CobiT en rapporteren over IT Governance

Bob van Kuijck en Bart Overbeek

De afgelopen jaren is duidelijk geworden dat de financiële markten geen genoegen meer nemen met enkel financiële berichtgeving van ondernemingen. De rapportage over interne beheersing in de vorm van 'In Control Statements' heeft haar entree gemaakt. Maar hoe sluit een dergelijke verklaring aan bij reeds aanwezige verklaringen over deelprocessen binnen ondernemingen?

Neem nu het voorbeeld van een verzekeringsmaatschappij. De pensioenuitvoerder wil als serviceorganisatie van een deelproces een SAS 70 verklaring ten behoeve van zijn klanten afgeven, de interne compliance-afdeling vraagt om aantoonbaar te voldoen aan de Wet Bescherming Persoonsgegevens en de organisatie als geheel wil een bedrijfsbreed In Control Statement afgeven. Ook bij de Vion Food Group1 speelt een dergelijk issue aangezien de Raad van Bestuur een In Control Statement wil afgeven. Dit artikel gaat specifiek in op de vraag hoe het management invulling kan geven aan de behoefte aan transparantie en zekerheid omtrent het functioneren van de ICT-organisatie als onderdeel van een 'Internal Control'-project.

Auteurs

dr. J.R.H.J. (Bob) van Kuijck RA RC, Corporate Director Internal Audit bij VION Food Group en Universitaire Hoofddocent aan de IT-auditopleiding van de VU.

drs. B. (Bart) Overbeek RE is Senior Internal Auditor bij VION Food Group.

Na enkele financiële debacles werd medio 2002 de Sarbanes Oxley wetgeving ingevoerd in de Verenigde Staten. Deze wetgeving heeft in de afgelopen jaren bij een behoorlijk aantal ondernemingen wereldwijd de projectenkalender beheerst. Voor een aantal Nederlandse ondernemingen die een beursnotering hebben in de Verenigde Staten was het boekjaar 2006 zelfs het jaar van de waarheid. Het jaarverslag over 2006 dient namelijk een 'Internal Control Statement' te bevatten dat beoordeeld is door een externe accountant. Ook de Nederlandse Code Tabaksblat heeft vele ondernemingen ertoe aangezet om transparant te maken hoe zij hun intern risicobeheersings- en controlesysteem hebben ingericht. Een behoorlijk aantal organisaties heeft in dit kader een proactieve houding aangenomen [KUIJ03] en heeft Internal Control-projecten opgestart zonder dat direct aan de SOx eisen voldaan moest worden. Daarbij hebben sommige ondernemingen gekozen voor een SOx-lite benadering [KUIJ06].
Een organisatie die een Internal Control-project opstart maakt veelal gebruik van *templates* die richting geven aan de uitwerking van de risicoanalyse en interne controle binnen reguliere bedrijfsprocessen, zoals inkoop en verkoop. Deze *templates* bevatten een algemene procesbeschrijving en een set van 'standaard' interne controlemaatregelen. In de praktijk zien we echter vaak dat ICT-processen en activiteiten summier worden behandeld of zelfs buiten beschouwing worden gelaten. Hoewel geautomatiseerde interne procescontroles onderdeel zijn van de bedrijfsprocessen, blijken er veelal geen templates beschikbaar voor de algemene processen in de ICT-organisatie (onder ander *change management en configuration management*). Zijn deze wel beschikbaar dan zijn ze vaak niet geïntegreerd of aan elkaar gerelateerd. Bovendien gebruikt de ICT-afdeling vaak haar eigen beheersingsmodellen om structuur aan te brengen in haar activiteiten. Daarbij kan worden gedacht aan ITIL, CMMI, ISO17799, CobiT [COBI05], Val IT en PRINCE2. Het beoordelen van de ICT in een Internal Control-project is dan ook een lastige zaak als rekening moet worden gehouden met deze verschillende raamwerken en standaarden. Het leidt er toe dat ICT als een losstaand onderdeel van een Internal Control-project wordt gezien. Dit artikel beoogt een aantal handvatten aan te reiken voor een organisatie om de beheersing van de ICT te operationaliseren in het kader van een Internal Control-project.

Diversiteit aan ICT-beheersingsmodellen

Een centrale ICT-afdeling van een grote organisatie krijgt de laatste jaren van haar interne klanten allerlei vragen en verzoeken die direct gerelateerd zijn aan Internal Control-projecten of andere kwaliteitsprogramma's. In de basis hebben al deze vragen betrekking op de kerngebieden van interne beheersing zoals genoemd in het COSO-model, te weten betrouwbaarheid van de financiële verslaggeving, effectiviteit en efficiëntie van de beheersing van processen en het voldoen aan wet- en regelgeving. De vraag naar zekerheid over de interne ICT-beheersing kan uit verschillende hoeken van de organisatie komen en qua aard, diepgang en timing nogal eens verschillen.

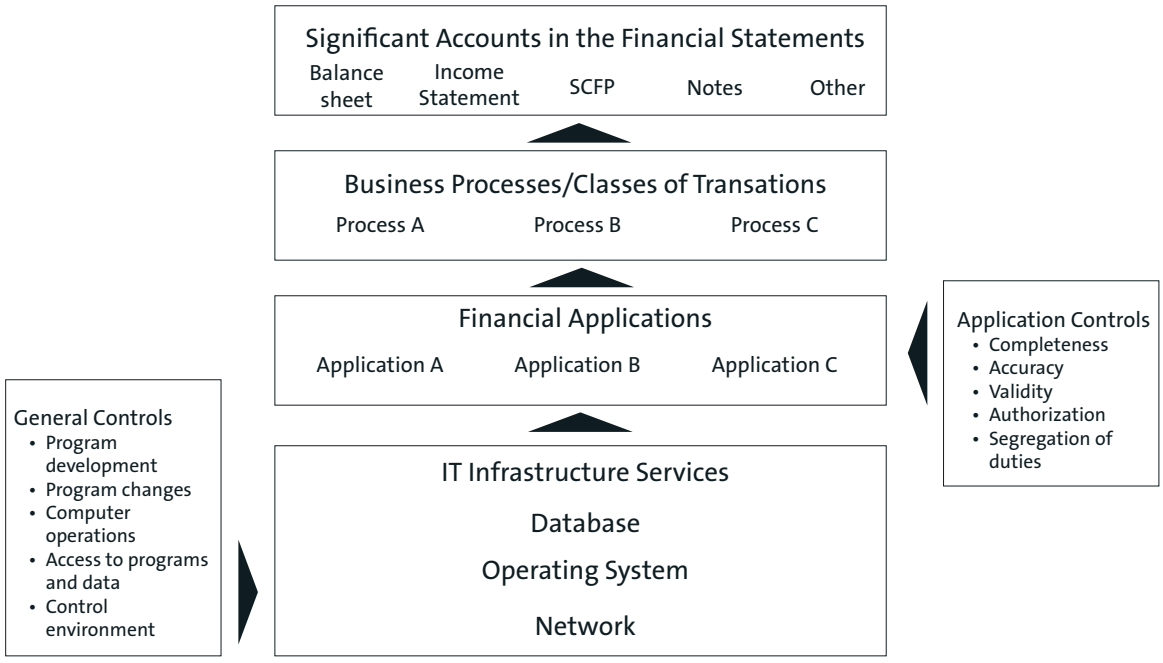
Het 'Service Level Management'-proces, waarbinnen de ICT-organisatie verantwoording aflegt over haar dienstverleningsniveau aan de organisatie, biedt onvoldoende informatie over de ICT-beheersing zoals bedoeld vanuit COSO perspectief. Veelal gaat het daarbij om de effectiviteit en efficiëntie van een bepaald deel van de ICT-organisatie. In Control-vraagstukken vereisen toch een bredere aanpak waarbij betrouwbaarheid van geautomatiseerde gegevensverwerking ten behoeve van een betrouwbare financiële verslaggeving en het voldoen aan wet- en regelgeving tenminste ook aandachtsgebieden zijn. Mulders beschrijft dit bijvoorbeeld in het kader van SAS 70 implementaties [MULD05].

Omdat veel van de door de ICT-organisatie gebruikte beheersingsmodellen toegesneden zijn op de beheersing van een specifieke problematiek is het begrijpelijk dat ieder model op zijn eigen gebied wordt ingezet. Het gevolg hiervan is dat er ook op verschillende plaatsen documentatie voorhanden is en modellen elkaar (deels) overlappen. In het kader van het afgeven van zekerheid over de kwaliteit van de ICT-beheersing is het duidelijk dat er behoefte is aan een eenvoudige – zelfs modulaire – ontsluiting van deze fragmentarische documentatie van risicoanalyses en interne beheersmaatregelen. Dit komt de efficiency ten goede en kan het afgeven van een In Control Statement vereenvoudigen. Ook Van den Biggelaar [BIGG04] geeft aan dat standaardisatie van de ICT-omgeving een 'Internal Control'-project efficiënter kan maken. Maar is het mogelijk om één, overkoepelend model in te zetten?

Structuur in ICT-beheersing

Alvorens in te gaan op een dergelijk overkoepelend model voor ICT-beheersing, wordt aandacht besteed aan de plaats van ICT-beheersing binnen de organisatie. Het ICT-management is primair verantwoordelijk voor de beheersing van de ICT-processen en ondersteunt de gebruikersorganisatie met ICT in de bedrijfsprocessen. De gebruikersorganisatie bepaalt in belangrijke mate hoe de bedrijfsprocesbeheersing wordt ondersteund door ICT-applicaties. Door de verantwoordelijkheden scherp te definiëren tussen enerzijds de gebruikersorganisatie en anderzijds de ICT-organisatie, wordt voorkomen dat overlap ontstaat tussen de verantwoordelijkheid in de verschillende beheersingsgebieden. Om dit duidelijk te maken wordt verwezen naar de relatie tussen bedrijfsprocessen en de financiële verslaglegging binnen een onderneming zoals weergegeven door het IT Governance Institute (zie figuur 1).

In een notendop laat figuur 1 zien dat *general controls* de beheersing waarborgen van de IT infrastructure services, die vervolgens applicaties ondersteunen. De applicaties bevatten *application controls*, die een bijdrage leveren aan de beheersing van bedrijfsprocessen. Deze bedrijfsprocessen voeden vervolgens de (financiële) verslaglegging binnen de onderneming.



Figuur 1: Positie van application controls en general controls binnen de organisatie (Bron:[ITGI06]).

General controls

De *general controls* kunnen worden omschreven als de maatregelen die zich richten op de beheersing van de basis ICT-processen. In figuur 1 is aangegeven dat deze controls met name betrekking hebben op de databases, operating systemen en netwerken. Daarnaast hebben ze ook betrekking op de algemene applicatiebeheersing, zoals het invoeren van wijzigingen in de programmatuur en algemene beveiligingsinstellingen van een applicatie. De gedefinieerde categorieën van controls, zoals 'Program Changes' en 'Computer Operations' vormen de minimale vereiste voor de betrouwbaarheid van financiële verslaglegging. Binnen de scope van een Internal Control Statement wordt uiteraard aan een meer brede beheersing van ICT-activiteiten geappelleerd.

Application controls

Naast *general controls* zijn ook *application controls* van belang bij het beheersen van ICT. *Application controls* zijn beheersmaatregelen die opgenomen zijn in applicaties (onder andere invoercontroles en autorisaties). *Application controls* maken daarmee onderdeel uit van de interne controle van een bedrijfsproces. Het bestaan van *application controls* in een applicatie op zich, is nog geen garantie voor een effectieve werking gedurende een bepaalde periode.

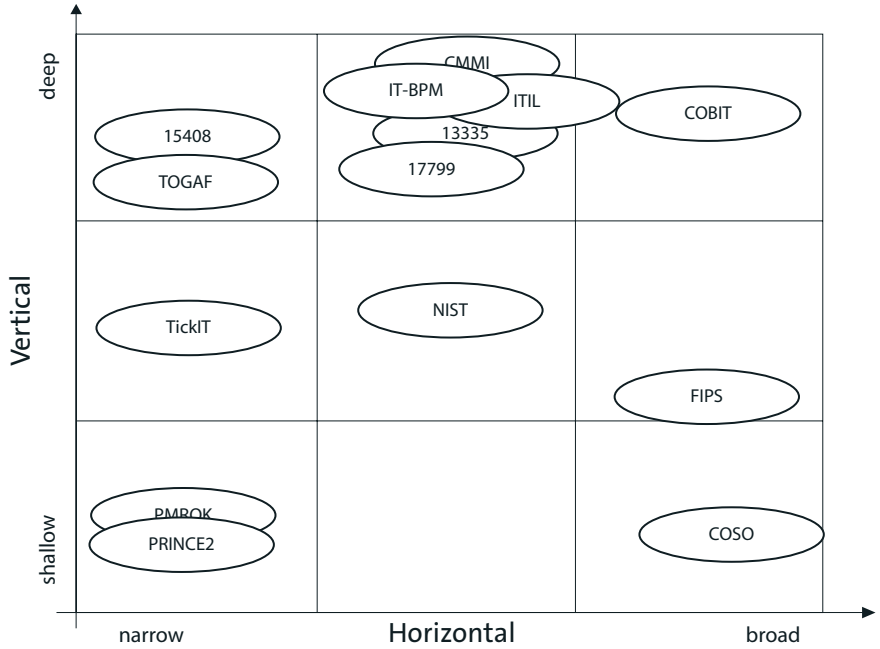
Het ICT-management is primair verantwoordelijk voor de *general controls*, terwijl de rest van de organisatie primair verantwoordelijk is voor *application controls*. Een dergelijk onderscheid maakt scherpere sturing binnen de organisatie mogelijk. De *application controls* zijn onderdeel van de reguliere bedrijfsprocessen. Op het snijvlak van 'business' en ICT komen de vraag naar ICT en het aanbod van ICT samen, ook wel het ontkoppelvlak genoemd. De vraag naar ICT wordt doorgaans vastgelegd in een programma van eisen, welke door de ICT-organisatie wordt vertaald in oplossingen. Voor het programma van eisen kan de ICT-organisatie echter geen verantwoordelijkheid nemen. Het snijvlak van 'business' en ICT is dan ook een gedeelde verantwoordelijkheid, waarbij naar onze mening de ICT-organisatie vanuit dienstverleningsoogpunt het initiatief neemt. De conclusie is dan ook dat activiteiten die moeten leiden tot een In Control Statement voor de ICT-organisatie, zich dienen te concentreren op de *general controls*. *Application controls* worden al meegenomen in de beoordeling van de reguliere bedrijfsprocessen.

CobiT als overkoepelend model

De SOx-wetgeving in de VS heeft er voor gezorgd dat de aandacht voor interne beheersing is toegenomen en dat het COSO-model als standaard voor interne beheersing wereldwijd nog meer is geaccepteerd. Het COSO-model wordt veel toegepast binnen organisaties voor de bedrijfsbrede beheersing van risico's. Het is echter niet specifiek ontwikkeld voor ICT-beheersing. ISACA heeft de afgelopen jaren nadrukkelijk geijverd om CobiT te laten aansluiten op IT-beheersing in het licht van de SOx-wetgeving. Maar sluit het model aan op de verschillende beheersingsmodellen die in gebruik zijn bij een onderneming, in feite de bestaande IT-governance structuur?

Het CobiT-model [COBI05] van het IT Governance Institute (ITGI) komt in diverse publicaties naar voren als overkoepelend raamwerk voor ICT-beheersing. Van den Biggelaar e.a. [BIGG06] spreken over een bruikbaar handvat voor het definiëren en implementeren van *key controls*. NOREA [NORE04] positioneert CobiT als governancemodel voor ICT-processen (*general controls*).

Het IT Governance Institute (ITGI) heeft in een publicatie een overzicht van *International IT Guidance* [ITGI06-1]



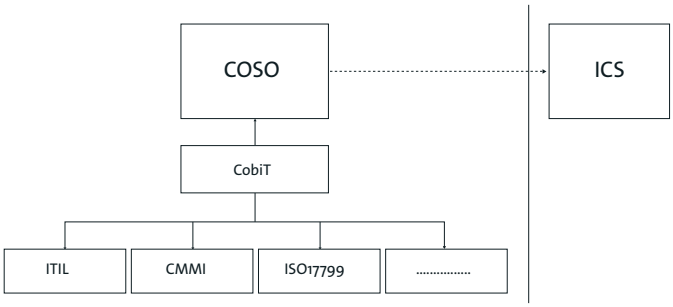
Figuur 2: De diepgang van ICT-beheersingsmodellen uitgezet tegen reikwijdte (Bron: ITGI06-1).

gegeven met daarbij een referentie aan haar 'eigen' model CobiT. De publicatie geeft inzicht in het toepassingsgebied van een aantal internationaal bekende ICT-beheersingsmodellen. De publicatie evalueert de reikwijdte en diepgang van de modellen. De reikwijdte van het model zegt iets over de mate waarin en de wijze waarop ICT-activiteiten binnen een organisatie door het model worden afgedekt. De diepgang van een model is van belang binnen een Internal Control-project. Enerzijds is dit noodzakelijk om de beheersing voldoende concreet te maken, zodat de ICT-beheersing vanuit de bestaande situatie aan het paraplumodel gekoppeld kan worden. Anderzijds moet het model voldoende fijnmazig zijn om tot een gebalanceerde verklaring te kunnen komen ten aanzien van de ICT-activiteiten binnen de onderneming. De diepgang en reikwijdte van de vergeleken modellen uit de eerder genoemde ITGI-publicatie zijn weergegeven in figuur 2.

Uit figuur 2 is op te maken dat CobiT zowel qua diepgang als ook reikwijdte het beste scoort ten opzichte van de andere modellen. Ook hier wordt weer benadrukt dat COSO voldoende breed is voor ICT-beheersing, maar zoals eerder besproken de diepgang ontbeert. Modellen als ITIL, CMMI en ISO17799 scoren relatief goed, maar missen de breedte die een paraplu-model in zich moet hebben.

Efficiency

Het transparant maken van de interne beheersing op ICT gebied dient op een efficiënte wijze te geschieden. Het overkoepelend model voor ICT-beheersing dient idealiter dan ook aan te sluiten bij de beheersingsmodellen die de onderneming reeds gebruikt bij specifieke ICT-processen. Daarbij moet zoveel mogelijk gebruik worden gemaakt van de reeds aanwezige documentatie, zodat zo min mogelijk aanvullende documentatie moet worden vervaardigd.
Relatief veel organisaties die werken aan een In Control Statement, hebben het COSO-model als uitgangspunt gehanteerd bij de start van een Internal Control-project en er bestaan diverse *mappings* van de control objectives uit CobiT naar het COSO-model. Daarnaast kan CobiT gebruik maken van de meer gedetailleerde modellen binnen de ICT-organisatie, zoals ITIL of CMMI. Ook het ITGI bevestigt deze zienswijze. Daarnaast wijst Fabian bijvoorbeeld op de onderlinge afhankelijkheid van ITIL en CobiT [FABI07]. De relatie tussen CobiT en andere modellen wordt weergegeven in figuur 3.
Het voorgaande maakt duidelijk dat CobiT voldoet aan de gestelde eis van efficiency en bovendien de gewenste breedte en diepgang mogelijk maakt. CobiT kan dus fungeren als paraplumodel binnen een bedrijfsbreed Internal Control-project. Kortom, COSO kan als algemeen raamwerk voor beheersing van bedrijfsrisico's worden gebruikt (inclusief *process controls* en *application controls*) en CobiT specifiek voor de beheersing van ICT-processen. Door de inzet van CobiT wordt maximaal een aansluiting gemaakt met de bestaande IT governance-structuur en wordt additionele documentatie binnen de organisatie beperkt.



Figuur 3: CobiT en bestaande ICT-beheersingskaders.

De theorie in de praktijk

De vraagstelling uit de introductie van dit artikel was hoe het management binnen een organisatie zekerheid en transparantie kan verschaffen omtrent het functioneren van de ICT-organisatie. Uit de evaluatie van de eisen te stellen aan een ICT-beheersingsmodel blijkt dat CobiT voldoet als te hanteren procesmodel. Maar hoe kan dit worden geoperationaliseerd in de praktijk? Concreet zal er een aantal stappen doorlopen moeten worden om tot een 'gevuld' ICT-beheersingsmodel te komen. Hieronder worden de stappen weergegeven en aansluitend besproken. Vervolgens wordt besproken hoe de VION Food Group CobiT operationaliseert binnen het lopende Internal Control-project.

Stap 1: Inventariseren bestaande detailmodellen
Stap 2. Inventariseren bestaande '*control activities*'
Stap 3: Vaststellen van de volledigheid van '*control activities*'
Stap 4: Selectie van '*key controls*'
Stap 5: Operationalisering van het Internal Control-raamwerk

Stap 1: Inventariseren bestaande detailmodellen

Het invoeren van CobiT start met de inventarisatie van reeds bestaande ICT-beheersingsmodellen in de organisatie. De gebruikte modellen zullen veelal op deelgebieden ingezet zijn binnen de organisatie. Zo zal bijvoorbeeld ITIL een geschikt model zijn voor de beheerorganisatie, terwijl CMMi meer geschikt is voor de ontwikkelorganisatie. De modellen worden geïnventariseerd en gepositioneerd binnen CobiT. Op deze wijze kan ook worden vastgesteld of alle ICT-elementen die nodig zijn voor het 'Internal Control Statement' (ICS) op hoofdlijnen zijn afgedekt.

Stap 2: Inventariseren bestaande control activities

De volgende stap betreft het inventariseren van bestaande *control activities* binnen de ICT-organisatie. Deze activiteiten hebben vaak al een plek gekregen binnen de detailmodellen zoals ITIL en CMMI. De *control activities* worden zo veel mogelijk via de bestaande modellen gekoppeld aan CobiT-processen. Bij deze inventarisatie is het erg belangrijk om de meest belangrijke controls op te nemen in het CobiT raamwerk, de zogenaamde *key controls*. Hoewel de *key controls* pas in een later stadium worden vastgesteld is het goed om de inventarisatie met deze focus uit te voeren. Op deze

wijze kan het aantal te monitoren beheersmaatregelen beperkt worden gehouden.

***Stap 3: Vaststellen van de volledigheid van** control activities*

De bestaande *control activities* worden voorts gekoppeld aan het CobiT-model. Hierdoor wordt duidelijk op welke vlakken nog geen *control activities* in de organisatie aanwezig zijn. In feite wordt CobiT gebruikt om de volledigheid van de ICT-beheersing te toetsen. CobiT-processen die niet zijn afgedekt kunnen alsnog ingevuld worden door nieuwe *control activities* te ontwerpen. Op het laagste niveau wordt binnen CobiT gesproken van meetbare indicatoren, die concreet genoeg aangeven in welke richting gezocht of ontworpen dient te worden. Kortom, CobiT is een goed hulpmiddel bij het opsporen of formuleren van ontbrekende *control activities.*

***Stap 4: Selectie van** key controls*

In deze stap dienen, in het hele spectrum van geïdentificeerde beheersmaatregelen binnen CobiT, de belangrijkste beheersmaatregelen (*key controls*) benoemd te worden. De *key controls* dienen voorts door de verantwoordelijke organisatie, in continuïteit, gemonitord te worden. Op deze wijze is het mogelijk periodiek een Internal Control Statement af te geven. Dit kan niet alleen voor de organisatie als geheel, maar ook specifiek voor (delen van) de ICT-beheersing.

Stap 5: Operationalisering van het Internal Control-raamwerk

In de laatste stap dient het Internal Control-raamwerk, gebaseerd op CobiT, in gebruik te worden genomen. Dit betekent dat de *key controls* met de bijbehorende frequentie beoordeeld moeten worden op effectieve werking, dat dit proces gemonitord dient te worden door de reviewers en dat de bevindingen gedocumenteerd dienen te worden.

In het navolgende wordt de uitvoering van het stappenplan binnen VION Food Group behandeld.

CobiT binnen VION Food Group

In de inleiding van dit artikel werd aangegeven dat VION Food Group (VION) werkt aan een project dat moet leiden tot een Internal Control Statement in het voorjaar van 2008. Ook de ICT-organisatie binnen VION is integraal onderdeel van dit Internal Control-project. Door VION is op basis van een voorstudie gekozen voor een combinatie van COSO en CobiT. De Internal Audit afdeling van VION ondersteunt de organisatie bij het bereiken van deze doelstelling, een werkwijze die wordt onderschreven door Lambeth [LAMB07].
De Internal Audit afdeling heeft eind 2006 binnen VION een ICT risico-inventarisatie uitgevoerd die is uitgemond in een strategie en een plan voor de audit van de ICT-organisatie in 2007-2008. Bij deze inventarisatie is gebleken dat de inzet van beheersingsmodellen binnen de ICT-organisatie nog beperkt is, waardoor deze ook nog onvoldoende bij kunnen dragen aan de vulling van het CobiT-model. Daarentegen wordt de invoering van CobiT dan ook niet belemmerd door reeds bestaande beheersingsmodellen en documentatie op het gebied van ICT. Ondanks dat modellen voor ICT-beheersing nog beperkt zijn ingevoerd en *control activities* niet of nauwelijks zijn gedocumenteerd, zijn deze in praktijk vaak wel (impliciet) aanwezig.

Bij het inventariseren van aanwezige *control activities* binnen VION heeft de Internal Audit afdeling een instrumentele rol. Door ICT-audits uit te voeren binnen de ICT-organisatie wordt gezamenlijk met de betrokkenen vastgesteld welke *control activities* op ICT gebied reeds beschikbaar zijn en welke nog ontbreken. Door gebruik te maken van actieplannen wordt invulling gegeven aan het proces van verbetering van ICT-beheersing. Hierbij worden niet alleen beheersmaatregelen benoemd die een betrouwbare geautomatiseerde gegevensverwerking moeten waarborgen, maar wordt ook aandacht besteed aan de efficiency en effectiviteit van ICT-processen. Tegelijkertijd wordt in dit proces documentatie gegenereerd en de *key controls* geselecteerd die worden opgenomen in CobiT. Vervolgens wordt de structurele monitoring opgestart. Conform het ICT-auditplan 2007-2008 zal in de beginjaren de focus zich richten op de belangrijkste processen en in de loop van de jaren worden gradueel alle ICT-processen in kaart gebracht.
Het documentatie- en monitoringproces in de organisatie kan ondersteund worden door een geautomatiseerde tool die de documentatie, de noodzakelijke monitoring en de rapportage over de effectiviteit mogelijk maakt. Binnen VION wordt hiervoor reeds gebruikgemaakt van de tool BWise die ook wordt ingezet voor het SOx-lite project [KUIJ06]. De documentatie bestaat doorgaans uit procesbeschrijvingen waarin de *key controls* geïdentificeerd worden, daarnaast worden de *key controls* nader gespecificeerd in matrices. Per key control worden een aantal kenmerken vastgelegd, zoals het risico dat wordt gemanaged, de frequentie waarmee de key control wordt gemonitord en de verantwoordelijke reviewer.
De CobiT-processen zullen binnen BWise op vergelijkbare wijze als de andere bedrijfsprocessen binnen VION worden vastgelegd. De verantwoordelijke ICT-managers worden vervolgens periodiek gevraagd om van de benoemde *key controls* aan te geven of deze effectief werken binnen de processen. Deze informatie over de ICT-beheersing vormt de basis om tot een *In Control Statement* te komen voor de ICT-organisatie als onderdeel van het bedrijfsbrede In Control Statement.

Conclusie

De combinatie COSO-CobiT is een veel voorkomende combinatie binnen organisaties die een In Control Statement (willen) afgeven. Met name op het terrein van *control over financial reporting* ten behoeve van SOx-compliance komt het gebruik van COSO en CobiT regelmatig voor. Ondanks dat de scope binnen dergelijke omgevingen beperkt blijft tot de betrouwbaarheid van financiële verslaglegging, kan CobiT ook goed in een breder kader worden ingezet. De Internal Control-projecten die binnen veel organisaties momenteel

worden uitgevoerd, zoals ook binnen de VION Food Group, hebben behoefte aan een dergelijk breed inzetbaar model dat bovendien de juiste diepgang kent. Daarnaast is met name de inpasbaarheid van CobiT binnen bestaande beheersingsmodellen op het gebied van ICT een belangrijke eis. CobiT geeft hier goed invulling aan doordat het model als paraplu kan fungeren voor de ICT-beheersing. Bestaande beheersingsmodellen, zoals ITIL en CMMI, kunnen binnen het CobiT-raamwerk worden verankerd en geven meer in detail aan hoe de ICT-activiteiten kunnen worden ingericht en beheerst. CobiT heeft in dit opzicht met name de control-focus en bewaakt de volledigheid van de ICT-beheersing. ■

Literatuurverwijzingen

[BIGG04] drs. ing. S.R.M. van den Biggelaar RE, Standaardisatie van alles: de laatste trend?, Compact, 2004/4.

[BIGG06] drs. ing. S.R.M. van den Biggelaar RE, drs. S. Janssen RE, drs. G.J.L Lamberiks; SAS 70 in een ICT-fabriek; Accesoire, fabrieksoptie of onderdeel van de standaard?; Compact, 2006/1.

[COBI05] IT Governance Institute, Control Objectives for Information and Related Technology, 4th Edition, 2005.

[FABI07] R. Fabian, Ph.D., I.S.P., Interdependence of CobiT and ITIL, Information Systems Control journal, volume 1, 2007.

[ITGI06] IT Governance Institute, IT Control Objectives for Sarbanes-Oxley, The Role of IT in the Design and Implementation of Internal Control over Financial Reporting, 2nd Edition, September 2006.

[ITGI06-1] IT Governance Institute, CobiT Mapping, Overview of International IT Guidance, 2nd Edition, 2006.

[KUIJ03] dr. J.R.H.J. van Kuijck RA RC, drs. R.J. Bogtstra RA CIA, De managementverklaringen in Sarbanes-Oxley, Naar een beheerst en transparant proces van externe informatieverschaffing, Compact, 2003/3.

[KUIJ06] dr. J.R.H.J. van Kuijck RA RC, SOx-lite approach, Column de toestand in de auditwereld, Audit Magazine, december 2006.

[LAMB07] J. Lambeth, CISA, CISSP, Using CobiT as a Tool to Lead Enterprise IT Organizations, Information Systems Control Journal, Volume 1, 2007.

[MULD05] drs. H.A. Mulders RA, SAS 70-implementaties: kansen en bedreigingen, Audit magazine, 2005/9.

[NORE04] NOREA, IT Governance, een verkenning, 2004.

Noten

1. De Vion Food Group genereerde in 2007 wereldwijd een omzet van meer dan circa € 7,5 miljard met meer dan 15.000 medewerkers (www.vionfood.com). De Internal Audit afdeling biedt het hoofdkantoor van VION ondersteuning bij de invoering van het bedrijfsbrede 'In Control Statement'.