelen voor de preventie en detectie van virussen.

Kortom, Security Management is de beheerdiscipline die zich bezighoudt met het waarborgen van het vereiste niveau van fysieke en logische beveiliging van de IT-middelen en de omgeving waarin deze zich bevinden.

Availability Management

Met afdelingen die IT-services afnemen, kunnen afspraken worden gemaakt over de beschikbaarheid van deze services. Niet alleen afspraken over wat gebeurt bij een stroomstoring of het uitvallen van een disk, maar ook in geval van grote calamiteiten als brand en wateroverlast. Zowel aspecten met betrekking tot de robuustheid (continue werking) van de infrastructuur als aspecten betreffende de uitwijk en het uitwijkplan zijn hierbij van toepassing. Het rekencentrum moet maatregelen nemen om onder alle mogelijke omstandigheden aan het gewenste niveau van beschikbaarheid te kunnen voldoen.

Merk op dat hierbij onderscheid wordt gemaakt tussen de continue werking en de uitwijkvoorzieningen. Onder de continue werking wordt verstaan de mate waarin apparatuur en programmatuur na het optreden van een storing blijven werken zonder stagnatie van de operationele verwerking. Maatregelen die kunnen worden getroffen om de continue werking te waarborgen zijn bijvoorbeeld het dubbel uitvoeren van componenten of het installeren van noodstroomvoorzieningen.

De uitwijkvoorzieningen duiden op de mate waarin de totale geautomatiseerde informatievoorziening hervat kan worden indien door omstandigheden uitval van het systeem optreedt. Dit kan eventueel op een andere (fysieke) plaats zijn indien de huidige plaats door omstandigheden niet beschikbaar is. Deze omstandigheden kunnen bijvoorbeeld brand of een aardbeving zijn. Maatregelen ter waarborging van de continuïteit zijn bijvoorbeeld het aanhouden van 'hot sites' of 'cold sites' en het op adequate wijze maken en registreren van back-ups.

Het is duidelijk dat iedere maatregel kosten met zich meebrengt en dat hoe 'beter' de maatregel is hoe hoger de kosten zijn. Daarom is het noodzakelijk om een afweging te maken tussen de noodzakelijkheid van de te treffen maatregelen en de eraan verbonden kosten.

Kortom, Availability Management is de beheerdiscipline die zich richt op alle activiteiten met betrekking tot de continue werking van de IT-infrastructuur en de uitwijkvoorzieningen van de IT-infrastructuur, teneinde het vereiste niveau van beschikbaarheid te waarborgen.

Accounting Management

Alle activiteiten die door of namens afdelingen op de IT-infrastructuur worden uitgevoerd, worden op een zodanige wijze geregistreerd dat achteraf analyse van de systeemactiviteiten mogelijk is. Deze vastlegging kan worden gebruikt voor verschillende doeleinden, zoals het bepalen van de kosten van de IT, het doorberekenen van de kosten aan de klant of het dienen als audit trail.

Merk op dat de beheerdiscipline Accounting Management niet het doorbelasten van kosten inhoudt (het zogenaamde charging). De gegevens die bij het proces van Accounting Management worden vastgelegd, kunnen wel worden gebruikt voor onder andere het doorbelasten of doorberekenen van de IT- en automatiseringskosten.

Het rekencentrum moet maatregelen nemen om aan het gewenste niveau van beschikbaarheid te voldoen.

Kortom, Accounting Management is de beheerdiscipline die betrekking heeft op het vastleggen van gebeurtenissen in de IT-infrastructuur en het waarborgen van de vereiste betrouwbaarheid van deze vastleggingen ten behoeve van de controleerbaarheid.

Operations Management

De IT-infrastructuur van de organisatie bestaat uit diverse platformen en informatiesystemen. Hierbij worden allerlei activiteiten uitgevoerd, zoals het monitoren van de systemen, het opstarten van de batches, het afsluiten van applicaties, het distribueren van output, het bijhouden van de voorraad print- en mediabenodigdheden en het schoonhouden van de vitale apparatuur. Er zijn dus talloze activiteiten die ervoor zorgen dat de applicaties dagelijks actief zijn en dat de verwerking niet alleen overdag maar ook 's nachts plaatsvindt. Duidelijk is dat ook aan deze werkzaamheden normen moeten worden gesteld, zeker gezien het feit dat een aantal van deze activiteiten kunnen worden betiteld als 'kritiek'.

Operations Management is de sturende activiteit van alle operationele taken. Zo worden dagelijks de applicaties en computersystemen opengesteld en afgesloten voor gebruik. Daarnaast wordt de outputdistributie, het zor-

De beheerdisciplines vertalen de activiteiten in een beheerorganisatie naar de kwaliteitsaspecten van een EDP-auditor.

gen dat de gewenste output op de juiste plek komt, ook vanuit het Operations Management verzorgd.

Het op voorraad hebben van voldoende print- en mediabenodigdheden (tapes, diskettes, toner, etc.) alsmede het schoonhouden van de vitale apparatuur (zoals tape devices en printers) zijn ten slotte ook voorbeelden van taken die door het Operations Management worden uitgevoerd.

Kortom, Operations Management is de beheerdiscipline die alle activiteiten omvat met betrekking tot het plannen en uitvoeren van dagelijkse, operationele activiteiten ten behoeve van het waarborgen van de adequate werking van de IT-infrastructuur.

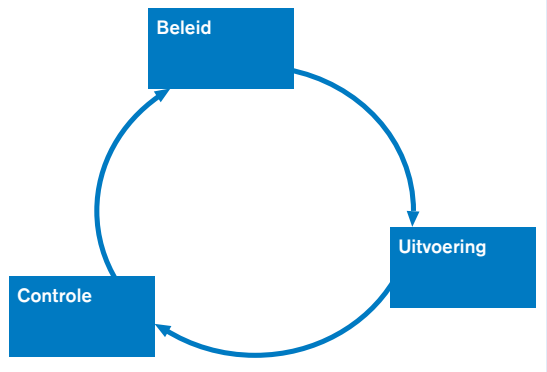
Een procesmodel voor elke beheerdiscipline

Het beheer van IT wordt omkleed met beheeractiviteiten die kunnen worden gegroepeerd volgens bijvoorbeeld bovenstaande disciplines. De toegevoegde waarde van deze disciplines zit niet alleen in het gestandaardiseerd uitvoeren van de nodige beheeractiviteiten, maar vooral ook in het op gestructureerde wijze verbeteren van de uitvoering van de beheeractiviteiten.

Managementcyclus

Om het beheer op gestructureerde wijze te verbeteren kan de organisatie het procesmodel van de managementcyclus hanteren. Dit model bestaat uit een drietal processen, zoals in figuur 4 is weergegeven.

Beleidsvorming voor een beheerdiscipline
Dit proces behandelt het strategische niveau van een beheerdiscipline. In het proces 'Beleid' worden het beleidskader, de verantwoordelijkheden en de uitgangspunten voor de uitvoering van de activiteiten verwoord, zodat richting en sturing aan de betreffende beheerdiscipline kan worden gegeven.



Figuur 4. De management-cyclus.

Uitvoering van een beheerdiscipline
Het proces 'Uitvoering' houdt zich bezig met de vertaling van het beleidskader en de uitgangspunten naar richtlijnen, procedures en maatregelen. Om te voldoen aan de geformuleerde doelstelling in het beleid dient de organisatie invulling te geven aan het proces 'Uitvoering' van de afzonderlijke beheerdisciplines. De beleidslijnen dienen herkenbaar in de richtlijnen, procedures en maatregelen te zijn verwoord. Het proces bevindt zich op het operationele niveau van een beheerdiscipline. In de procedures wordt aangegeven wie een bepaalde handeling moet uitvoeren, waarmee de handeling moet worden uitgevoerd, welke gegevens daarbij moeten worden vastgelegd en waarom een bepaalde handeling moet worden uitgevoerd.

Controle op uitvoering en beleid
Ten slotte moet de organisatie door middel van het proces 'Controle' continu bezig zijn met het toezicht houden op de uitvoering van de activiteiten, het bewaken van de voortgang van de activiteiten en het rapporteren over de status van de ontwikkeling c.q. volwassenheid van elke betrokken discipline. Aangezien elke discipline aan veranderingen onderhevig is dient de organisatie invulling te hebben gegeven aan het proces 'Controle'. Dit proces bevindt zich op het tactische niveau binnen een discipline, omdat hiermee een schakel wordt gevormd tussen het strategische en het operationele niveau.

Op basis van de rapportages uit het proces 'Controle' is het mogelijk dat de uitvoering van de beheerdiscipline in kwestie moet worden bijgesteld. Daarnaast kan het zo zijn dat niet de uitvoering, maar het beleidskader en de uitgangspunten voor de discipline moeten worden aangepast. Hiermee is de managementcyclus volledig en heeft de organisatie een proces ingericht dat zich continu bezighoudt met het verbeteren van de kwaliteit van de betreffende beheerdiscipline en als gevolg daarvan met het continu verbeteren van het beheer van de IT.

De verschillende onderzoeksniveaus

Tijdens het uitvoeren van een technical audit wordt dus niet alleen beoordeeld in hoeverre de noodzakelijke beheeractiviteiten worden uitgevoerd en op welke wijze de technische implementatie is ingericht. De KEA-aanpak leidt eveneens tot het beoordelen van de aanwezigheid van een managementcyclus met betrekking tot het beheer van de IT.

Indien het piramidemodel vanaf een metaniveau wordt beschouwd, kan men, net zoals in elke afzonderlijke discipline, drie niveaus van beheer onderkennen. Hierbij wordt onderscheid gemaakt in strategisch, tactisch en operationeel niveau.

Het strategisch niveau bepaalt de te varen koers voor de beheerorganisatie. De beheerdiscipline IT Policy and Organisation beschrijft de IT-organisatie op strategisch niveau. De overige beheerdisciplines beschrijven het tactische niveau van het beheer. Op tactisch niveau vindt een vertaling plaats naar de diverse beheerdisciplines die een organisatie moet inrichten om invulling te kunnen geven aan de doelstellingen verwoord op het strategisch niveau. De beheerdisciplines op het tactische niveau kun-

nen worden gezien als de nadere uitwerking van de discipline IT Policy and Organisation. In principe kan worden gesteld dat de tactische beheerdisciplines vertaling en invulling geven aan het proces 'Uitvoering' van de discipline IT Policy and Organisation. De daadwerkelijke uitvoering van de beheeractiviteiten vormt het operationele niveau waarbij gebruik wordt gemaakt van allerlei procedures, werkinstructies en implementatiehandleidingen zoals in figuur 5 is weergegeven.

Spelen met scope en diepgang

In het voorgaande is uitvoerig stilgestaan bij de componenten van de KEA-aanpak voor technical auditing. Om deze opsomming concreet te maken worden enkele voorbeelden beschreven op welke wijze, in de praktijk, gebruik wordt gemaakt van deze aanpak.

Het raamwerk kan worden gebruikt voor het beoordelen van een volledig rekencentrum, maar kan tevens worden gebruikt voor het beoordelen van het beheer rondom één enkele component binnen de gehele IT-infrastructuur. Bij het beoordelen van een rekencentrum kan bijvoorbeeld worden gedacht aan het afgeven van een Third Party Mededeling (TPM) over het (uitbestede) beheer van de IT. Het vormen van een oordeel over het beheer rondom een firewall is een voorbeeld van het beoordelen van één technische component.

Onderscheid kan worden gemaakt tussen beheerdisciplines die hoofdzakelijk intern zijn gericht ten behoeve van de eigen beheerorganisatie (zoals Capacity Management, Workload Management en Accounting Management) en beheerdisciplines die gericht zijn op de externe communicatie met SO en GO (zoals Service Level Management, Change Management en Problem Management).

Beheerdisciplines in relatie tot de kwaliteitsaspecten

Met behulp van de beheerdisciplines kan een vertaalslag worden gemaakt van de activiteiten in een beheerorganisatie naar de kwaliteitsaspecten die een EDP-auditor gebruikt. Zo kan met deze benadering per kwaliteitsaspect enerzijds worden beoordeeld in hoeverre de beheerdisciplines ondersteuning verlenen aan een kwaliteitsaspect en anderzijds in hoeverre per beheerdiscipline de kwaliteitsaspecten aanwezig zijn. Hierdoor wordt een passend communicatiemiddel geschapen dat zowel door de IT-beheerorganisatie, het management als ook door de EDP-auditors wordt verstaan.

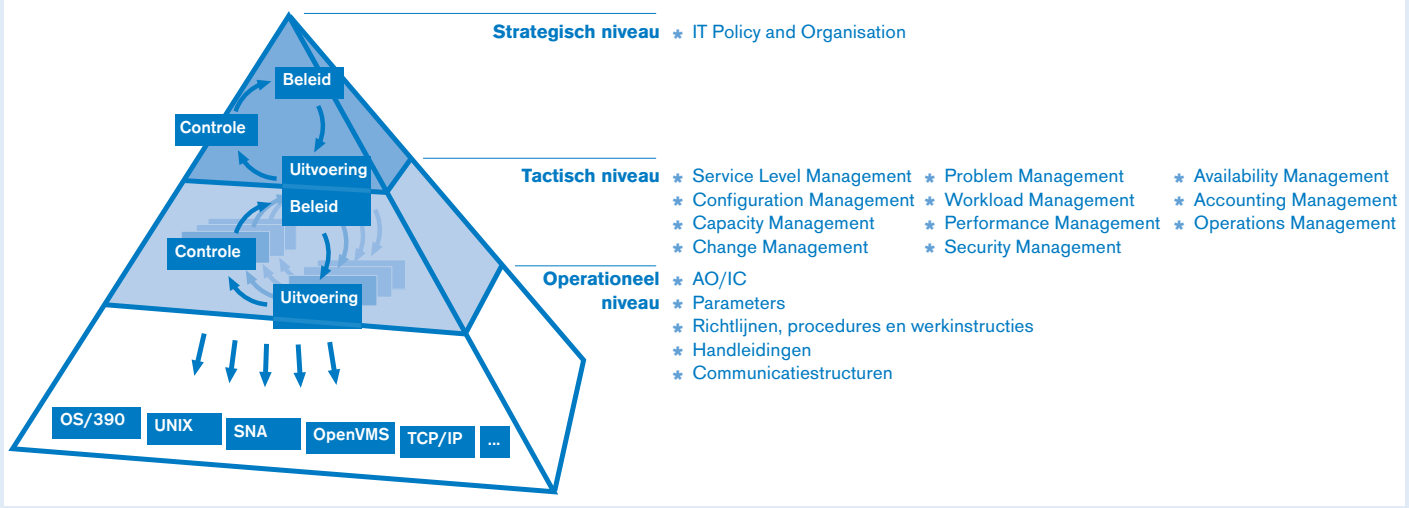
Kortom, het is mogelijk een onderzoek te doen naar één kwaliteitsaspect binnen alle beheerdisciplines, naar alle kwaliteitsaspecten van één beheerdiscipline of naar één kwaliteitsaspect van één beheerdiscipline en naar alle mogelijke combinaties hiervan. In tabel 1 worden twee voorbeelden van deze mogelijkheden weergegeven.

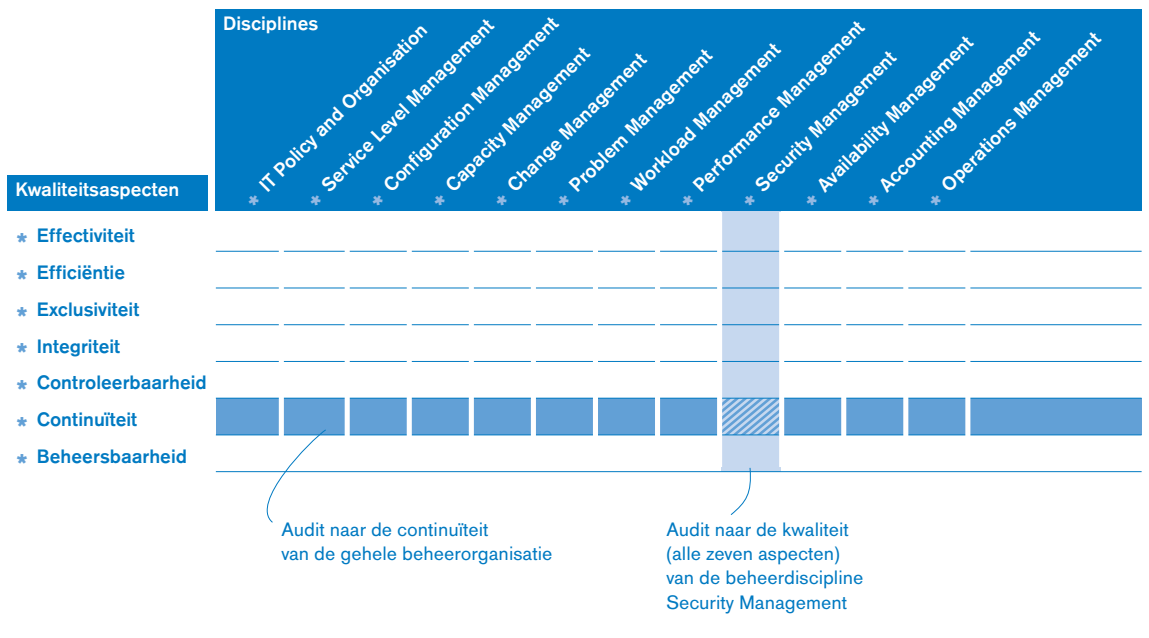
Rekencentrumaudit

Bij een rekencentrumaudit wordt de kwaliteit van de VTO-beheerorganisatie, van de relatie van de VTO met de GO en van de relatie van de VTO met de SO per te onderkennen beheerdiscipline beoordeeld door vast te stellen in hoeverre de beheerprocedures zijn beschreven (opzet), in hoeverre de beheerprocedures daadwerkelijk zijn ingericht op enig moment (bestaan) en in hoeverre de kwaliteit van het bestaan van de beheerprocedures gedurende het gehele jaar is gewaarborgd (werking).

Bij een rekencentrumaudit kan, al naargelang de gewenste diepgang, elke beheerdiscipline op uitvoeringsniveau worden onderverdeeld in:
* *organisatie, procedures en richtlijnen*. Elke beheerdiscipline dient binnen de organisatorische inrichting te zijn belegd. Het betreft het toewijzen van verantwoordelijkheden, het formaliseren van richtlijnen en het hanteren van procedures ter ondersteuning van de uitvoering van de beheerdiscipline.

Figuur 5.
Het piramidemodel.





Tabel 1. Matrix kwaliteitscriteria versus beheerdisciplines.

* *hardware*. Elke beheerdiscipline kan (deels) worden ondersteund door een hardwarecomponent van de IT-infrastructuur.
* *software*. Elke beheerdiscipline kan (deels) worden ondersteund door een softwarecomponent van de IT-infrastructuur.
* *beheer-/hulpmiddelen*. Elke beheerdiscipline kan worden ondersteund door een geautomatiseerd beheer-/hulpmiddel.

Om nog verder op het model in te zoomen kunnen de hulpmiddelen dienen ter ondersteuning van het doel/resultaat (beveiligingspakket, jobscheduler) van een beheerdiscipline en/of ter ondersteuning van de uitvoering van een beheerdiscipline (probleemregistratiepakket). Het hulpmiddel zelf kan echter, zoals uit tabel 2 blijkt, tevens object van onderzoek zijn.

Audit van technische objecten

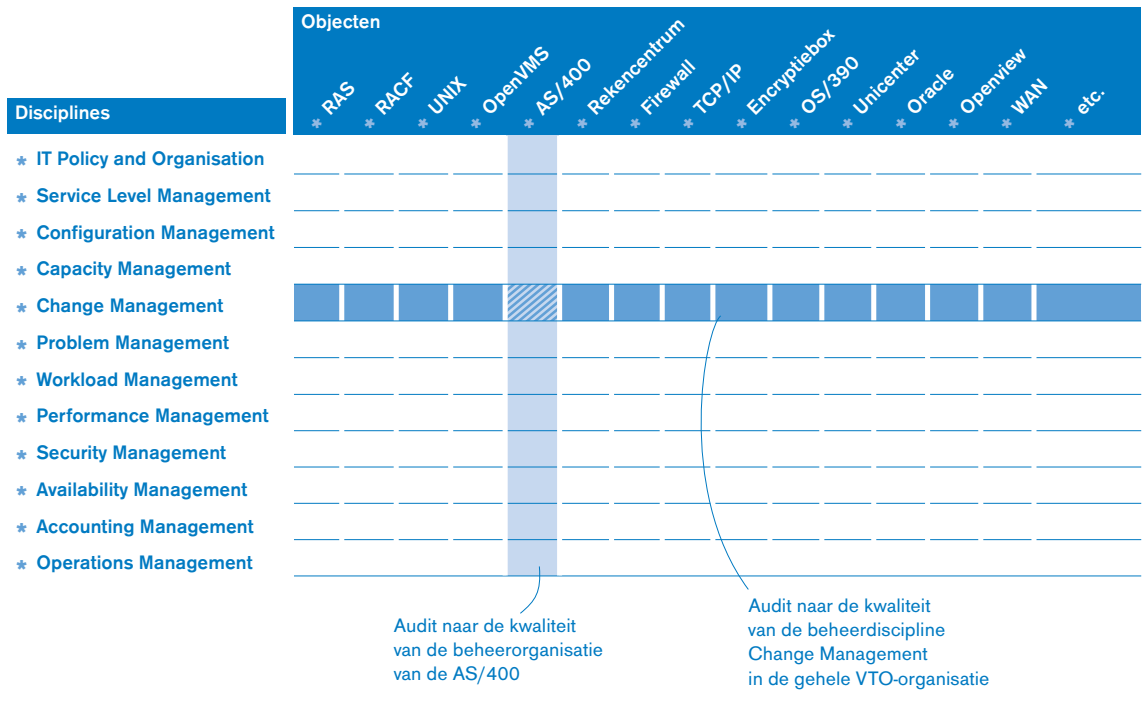
Bij de beoordeling van een technisch object (NOREA-geschrift 1 hanteert de term technisch systeem) kan een oordeel worden gegeven over de kwaliteit van de opzet en het bestaan van de technische implementatie. De audit bestaat uit het beoordelen van technische objecten, zoals:
* operatingsystemen, onder andere UNIX-versies, Windows NT-omgevingen;
* netwerkbesturingssystemen;
* databasemanagementsystemen;
* beheerproducten;
* overige IT-componenten, zoals firewalls en encryptieboxen.

In dergelijke onderzoeken is het resultaat een oordeel omtrent de implementatie op het moment van onderzoek. In het geval tijdens het onderzoek het piramidemodel wordt toegepast om van één of meer objecten te beoordelen hoe per beheerdiscipline met het betreffende object wordt omgegaan, kan een oordeel worden gegeven over de kwaliteit van de implementatie op langere termijn (werking). In tabel 2 worden twee voorbeelden van onderzoeken weergegeven.

In beheer nemen nieuwe IT-component

Het piramidemodel vormt tevens een volledig referentiemodel bij het 'in beheer nemen' van een nieuwe component van de IT-infrastructuur. Voor een optimaal beheer van de nieuwe component moeten alle verantwoordelijkheden en taken verbonden aan de beheeractiviteiten in de organisatie zijn belegd. Daarnaast zal moeten worden besloten waar gebruik zal worden gemaakt van de reeds in de organisatie aanwezig zijnde beheerhandelingen en -activiteiten.

Er zal een beleidskader moeten zijn geschreven voor het beheer, vervolgens zullen afspraken ten aanzien van aspecten als beschikbaarheid en responstijden moeten zijn gemaakt. De nieuwe component, met al zijn eventuele parameters en subcomponenten, zal moeten worden opgenomen in het configuratieoverzicht. De component moet in de capaciteitsplanning worden opgenomen en de relatie met de reeds aanwezige componenten moet bekend zijn. Eventuele wijzigingen tijdens de levenscyclus van de component zullen op weloverwogen en doordachte wijze moeten worden aangebracht. Bekend dient te zijn op welke wijze problemen en incidenten met betrekking tot de component kunnen worden aangemeld en vervolgens moeten worden opgelost. Een keuze wordt gemaakt ten aanzien van de wijze waarop de component zal worden ingezet, zodat de totale workload optimaal kan worden verdeeld. Vervolgens dient bekend te zijn op welke wijze de instellingen van de component de responstijd van zowel de component zelf als de end-to-end responstijd kunnen beïnvloeden, zodat aan de gemaakte afspraken kan worden voldaan. De component dient op dusdanige wijze te zijn afgeschermd voor onbevoegden dat de integriteit en continuïteit van de



Tabel 2. Matrix beheer-disciplines versus objecten.

component en de gehele IT-infrastructuur niet in gevaar komen. Daarnaast dient de component niet de reeds aanwezige beveiligingsinfrastructuur te ondermijnen. Bij het optreden van calamiteiten moeten zo snel mogelijk oplossingen kunnen worden aangedragen. Tevens dient een keuze voor eventuele dubbele uitvoering van componenten of verbindingen te zijn gemaakt. De loggingmogelijkheden van de component dienen optimaal te worden benut. Dit houdt in dat niet alles moet worden gelogd, maar juist alleen die aspecten waaraan waardevolle managementinformatie te ontlenen valt. Hierbij moet niet enkel worden gedacht aan langetermijninformatie, maar ook aan operationele beheerinformatie. Ten slotte moeten allerlei procedures en werkinstructies aanwezig zijn, zodat te allen tijde bekend is op welke wijze de component beheerd kan worden en operationeel kan worden gehouden.

Het model is derhalve zowel relevant voor degenen die het IT-beheer gaan uitvoeren, als voor het management dat wil weten of het IT-beheer ook daadwerkelijk adequaat is ingevuld en wordt uitgevoerd. Daarnaast biedt het model een referentiekader voor een EDP-auditor ter beoordeling van de status van het IT-beheer. Kortom, het model biedt houvast en aanknopingspunten bij tal van onderzoeksobjecten en is toepasbaar in het brede scala van technical audits.

Tot slot: Continue verbetering van het beheer van IT

Bedrijven en organisaties moeten streven naar het professionaliseren van het beheer van de IT. Aangezien dit een continu proces is, zou periodieke beoordeling van het beheer hierbij een toetsende en sturende rol kunnen vervullen. Zowel bij de organisaties als bij de EDP-auditors ontstaat het besef dat een aanpak waarbij gebruik wordt gemaakt van een procesmatige benadering leidt tot een gestructureerde en volledige aanpak (van het beoordelen) van het IT-beheer. Het hierboven gepresenteerde KEA-piramidemodel biedt een uitstekend raamwerk voor het beoordelen van het IT-beheer, zodat gezamenlijk kan worden gestreefd naar daadwerkelijke professionalisering van IT-beheer.

Het model kan tevens in een meerjarenauditplan van de EDP-auditor worden geplaatst, waarbij op gestructureerde wijze kan worden beoordeeld in hoeverre het beheer van de IT naar professionaliteit aan het groeien is. Indien de organisatie zelf nog niet de managementcyclus volledig heeft geïmplementeerd, kan de EDP-auditor door middel van een technical audit voor het proces 'Controle' zorg dragen. Met als gevolg dat op deze wijze sturing aan het beheer ('Beleid' en 'Uitvoering') kan worden gegeven en deze audit derhalve een directe toegevoegde waarde heeft voor de organisatie. In een later stadium, als de organisatie zelf volgens de managementcyclus functioneert, ligt de toegevoegde waarde van een technical audit voornamelijk in een onafhankelijke en onpartijdige blik die een EDP-auditor op het IT-beheer kan werpen.

Door het toepassen van het piramidemodel kan een oordeel worden gegeven over de kwaliteit van de implementatie op langere termijn.

De technical audit kan input leveren om verbeteringsacties voor het beheer op te zetten. Vanuit het onderzoek zal een gezamenlijke invulling worden gegeven aan de verbeterpunten (waarbij een voor zowel de onderzochte organisatie als de EDP-auditor bevredigend resultaat moet worden bereikt). In samenwerking met de EDP-auditor zal voor een stap-voor-stap-benadering worden gekozen, waarbij de directbetrokkenen van de organisatie actief deelnemen aan het verbeteren van de betreffende beheeractiviteiten. Het 'learning by doing'-effect zal dan ook optimaal zijn.

Deze benadering van technical auditing, waarbij zowel beheerdisciplines als de technische implementaties worden beoordeeld, zal leiden tot een synergie voor de beheerorganisatie, het management en de EDP-auditor. Hierbij is het gezamenlijke doel dat IT inderdaad als strategisch wapen kan worden ingezet, terwijl de betrouwbaarheid en de continuïteit van de IT-infrastructuur zijn gewaarborgd en het IT-beheer effectief en efficiënt wordt uitgevoerd.

Literatuur

[ITIL90]
Diverse publicaties, HMSO Crown Copyright Unit Norwich UK.

[Looij95]
M. Looijen, *Beheer van informatiesystemen*, Kluwer Bedrijfswetenschappen, Deventer 1995.

[Neis98]
Prof. A.W. Neisingh RE RA, *Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?*, Compact 1998/3.

[Nele96]
G.N. Nelemans, *Basisnormen voor IT-infrastructuur, Rapport naar aanleiding van een afstudeerstage uitgevoerd in opdracht van KPMG EDP Auditors*, Technische Universiteit Delft, Faculteit der Technische Wiskunde en Informatica, 1996.

[NORE98]
NOREA-geschrift 1, *IT-auditing aangeduid*, 1998.

[Vogd98]
Foppe Vogd, voorzitter van de onafhankelijke Nederlandse organisatie IT Service Management Forum (itSMF), *Leeuwendeel van de kosten van IT zit in beheer en exploitatie*, Automatisering Gids, nr. 29/30, 17 juli 1998.