VIRTUALISATIE:

alleen maar **voordelen?** (deel 2)

In het eerste deel van dit artikel *(De EDP-Auditor 2009-1)* kwam het concept virtualisatie aan bod. Ook is ingegaan op de oorsprong van virtualisatie en zijn toepassingen van deze techniek toegelicht. Om de behandelde theorie vervolgens te relateren aan de praktijk, werd een casus beschreven. Daarnaast is aandacht besteed aan aandachts- en knelpunten met betrekking tot de toepassing van virtualisatie. Om ten slotte te illustreren wat voor invloed de toepassing van virtualisatie heeft op de IT-processen, werden de ITIL-processen onder de loep genomen. In dit tweede deel van het artikel wordt een raamwerk ontwikkeld dat de IT-auditor kan helpen de risico's te identificeren bij een virtualisatietraject.

ANGELO MONTERO

Ter inleiding wordt begonnen met een stuk waarin op hoofdlijnen de zorgpunten van een IT-manager worden benoemd. Om een raamwerk toegespitst op een specifiek onderwerp op te stellen, dient het onderwerp allereerst afgebakend te zijn. Daarom worden op basis van het NOREA-geschrift nr. 1 relevante IT-domeinen en -objecten geselecteerd.
Uiteindelijk worden met behulp van COBIT relevante fasen tijdens een virtualisatietraject gedefinieerd. Deze cyclus wordt de virtualisatiemanagementcyclus genoemd. Elke fase is verder uitgewerkt door een synthese van alle voorgaande paragrafen: toepassingen, casus, aandachtspunten, IT-management, IT-domeinen en COBIT zelf. Het artikel wordt afgesloten met een korte conclusie.

IT-MANAGEMENT

De IT-manager heeft meer nodig dan een verhaal over de toepassingen en aandachtspunten van virtualisatie (zie *de EDP-Auditor* 2009/1). Belangrijk bij risicomanagement is om naast risico's aankaarten, ook oplossingen of instrumenten hiervoor aan te dragen. Vragen waar de IT-manager voortdurend mee zit, zijn onder andere [LAUD06]:

- Investering in IT-systemen: hoe kunnen organisaties maximaal rendement halen uit hun investeringen?
- Bedrijfsstrategie: wordt IT effectief gebruikt? En zo niet, welke complementaire bedrijfsmiddelen zijn er nodig om dit te realiseren?
- Globalisering: wordt er gebruikgemaakt van IT-middelen (bij voorkeur gestandaardiseerd) die mondiaal ondersteund worden, zodat de organisatie de aansluiting internationaal niet mist?
- IT-infrastructuur: is de IT-infrastructuur flexibel en schaalbaar ingericht om de snelle innovatieve IT-ontwikkelingen te kunnen volgen?
- Complexiteit en beveiliging: hoe kunnen organisaties hun IT-systemen beveiligen zonder dat het gebruik en beheer te complex worden?

Deze punten worden later gebruikt om de voor virtualisatie relevante onderwerpen binnen COBIT te identificeren.

VIRTUALISATIEMANAGEMENT-CYCLUS

De in het eerste deel van het artikel beschreven casus staat niet op zichzelf. Het blijkt dat een aantal fasen – cycli – standaard doorlopen wordt bij een virtualisatietraject binnen een organisatie [MARS06]. De basis van deze cyclus is de door Deming beschreven *plan-do-check-act*-cyclus.

Om tot de virtualisatiemanagementcyclus te komen, is gekozen voor COBIT, omdat dit raamwerk zelf een cyclus alsmede alle IT-processen beschrijft. COBIT beschrijft de volgende hoofdfasen: planning en organisatie, acquisitie en implementatie, levering en ondersteuning en ten slotte evaluatie en *monitoring*. Een *mapping* van deze hoofdfasen van COBIT met de praktijkcasus resulteert in de zes fasen die zijn weergegeven in figuur 1. Bij de verdere uitwerking van het raamwerk wordt gebruik gemaakt van de processen die in COBIT bij de genoemde hoofdfasen horen.

Figuur 1 De zes fasen van de virtualisatiemanagementcyclus

VIRTUALISATIE IT-DOMEINEN EN -OBJECTEN

De genoemde fasen bevatten voor virtualisatie relevante auditobjecten. Om straks bij de synthese van het virtualisatieraamwerk op een effectieve wijze een selectie te maken uit COBIT, is besloten om gebruik te maken van een objectgeoriënteerde auditaanpak. Deze aanpak is ontleend aan NOREA-geschrift nr. 1 [NORE98].
Met betrekking tot virtualisatie zijn de domeinen Informatiestrategie, Informatiemanagement/Informatietechnologiemanagement (IM/IT-management), Technische systemen en Operationele ondersteuning interessant. Omdat er bij virtualisatie geen sprake is van ontwikkeling van een informatiesysteem, valt het domein Informatiesysteem weg. Ook wordt virtualisatie niet gebruikt om industriële processen te ondersteunen en is het domein Processystemen niet relevant. Omdat de keuze voor virtualisatie moet aansluiten op de organisatiedoelstellingen, is het domein Informatiestrategie van belang. Het domein Informatiestrategie omvat objecten zoals het informatiebeleid, informatieplanning en informatiearchitectuur. Hierna ga ik in op de overige domeinen.

Met betrekking tot IM/IT-management kunnen de volgende objecten onderscheiden worden in relatie tot virtualisatie: plannen en organiseren, budgetteren, beslissen en innoveren. Een verdere verbijzondering leidt tot meer concrete auditobjecten. Hierbij valt te denken aan het definiëren van de doelstelling ten aanzien van technische systemen, het maken van businesscases ten behoeve van prioriteitsstelling van projecten en het bepalen van prioriteiten voor de introductie van nieuwe technologieën.
De Operationele automatiseringsondersteuning van een organisatie en het domein Technische systemen hebben betrekking op de installatie, het beheer en het onderhoud van de automatiseringsmiddelen die ter beschikking staan van een organisatieonderdeel. Tot deze domeinen behoren de beheerorganisatie, beveiliging, autorisatie, risicomanagement, resource management, capaciteits-

management en versiebeheer.
Bij al de van toepassing zijnde domeinen met bijbehorende objecten zijn ook de kwaliteitsaspecten te benoemen. Deze zijn ook beschreven in NOREA-geschrift nr. 1 en worden later ook gebruikt bij de totstandkoming van het virtualisatieraamwerk.

UITWERKING VIRTUALISATIE-MANAGEMENTCYCLUS

De volledige virtualisatiemanagementcyclus komt tot stand als synthese van de kernpunten uit de vorige paragrafen. Recapitulerend: als kapstok worden COBIT 4.0 en informatie uit de praktijkcasus gebruikt. Om de verzameling te beschrijven en processen gericht te selecteren, wordt gebruikgemaakt van een objectgeorienteerde aanpak. Om de processen met betrekking tot virtualisatie specifiek te maken, wordt een *mapping* uitgevoerd tussen de processen en de genoemde aandachtspunten en toepassingen betreffende virtualisatie. In figuur 1 is de virtualisatiemanagementcyclus afgebeeld met daarin de onderkende fasen. De aanleiding tot virtualisatie vloeit voort uit de *business-IT-alignment*-eisen en bedrijfsdoelstellingen. In dit specifieke geval van virtualisatie gaat het erom dat IT op een efficiënte en effectieve wijze de business ondersteunt. De aandachtspunten hierbij zijn de bedrijf- en IT-strategie en het IT-beleid.
Nadat de IT-manager onderkend heeft dat er geïnvesteerd dient te worden in IT om de efficiëntie en effectiviteit van IT – en dus van de business – te verbeteren, vindt een vooronderzoek plaats. De huidige TCO en benutting van *serverprocessor*capaciteit en bijbehorende knelpunten dienen eerst in kaart te worden gebracht. Ook de principes, voor- en nadelen van de verschillende virtualisatieproducten worden in deze fase geanalyseerd.
Voorafgaande aan een beslissing wordt nu een businesscase opgesteld. Deze bevat onder meer een kostenanalyse, impactanalyse op de bestaande systemen en organisatie, gemoeide risico's, verwachte ROI en verwachte niet-financiële baten. De totstandkoming van de definitieve besluitvorming is ook een punt van aandacht. Hierbij spelen de bevoegdheden en prioritering van investeringen een rol.
De businesscase dient als input voor de aanschaf van soft- en hardware. Na het aanvragen en vergelijken van offertes worden er keuzes gemaakt voor producten en leveranciers. Na de aanschaf wordt zowel soft- als hardware geconfigureerd en geïnstalleerd. Doorlooptijd en budget zijn essentieel in deze fase. Niet minder belangrijk is om de gebruikers op te leiden in de bediening en het gebruik van de nieuwe systemen.

Op het gebied van beheer zijn wijzigingsbeheer, versiebeheer, licentiebeheer, capaciteitsbeheer, autorisatiebeheer en *back-up* en *recovery* van belang. Ook het aantal bestede uren aan opdrachten, gemaakte kosten en de kwaliteit van de dienstverlening zijn relevante aspecten. Een bijkomend punt van aandacht is de beveiliging van de configuratiebestanden van de virtuele machines. Verder is het van belang dat de nodige functiescheiding is aangebracht binnen de beheerorganisatie. Beheerders van de virtualisatielaag en de virtuele machines dienen gescheiden te zijn van beheerders van het besturingssysteem en applicatie.
In de monitoring- en evaluatiefase wordt geanalyseerd of de beoogde baten door middel van virtualisatie zijn gehaald. Hierbij gaat het om zowel financiële als niet-financiële zaken. In het geval van virtualisatie gaat het hier voornamelijk om de kwaliteitsaspecten efficiëntie, effectiviteit, vertrouwelijkheid, integriteit en beschikbaarheid. Verder wordt ook gekeken in hoeverre aan de *service levels* wordt voldaan. In tabel 1 staat een overzicht van alle fasen uit de virtualisatiemanagementcyclus en de onderliggende aandachtsvelden.

UITWERKING FASEN VIRTUALISATIEMANAGEMENTCYCLUS

Per fase en bijbehorende aandachtsgebieden kan een verdiepingsslag gemaakt worden. Om u een idee te geven hoe dit uitgewerkt kan worden, is de fase 'Beheer en exploitatie' uitgewerkt in tabel 2. In de eerste kolom wordt het aandachtspunt vermeld, waarna in de tweede kolom mogelijke risico's worden weergegeven. In de derde kolom worden richtlijnen gegeven, die gerelateerd zijn aan het aandachtspunt en bijbehorende risico's. In

1. Businessbehoefte	2. Vooronderzoek	3. Besluitvorming	4. Acquisitie en implementatie	5. Beheer en exploitatie	6. Evaluatie en monitoring
IT-strategie	Kennis vergaren	Businesscase	Aanschaf middelen	Organisatie	Kosten-batenanalyse
IT-beleid	Marktanalyse	Project- prioritering	Training en opleiding	Wijzigingsbeheer	Prestatieanalyse
	Inzicht TCO	Bevoegdheden	Standaardisatie	Kostenbeheer	Audits
	Identificeren knelpunten	Risicoanalyse	Migratie	Versiebeheer	Service level management
		Impactanalyse		Capaciteitsbeheer	
		Kosten/baten-analyse		Autorisatiebeheer	
				Licentiebeheer	
				Back-up en restore	
				Patch- en releasebeheer	
				Informatiebeveiliging	

Tabel 1 Fasen van de virtualisatiemanagmentcyclus met onderliggende aandachtsgebieden

5. Beheer & exploitatie	Risicoanalyse	Richtlijnen	Kwaliteitsaspect
Organisatie	Indien in de beheerketen beheerders meerdere taken uitvoeren waarbij ook nog alle bevoegdheden binnen één functie liggen, kan dit leiden tot functievermenging. Het gevolg is dat misbruik kan worden gemaakt van de systemen zonder dat dit te achterhalen is. Er is geen 'tegengesteld belang' in de keten aanwezig om een adequaat AO/IC te waarborgen.	Er dient een functiescheiding te zijn tussen het beheer van de virtuele machines en het beheer van het guest-besturingssysteem en de bijbehorende applicatie op de virtuele servers.	Integriteit, beschikbaarheid en exclusiviteit.
Wijzigingsbeheer	Het onbeheerst aanmaken van virtuele machines leidt tot onoverzichtelijkheid, die het beheer niet ten goede komt. Hierdoor kunnen fouten worden gemaakt waardoor de BIE-kwaliteitsaspecten worden beïnvloed. Door de portabiliteit van virtuele machines kunnen complete servers met weinig inspanning worden verplaatst. Dit is ook een risico bij onbeheerst transport van virtuele servers naar de productieomgeving.	Er dienen duidelijke procedures te zijn beschreven betreffende de aanvraag, aanmaak, transport en beheer van virtuele servers. *Logging* en controle op naleving zijn essentieel in dit geval, om het wijzigingsbeheer proces te ondersteunen.	Integriteit, beschikbaarheid en exclusiviteit.
Kostenbeheer	Het ontbreken van inzicht in de aanschaf en beheerkosten na implementatie van virtualisatie, maakt het onmogelijk om te bepalen of virtualisatie het gewenste effect heeft gehad en maakt sturing ook onmogelijk. Hierdoor wordt een gekleurd beeld geschapen van de investering.	Stel een financieel model op om de gemaakte kosten die gemoeid zijn met de invoering van virtualisatie en het beheer bij te houden.	Effectiviteit en efficiëntie.
Versiebeheer	Het niet inzichtelijk hebben van de verschillende versies van virtuele machines kan leiden tot wildgroei van virtuele machines. Het gevolg hiervan is dat verkeerde versies gebruikt worden waardoor de BIE kwaliteitsaspecten worden aangetast.	Speciale aandacht moet worden besteed aan versiebeheer van de configuratiebestanden van de virtuele machines. Er dienen beschreven procedures te zijn om te waarborgen dat de juiste versies gebruikt worden en dat oude versies buiten gebruik gesteld worden.	Integriteit, beschikbaarheid en exclusiviteit.
Capaciteitsbeheer	Als er niet voldoende aandacht wordt besteed aan beschikbare en benutte capaciteit, bestaat het risico dat kritieke servers capaciteit tekortkomen, hetgeen de beschikbaarheid aantast.	De processorcapaciteit van fysieke en virtuele servers dient voortdurend gemonitord te worden. Voor kritieke servers is automatische dynamisch toewijzing van meer capaciteit zelfs aan te raden.	Beschikbaarheid.
Autorisatiebeheer	Beheerders die toegang hebben tot een server of data van anderen kunnen de BIE-aspecten aantasten.	Er dient gebruik te worden gemaakt van autorisaties om toegang tot de verschillende virtuele machines te beheersen. Hierbij hoort ook de scheiding van de diverse omgevingen.	Integriteit, beschikbaarheid en exclusiviteit.
Licentiebeheer	Het gebruik van software zonder zich aan de licentievoorwaarden te houden, kan leiden tot boetes.	Er dient aandacht te worden besteed aan licenties van besturingsystemen en applicaties. Hierbij speelt het principe van één licentie per fysieke CPU een belangrijke rol.	Effectiviteit.
Back-up en restore	Door het ontbreken van actuele back-up data en virtuele machines is het restoren of recovery onmogelijk, waardoor de continuïteit van bedrijfsvoering wordt verstoord.	Net als bij andere digitale gegevens moeten ook van virtuele machines regelmatig back-ups gemaakt worden.	Beschikbaarheid.
Patch- en releasebeheer	Het niet up-to-date houden van de virtualisatiesoftware kan mogelijke lekken in deze softwarelaag in stand houden. Die kunnen door onbevoegden misbruikt worden.	Besteed aandacht aan patch- en releasebeheer. Volg de richtlijnen van de leverancier om eventuele kwetsbaarheden tijdig te elimineren.	Integriteit, beschikbaarheid en exclusiviteit.
Informatiebeveiliging	Virtuele machines zijn in feite 'platte' bestanden en worden ook als bestanden opgeslagen. Het kopiëren van een complete server kost weinig inspanning. Ongeautoriseerd toegang tot deze bestanden kan dus van invloed zijn op de verschillende kwaliteitsaspecten.	Bestanden die betrekking hebben op virtuele machines – in feite de virtuele machines zelf - dienen veilig opgeslagen te worden. Alleen geautoriseerde medewerkers mogen toegang krijgen tot deze bestanden. Autorisatiebeheer en wijzigingsbeheer dienen het proces van informatiebeveiliging te ondersteunen.	Integriteit, exclusiviteit en beschikbaarheid.

Tabel 2 Uitwerking van de vitualisatiemanagementcyclus, Beheer & Exploitatie

de laatste kolom staan de kwaliteitsaspecten die van toepassing zijn.

CONCLUSIE

De IT-auditor kan een belangrijke rol vervullen in het hele virtualisatietraject. Met de virtualisatiemanagementcyclus heb ik getracht om een aanzet te geven voor een raamwerk dat de IT-auditor daarbij kan hanteren. ■

Literatuur

[LAUD06] Laudon, K.C. en J.P. Laudon, *Bedrijfsinformatiesystemen*, Prentice Hall, 2006.
[MARS06] Marshall, D., W.A. Reynolds en D. McCrory, *Advanced Server Virtualization*, Auerbach Publications, 2006.
[NORE98] Norea, *IT-auditing aangeduid*, NOREA-geschrift no. 1, NOREA, 1998.

ir. M.J. (Angelo) Montero RE is sinds 1 maart 2009 werkzaam bij de Rijksauditdienst. Daarvoor werkte hij bij de EDP Audit Pool als IT-auditor. Het artikel is gebaseerd op de afstudeerscriptie van de auteur in het kader van de afronding van de IT-auditopleiding aan de Vrije Universiteit in Amsterdam. Dit artikel is op persoonlijke titel geschreven.