IT-auditing afbakenen in het kader van de jaarrekeningcontrole

Stan van Bommel en Mark van Goor

SAMENVATTING In dit artikel gaan wij in op de wijze waarop de accountant en IT-auditor gezamenlijk verantwoord invulling kunnen geven aan de jaarrekeningcontrole in een complexe IT-omgeving. Hierbij staat de selectie van general IT-controls centraal en wordt specifiek voor dit onderwerp een methodiek aangereikt om de selectie te onderbouwen en inzichtelijk te maken. Vanuit de praktijk merken wij dat er onduidelijkheid bestaat over de general IT-controls die jaarlijks dienen te worden onderzocht. Wij hebben daarom aan de hand van een concreet praktijkvoorbeeld een methode uitgewerkt op basis waarvan een gefundeerde selectie van te onderzoeken general IT-controls tot stand komt. Het inzicht in de onderbouwing van deze selectie krijgt vanuit klant- en vaktechnisch oogpunt steeds meer belang. De door ons uitgewerkte methode is direct toepasbaar in andere organisaties.

1 Inleiding

In het kader van de jaarrekeningcontrole steunt de accountant in toenemende mate op gegevens uit geautomatiseerde systemen. Om de betrouwbaarheid van deze gegevens te garanderen, dienen organisaties beheersmaatregelen te hebben geïmplementeerd ten aanzien van de automatisering. Deze algemene beheersmaatregelen worden ook wel aangeduid als 'general IT-controls'.

C.F. van Bommel RE en Drs. H.M. van Goor RE CISA zijn als IT-auditors werkzaam bij de afdeling Internal Audit van de PGGM. Zij houden zich onder andere bezig met het uitvoeren van interne risk based audits op IT-gebied. Daarnaast zijn zij betrokken bij de IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole en bij een aantal interne IT-projecten.
Met dit artikel willen de auteurs een bijdrage leveren aan de verdere professionalisering van IT-vakgebied in relatie tot de jaarrekeningcontrole. Zij houden zich aanbevolen voor uw reacties en verdere discussie over dit belangrijke onderwerp!

Om de general IT-controls in het kader van de jaarrekeningcontrole te onderzoeken, schakelt een accountant veelal een IT-auditor in. Zowel uit eigen ervaring als uit ervaringen uit de praktijk blijkt dat de samenwerking tussen de accountant en de IT-auditor vaak verre van optimaal is. De samenwerking tussen de accountant en IT-auditor voor het onderzoeken van de general IT-controls wordt bemoeilijkt door onduidelijkheden over definities, begrippen en methoden. Daarom hebben wij de theorie en praktijk met betrekking tot general IT-controls nader geanalyseerd. De inzichten die wij op grond van de analyse hebben verkregen, hebben wij binnen PGGM Internal Audit toegepast. Daarbij hebben wij een methodische benadering uitgewerkt ter onderbouwing van de selectie van de general IT-controls die in het kader van de jaarrekeningcontrole dienen te worden beoordeeld.

In onze uitwerking van de methodische benadering onderkennen wij drie hoofdonderwerpen:

1 het op basis van literatuur en praktijk definiëren van het begrip 'general IT-controls' en de methodische benadering daarvan;
2 het selecteren van de te onderzoeken general IT-controls in het kader van de jaarrekeningcontrole;
3 het vertalen van bevindingen uit general IT-controls onderzoeken naar de gevolgen ten aanzien van de jaarrekeningcontrole. Daarbij zal expliciet rekening worden gehouden met de aanwezigheid van compenserende maatregelen (application controls en user controls).

De drie hoofdonderwerpen werken wij uit in drie artikelen. Onderwerp 1, de analyse en de methodische benadering, hebben wij beschreven in een artikel dat is geplaatst in *Compact* 2004/2 (Van Bommel en Van Goor, 2004). In het voorliggende artikel werken wij

deze methodische benadering uit aan de hand van een concreet praktijkvoorbeeld (onderwerp 2). In het derde artikel zal de focus liggen op het vertalen van bevindingen met betrekking tot general IT-controls naar de gevolgen in het kader van de jaarrekeningcontrole (onderwerp 3). Daarbij zal onder andere worden ingegaan op de wijze waarop over bevindingen over general IT-controls wordt gerapporteerd en op de gevolgen voor de jaarrekeningcontrole indien er bevindingen zijn.

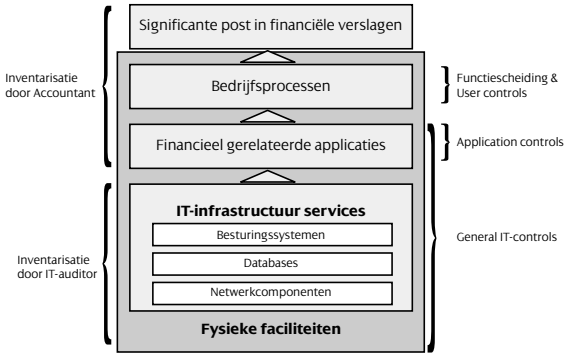
Allereerst schetsen wij in paragraaf 2 van dit artikel beknopt de theoretische achtergrond van onze methodiek. Vervolgens hebben wij in paragraaf 3 de methodiek uitgewerkt in een concreet praktijkvoorbeeld en tot slot hebben wij in paragraaf 4 een conclusie opgenomen.

2 General IT-controls: van theorie naar praktijk

Zowel uit eigen ervaring als uit ervaringen vernomen van vakgenoten merken wij dat er veel onduidelijkheid is over de precieze uitleg en de benadering van begrippen als general IT-controls, betrouwbaarheid en continuïteit. Daarnaast bestaat zowel bij de accountant als bij de IT-auditor onduidelijkheid over de selectie van general IT-controls die relevant zijn in het kader van de jaarrekeningcontrole. Op grond van de in de inleiding genoemde analyse hebben wij geconcludeerd dat beroepsorganisaties met name de vertaalslag tussen jaarrekeningposten, de geautomatiseerde gegevensverwerking en de general IT-controls nader dienen uit te werken en te actualiseren. Om invulling te geven aan deze vertaalslag pleiten wij voor het hanteren van een methodische benadering.

Onlangs is een nieuwe versie van de publicatie 'IT Control Objectives for Sarbanes-Oxley' verschenen (2004). Die publicatie bevat een figuur die nauw aansluit op de methodiek die wij hebben beschreven om de totstandkoming van de selectie van general IT-controls te bepalen en wij hebben de figuur daarom (aangepast) opgenomen. Op basis van de figuur kunnen organisaties inzichtelijk maken hoe financiële processen zijn ingericht en welke technologie kritiek is ter ondersteuning van die processen. Tevens is aan de linkerkant van de figuur onderscheid gemaakt in de delen die door de accountant dan wel de IT-auditor worden geïnventariseerd. Aan de rechterkant wordt onderscheid gemaakt in soorten controls die door de accountant en de IT-auditor worden beoordeeld in het kader van de jaarrekeningcontrole.

Figuur 1. Van posten in financiële verantwoordingen naar general IT-controls



Het startpunt van de methodiek is de jaarrekening van een organisatie. De accountant geeft invulling aan de jaarrekeningcontrole met behulp van een risicoanalyse (NIVRA, 2002). Hiervoor heeft de accountant een relatie gelegd tussen de balansposten en resultatenrekening in de jaarrekening van een organisatie en de onderliggende bedrijfsprocessen en ondersteunende applicaties. Op basis van het verkregen overzicht kan de IT-auditor vervolgens een relatie maken naar de bijbehorende onderliggende IT-infrastructuur. Daarna kan de accountant in samenwerking met de IT-auditor vaststellen welke general IT-controls minimaal moeten functioneren voor die organisatie. Hierbij maken wij gebruik van het CobIT- raamwerk (Control Objectives for Information en Related Technology (CobIT, 2000). Dit raamwerk is een internationale best practice voor IT-audits (zie voor relatie tussen accountantscontrole, COSO en CobIT: Koopman, 1998) en geeft inzicht in de beheersing van IT door het beschrijven van een set van beheersingsprocessen en -maatregelen. Vanwege het totaaloverzicht van beheersingsprocessen ten aanzien van IT-processen en de door CobIT in kaart gebrachte relatie tussen IT-beheersingsdoelstellingen en kwaliteitscriteria, leent deze standaard zich uitstekend voor het invullen van het onderzoek naar de general IT-controls. De in het kader van de jaarrekeningcontrole gehanteerde begrippen 'betrouwbaarheid' en 'continuïteit' hebben wij gekoppeld aan de relevante CobIT kwaliteitscriteria. Hierdoor ontstaat inzicht in beheersingsprocessen die aan 'betrouwbaarheid' en 'continuïteit' zijn gekoppeld. Deze selectie van beheersingsprocessen vatten wij op als general IT-controls. Dit overzicht dienen de accountant en IT-auditor te gebruiken voor het selecteren van general IT-controls voor de jaarrekeningcontrole. In

de bijlage van dit artikel is een nadere toelichting op CobIT opgenomen.

Als gevolg van het toepassen van bovengenoemde methodiek zijn de accountant en IT-auditor in staat om gefundeerd aan te geven welke onderzoeken de IT-auditor in het kader van de jaarrekeningcontrole moet uitvoeren. Ook kunnen zij hierover gezamenlijk verantwoording afleggen richting cliënten, toezichthouders en het maatschappelijk verkeer.

3 Praktijkvoorbeeld

Om concreet inzicht te geven in de wijze waarop de selectie van general IT-controls plaatsvindt, hebben wij de methodiek uitgewerkt door middel van een praktijkvoorbeeld. Daarbij hanteren wij de situatie bij het pensioenfonds PGGM waar wij als IT-auditor werkzaam zijn. PGGM is het pensioenfonds in de sector zorg en welzijn en beheert een pensioenvermogen van circa € 55 miljard ultimo 2003. Dit vermogen is opgebouwd uit jarenlang ontvangen pensioenpremies en beleggingsopbrengsten en vormt de bron voor het betalen van de pensioenen.
Het uitgewerkte voorbeeld is gebaseerd op de post 'premies'. Deze post betreft de premie-inkomsten die PGGM ontvangt van deelnemers aan de pensioenregeling van PGGM. Na de opbrengsten uit beleggingen is dit de grootste 'inkomende geldstroom' voor PGGM. Om inzicht te geven in de omvang van deze post hebben wij uit het jaarverslag 2003 van PGGM (2004) het mutatieoverzicht van het pensioenvermogen opgenomen (figuur 2).

Figuur 2. Mutatieoverzicht pensioenvermogen 2003

(Bedrag in miljoenen euro's)

	2003	2002
Aanwezig pensioenvermogen primo	*45.191*	*49.096*
Werkelijke baten en lasten		
Premies (15)	2.349	1.630
Waardeoverdrachten, per saldo (16)	73	-80
Pensioenen (17)	-1.528	-1.397
Pensioenuitvoeringskosten (18)	-110	-104
Overige baten en lasten, per saldo (19)	62	-69
Baten en lasten pensioenactiviteiten	**846**	**-20**
Opbrengst beleggingen (20)	6.951	-3.481
Rentelasten (21)	-3	-3
Kosten van vermogensbeheer (22)	-113	-96
Baten en lasten beleggingsactiviteiten	**846**	**-20**
Buitengewone baten en lasten (23)	**-12**	**-305**
Aanwezig pensioenvermogen ultimo	**52.860**	**45.191**

De post premies wordt samengesteld uit een aantal onderliggende posten (zie figuur 3), samengevoegd tot:
- 'Pensioen-, FLEX- en AP-regeling', premies voor reguliere pensioenopbouw;
- 'EP-regeling', periodieke premies voor een aanvullende pensioenproducten;
- 'Koopsommen', eenmalige premies voor aanvullende pensioenproducten.

Figuur 3. Totstandkoming post premies

(Bedrag in miljoenen euro's)

Posten van het mutatieoverzicht

15 Premies

Premies betreffen zowel periodieke als eenmalige koopsommen

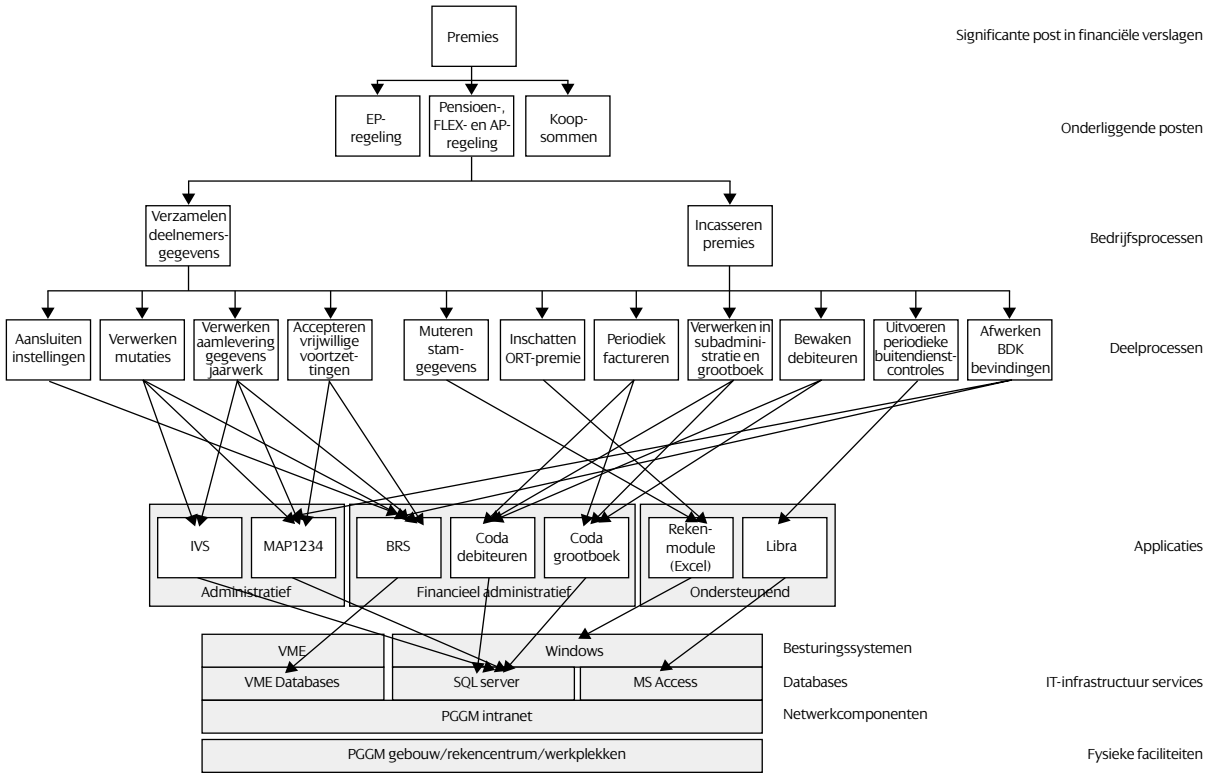
	2003	2002
Pensioenregeling	1.064	602
Flex-regeling	970	782
AP-regeling	276	241
EP-regeling	13	3
Totaal premies	2.323	1.628
Koopsommen	26	2
Totaal	**2.349**	**1.630**

Van de drie genoemde posten hebben wij de post 'Pensioen-, FLEX- en AP-regeling' verder uitgewerkt. Voor deze post hebben wij geïnventariseerd welke bedrijfsprocessen aan de post ten grondslag liggen en welke IT-objecten binnen deze bedrijfsprocessen worden gebruikt. In figuur 4 is het resultaat van onze inventarisatie weergegeven. Een toelichting op onze inventarisatie volgt in de paragrafen na de figuur. De toelichting is louter illustratief opgenomen om onze gedachtegang te volgen.

3.1 Van de post 'Pensioen-, FLEX- en AP-regeling' naar applicaties

Zoals ook in figuur 1 is aangegeven, vindt de vertaling van relevante posten naar applicaties plaats door de

Figuur 4. Uitwerking post premies



accountant. Daarbij is het startpunt het koppelen van de relevante posten aan processen. In ons praktijkvoorbeeld is het startpunt de post 'Pensioen-, FLEX- en AP-regeling'.

De post 'Pensioen-, FLEX- en AP-regeling' bestaat uit de twee processen, namelijk het verzamelen van deelnemersgegevens en het incasseren van premies.

Het doel van het proces 'verzamelen deelnemersgegevens' is het actueel houden van de gegevens die voor het incassoproces van belang zijn. Het startpunt van dit proces is enerzijds het registreren van instellingen die verplicht bij PGGM zijn aangesloten en anderzijds het accepteren en registreren van vrijwillige voortzettingen, oftewel deelnemers die buiten de verplichtstelling vallen. Door het jaar heen worden mutaties, zoals adreswijzigingen en in- en uitdiensttredingen, verwerkt die betrekking hebben op deelnemers aan de pensioenregeling. Na afloop van een jaar vindt verwerking van de aangeleverde definitieve gegevens inzake aangesloten instellingen en deelnemers plaats, het zogenaamde jaarwerk.

Het doel van het proces 'incasseren premies' is het borgen dat premies juist, volledig en tijdig worden geïnd bij instellingen en bij deelnemers. De premiepercentages worden als basis voor de premieberekening vastgelegd als stamgegevens. In de premie per deelnemer is een component opgenomen voor de premie met betrekking tot onregelmatigheid van werk. PGGM berekent deze specifieke component eenmaal per jaar door het inschatten van het onregelmatigheidstoeslag(ORT)percentage en het berekenen van de voorlopige premie hierover. Periodiek wordt aan de instellingen gefactureerd. De facturen verwerkt men daarna in de subadministratie en in het grootboek, op basis waarvan debiteurenbewaking plaatsvindt. Door het jaar heen controleren buitendienstmedewerkers de gegevens die door instellingen zijn aangeleverd omtrent deelnemers op juistheid en volledigheid. Het is mogelijk dat op basis van de bevindingen van deze buitendienstcontroles (BDK) vastgelegde gegevens worden gewijzigd.

Om de processen 'verzamelen deelnemergegevens' en 'incasseren premies' te kunnen uitvoeren, maakt

PGGM gebruik van de volgende applicaties:

- administratieve applicaties:
  - IVS (Individueel Verzekerdensysteem). Dit is een applicatie waarin de deelnemingen van enkele bijzondere instellingen en groepen deelnemers zijn vastgelegd;
  - MAP1234 (Migratie Architectuur Pensioenbedrijf). Binnen PGGM loopt een groot project genaamd MAP met als doel om in de komende jaren de huidige pensioensystemen stapsgewijs te migreren naar een nieuwe architectuur op basis van .Net. Het nieuwe pensioensysteem dat uit MAP voortkomt vervangt onder andere BRS;
- financieel administratieve applicaties:
  - BRS (Basis Registratie Systeem). Dit is een applicatie waarin gegevens over instellingen en deelnemers zijn vastgelegd;
  - CODA debiteuren. Dit betreft de subadministratie van debiteuren;
  - CODA grootboek. Dit betreft het centrale grootboek van PGGM;
- ondersteunende applicaties:
  - Rekenmodule. Dit betreft een 'end user computing toepassing' in Excel, waarmee pensioenmedewerkers berekeningen ten behoeve van BRS uitvoeren;
  - Libra (Laptop Interface Buitendienst voor Registratie van Afwijkingen). Dit is een applicatie die buitendiensmedewerkers gebruiken voor het raadplegen van gegevens uit BRS ten behoeve van de buitendienstcontrole. Bevindingen uit de controle worden in Libra geregistreerd en vervolgens in BRS verwerkt.

Tussen de genoemde applicaties bestaan relaties. Vanwege de overzichtelijkheid hebben we deze niet aangegeven in figuur 4.

3.2 Van applicaties naar general IT-controls

Zoals ook in figuur 1 is aangegeven, vindt de vertaling van applicaties naar general IT-controls plaats door de IT-auditor, aangezien voor deze vertaling een meer diepgaande ICT-kennis benodigd is van de ICT-infrastructuur die 'onder' de geïnventariseerde applicaties ligt. Op basis van de uitwerking van de post 'Pensioen-, FLEX- en AP-regeling' naar processen (door de accountant) is inzicht verkregen in ondersteunende applicaties, oftewel in de relevante IT-objecten op applicatieniveau. Vervolgens heeft de IT-auditor geïnventariseerd welke IT-infrastructuur services ten grondslag aan de applicaties liggen, waardoor de relevante IT-objecten inzichtelijk zijn. De volgende stap is dat de IT-auditor de IT-objecten aan CobIT koppelt, zodat blijkt welke general IT-controls in het kader van de jaarrekeningcontrole relevant zijn. Voor het koppelen hebben wij, als IT-auditor, gebruikgemaakt van de door CobIT aangegeven relevantie van IT-beheersdoelstellingen voor IT-objecten (zie bijlage), waarbij wij applicaties koppelen aan 'applications', besturingssystemen, databasemanagementsystemen en netwerken aan 'technology', databases aan 'data' en fysieke faciliteiten aan 'facilities'.

In tabel 2 is het resultaat van de koppeling van IT-objecten aan IT-beheersdoelstellingen weergegeven. Daarbij zijn alleen díe IT-beheersdoelstellingen opgenomen die betrekking hebben op de kwaliteitsdoelstellingen betrouwbaarheid of continuïteit. Hierdoor ontstaat inzicht in de IT-beheersdoelstellingen, oftewel de general IT-controls, die specifiek van toepassing zijn (in het kader van de jaarrekeningcontrole) voor de IT-objecten in dit uitgewerkte praktijkvoorbeeld. Uit de tabel wordt zichtbaar dat sommige IT-beheersdoelstellingen alleen betrekking hebben op applicaties, terwijl andere zich alleen richten op data, op technologie of op fysieke faciliteiten. Veel IT-beheersdoelstellingen raken meerdere categorieën van IT-objecten.

Uit de tabel blijkt ook dat er één IT-beheersdoelstelling is die in het geheel niet wordt geraakt door de IT-objecten, namelijk DS2 'Manage Third-Party Services'. Het is logisch dat DS2 in dit praktijkvoorbeeld niet van toepassing is, aangezien PGGM met betrekking tot de post 'premies' geen gebruikmaakt van diensten die worden geleverd door derden.

3.3 Van te onderzoeken general IT-controls naar een planning

Het uitgewerkte praktijkvoorbeeld heeft betrekking op slechts één post uit de jaarrekening van PGGM. Uiteindelijk moeten alle posten uit de jaarrekening via de aangegeven methodiek worden uitgewerkt door de accountant en IT-auditor, zodat de volledige omvang van de te onderzoeken general IT-controls inzichtelijk wordt. In eerste instantie lijkt het dat er daarna een grote hoeveelheid onderzoeken noodzakelijk zal zijn om alle general IT-controls af te dekken. Toch zal dit in de praktijk beperkt kunnen blijven, omdat veelal sprake zal zijn van uniforme IT-processen (general IT-controls) die van toepassing zijn voor veel, dan wel voor alle, onderzoeksobjecten. Hierbij kan bijvoorbeeld worden gedacht aan één uniform proces voor wijzigingenbeheer (CobIT AI6) voor alle relevante IT-objecten binnen een organisatie.

Naast het feit dat veelal sprake zal zijn van uniforme processen, is er nog een tweede reden waarom de hoeveelheid uit te voeren onderzoeken beperkt is. Het is immers niet noodzakelijk om ieder jaar alle general IT-controls met dezelfde diepgang te onderzoeken. Logischer is het hanteren van een meerjarencyclus.

Met betrekking tot ons praktijkvoorbeeld hebben wij voor de te onderzoeken general IT-controls een meerjarencyclus uitgewerkt. De frequentie van het moment waarop onderzoeken plaatsvinden is tot stand gekomen op basis van een risicoafweging, waarbij wij het belang van de IT-beheersprocessen voor de bedrijfsvoering hebben bepaald. Hiervoor hebben wij een onderscheid gemaakt tussen de vier domeinen van IT-beheersprocessen die CobIT kent.

Het *domein Delivery & Support* betreft de levering van de afgesproken IT-diensten inclusief de verwerking van data door informatiesystemen. Binnen deze diensten bevinden zich onder meer de traditionele beveiligings- en continuïteitsaspecten en training. Om deze diensten te leveren dienen ondersteunende IT-processen te zijn ingericht, die binnen CobIT zijn ondergebracht onder de overige drie domeinen Planning & Organisation, Acquisition & Implementation en Monitoring.
Het *domein Planning & Organisation* omvat de strategische en tactische aspecten van IT-beheersing en de identificatie van de beste manier waarop IT kan bijdragen om de doelstellingen van de organisatie te bereiken. Om de bij Planning & Organisation uitgewerkte IT-strategie te realiseren, moeten IT-oplossingen worden geïdentificeerd, ontwikkeld of aangeschaft, geïmplementeerd en geïntegreerd in de bedrijfsprocessen. Dit valt onder het *domein Acquisition & Implementation*, waaronder ook wijzigingen op en onderhoud van bestaande systemen vallen. Ten slotte omvat het *domein Monitoring* het sturingsmechanisme van het management en de onafhankelijke zekerheid geleverd door de interne en externe accountant en auditor of overigen. Dit houdt in dat alle IT-processen periodiek dienen te worden onderzocht op kwaliteit en op compliance met beheersingskaders.

In het kader van de jaarrekeningcontrole is het inherente risico van het domein Delivery & Support hoger dan het inherente risico van de andere drie domeinen. Immers, onder het domein Delivery & Support vallen de reguliere operationele IT-beheersprocessen. Daarom beschouwen wij de andere drie domeinen ondersteunend aan dit domein. Van de ondersteunende domeinen heeft het domein Acquisition & Implementation de meest directe relatie met het domein Delivery & Support. Overigens merken wij op dat de door ons gehanteerde hiërarchische indeling van de domeinen binnen CobIT zelf niet als zodanig wordt aangegeven; het betreft een eigen interpretatie van het raamwerk.

Binnen de vier genoemde domeinen kan nog een onderscheid worden gemaakt naar de relatie (primair of secundair, zie de toelichting op CobIT in de bijlage van dit artikel) van de IT-beheersprocessen met de kwaliteitsdoelstellingen betrouwbaarheid en continuïteit die relevant zijn in het kader van de jaarrekeningcontrole. Door vervolgens een weging aan te brengen tussen het resultaat van de combinatie domeinen/ inherent risico enerzijds en de primaire en secundaire relatie van de IT-beheersprocessen die onder de domeinen vallen anderzijds, is een categorie-indeling van relevantie van CobIT-domeinen (A-B-C-D) in het kader van de jaarrekeningcontrole af te leiden. Daarbij is de categorie A het meest relevant en de categorie D het minst. In tabel 1 zijn deze categorieën aangegeven, als eindresultaat van onze interpretatie.

Tabel 1. Categorieën van relevante CobIT-domeinen

	Relatie met kwaliteitsdoel-stellingen	
CobIT-domeinen	Primair	Secundair
Planning & Organisation	C	D
Acquisition & Implementation	B	C
Delivery & Support	A	B
Monitoring	C	D

De aangegeven categorieën kunnen de basis leveren voor een meerjarenplanning. Afhankelijk van de mate van relevantie zullen de domeinen met een bepaalde frequentie moeten worden onderzocht. De frequentie hangt samen met de jaarcyclus die wordt gehanteerd; in de praktijk komt vaak een driejaarscyclus voor.

Specifiek voor het praktijkvoorbeeld hebben wij tabel 2 aangevuld met een meerjarenplanning, op basis van een driejaarscyclus. Deze meerjarenplanning is het

eindresultaat van onze methodische benadering ter onderbouwing van de selectie van de general IT-controls die in het kader van de jaarrekeningcontrole dienen te worden beoordeeld.

Omdat de meerjarenplanning meerdere jaren omvat dient deze periodiek op actualiteit te worden getoetst en eventueel te worden aangepast. Zo dienen bijvoorbeeld nieuwe informatiesystemen in de planning te worden opgenomen en dienen uitgefaseerde informatiesystemen uit de planning te worden gehaald. Ook indien bijvoorbeeld een IT-proces (zoals Service Level Management) anders wordt ingericht, kan dit aanleiding zijn om de meerjarenplanning aan te passen. Een proces om te waarborgen dat dergelijke wijzigingen aan de Internal Audit worden doorgegeven is hierbij noodzakelijk.

Door het hanteren van een meerjarenplanning worden relevante processen in het kader van de jaarrekeningcontrole niet ieder jaar onderzocht. Om vast te stellen dat de uitvoering van deze processen niet is gewijzigd en dat processen goed hebben gelopen (bestaan en werking), dienen jaarlijks deelwaarnemingen te worden uitgevoerd, zodat toch zekerheid omtrent een betrouwbare werking wordt verkregen.

Toelichting bij tabel 2

In tabel 2 zijn horizontaal in de kop van de tabel de relevante door CobIT onderkende IT-beheersdoelstellingen, zoals 'PO2' en 'PO5' weergegeven. Voor iedere IT-beheersdoelstelling is in de rij onder de naam van de beheersdoelstelling aangegeven of deze betrekking heeft op 'betrouwbaarheid', aangegeven met een 'B' of op 'continuïteit', aangegeven met een 'C' (de rij 'kwaliteitsdoelstelling'). Een volledig overzicht van de IT-beheersdoelstellingen is opgenomen als bijlage.
Verticaal zijn in de tabel de relevante IT-objecten, zoals 'maatwerkapplicaties' en 'standaard applicaties' weergegeven. Voor ieder type IT-object is aangegeven welke concrete IT-objecten hier binnen PGGM onder vallen, als resultaat van de inventarisatie zoals aangegeven in figuur 4.
Vervolgens geeft de tabel aan, welke IT-beheersdoelstellingen betrekking hebben op welke IT-objecten.

Tabel 2. Selectie van general IT-controls en objecten van onderzoek

		General IT-controls (conform de CobIT-beheersdoelstellingen)																								
		PO2	PO5	PO8	PO9	PO11	AI2	AI3	AI4	AI5	AI6	DS1	DS2	DS3	DS4	DS5	DS6	DS9	DS10	DS11	DS12	DS13	M1	M2	M3	M4
Kwaliteitsdoelstellingen		B	B	B/C	B	B	B	B	B	B/C	B/C	B/C	B/C	C	C	B	B	B	C	B	B/C	B/C	B/C	B/C	B/C	B/C
Relvante objecten van onderzoek	Maatwerkapplicaties: - BRS - IVS - MAP - Libra	S	S	S	P/S	P/S	S		S	S	P/S	S		S	P	P/S	P	S	S			S	S	S	S	S
	Standaardapplicaties: - Coda debiteuren - Coda grootboek	S	S	S	P/S	P/S	S		S	S	P/S	S		S	P	P/S	P	S	S			S	S	S	S	S
	End user computing: - Rekenmodule	S	S	S	P/S	P/S	S		S	S	P/S	S		S	P	P/S	P	S	S			S	S	S	S	S
	Databases: - VME database - SQL server - MS Access	S		S	P/S					S	P/S	S			P	P/S	P		S	P		S	S	S	S	S
	Besturingsystemen: - VME - Windows		S		P/S	P/S		S	S	S	P/S	S		S	P	P/S	P	S	S				S	S	S	S
	Netwerk-componenten: - PGGM - intranet		S		P/S	P/S		S	S	S	P/S	S		S	P	P/S	P	S	S				S	S	S	S
	Fysieke faciliteiten		S		P/S	P/S			S	S	P/S	S		S	P	P/S	P	S	S		P	S	S	S	S	S

P: primaire relatie met kwalliteitsdoelstellingen
S: secundaire relatie met kwalliteitsdoelstellingen
B: betrouwbaarheid
C: continuïteit

Jaarlijks onderzoek
2-jaarlijks onderzoek
3-jaarlijks onderzoek
Geen onderzoek

Deze koppeling bestaat indien een 'P' of een 'S' is aangegeven op het snijvlak van een IT-object en een IT-beheersdoelstelling. Daarbij betekent een 'P' dat een IT-beheersdoelstelling een directe relatie heeft met een IT-object; bij een 'S' is de relatie minder sterk.
Ten slotte geven de kleuren in de tabel aan, met welke periodiciteit IT-beheersdoelstellingen onderzocht dienen te worden. Deze kleuren zijn afgeleid uit tabel 1, waarbij een 'A' uit tabel 1 is vertaald naar 'jaarlijks onderzoek', een 'B' naar '2-jaarlijks', een 'C' naar '3-jaarlijks' en een 'D' naar 'geen onderzoek'.

4 Conclusie

Om verantwoord invulling te geven aan de jaarrekeningcontrole in een complexe IT-omgeving dienen de accountant en IT-auditor nauw samen te werken. Hierbij dienen zij specifiek aandacht te besteden aan de onderbouwing en inzichtelijkheid van de selectie van relevante onderzoeksobjecten vanuit klant- en vaktechnisch oogpunt. Door gebruik te maken van de methodiek die wij in dit artikel via een praktijkvoorbeeld hebben uitgewerkt, kunnen deze doelstellingen worden bereikt. De onderbouwing is immers gestructureerd totstandgekomen en daardoor volgbaar. Op basis van de weergegeven tussen- en eindproducten kan op inzichtelijke wijze aan betrokkenen worden uitgelegd waarom naar bepaalde objecten wél onderzoek wordt verricht en naar andere niet. Het afleggen van verantwoording aan toezichthouders en het maatschappelijke verkeer wordt hierdoor ook beter mogelijk.

Hoewel het lijkt dat het IT-onderzoek omvangrijk wordt, zal dit in de praktijk meevallen zodra het stelsel eenmaal is ingericht. Dit komt omdat sprake is van een overlap van general IT-controls die relevant zijn voor bepaalde bedrijfsprocessen. Een onderzoek naar een general IT-control dekt immers meerdere bedrijfsprocessen af.

Door het inzichtelijk maken van de link van processen naar applicaties naar general IT-controls, kan de IT-auditor bij de uitvoering van zijn onderzoek zijn deelwaarneming zodanig kiezen dat díe objecten (applicaties) worden geraakt die relevant zijn in het kader van de jaarrekeningcontrole. Hierdoor krijgt de accountant zekerheid omtrent de betrouwbaarheid van de voor hem relevante objecten en kan hij zijn controlemix flexibel invullen. ■

Literatuur

Bommel, C.F. van en H.M. van Goor, (2004), IT-auditing in het kader van de jaarrekeningcontrole?, in: *Compact*, jg. 31, nr. 2, pp. 10-16.

IT Governance Institute, (2000), *COBIT, Third Edition – Control Objectives*, www.itgi.org.

IT Governance Institute, (2004), *IT Control Objectives for Sarbanes-Oxley – The importance of IT in the design, implementation, and sustainability of internal control over disclosure and financial reporting*, www.isaca.org.

Jaarverslag PGGM 2003 (2004).

Koopman, A. J.M., (1998), Accountantscontrole, COSO en CobIT, in: *Compact*, jg. 25, nr. 3, pp. 35-44.

NIVRA, (2002), *Richtlijnen voor de Accountantscontrole.*

Roos Lindgreen, E.E.O., (2005), COBIT. Opkomst, ondergang en opleving van een raamwerk voor informatiebeheersing, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 79, no. 5. pp. 206-211.

Zie bijlage op p. 292.

Bijlage

In tabel 3 hebben wij het CobIT framework weergegeven, bestaande uit:

- de beheersdoelstellingen (eerste kolom);
- de onderzoeksobjecten waarop de beheersdoelstellingen betrekking hebben (tweede, derde, vierde en vijfde kolom), waarbij de relevantie met een 'X' is weergegeven;
- de relaties met de kwaliteitsdoelstellingen en -criteria betrouwbaarheid (zesde, zevende en achtste kolom) en continuïteit (negende kolom). Voor het koppelen van de beheersdoelstellingen aan de kwaliteitscriteria maakt CobIT gebruik van een 'P' (Primair) en een 'S' (Secundair). 'Primair' houdt in dat de beheersdoelstelling direct van invloed is op een kwaliteitscriterium en in geval van 'Secundair' is de invloed op een kwaliteitscriterium beperkter of indirect. Alle beheersdoelstellingen waarachter een 'P' of een 'S' staat bij één of meerdere van de kwaliteitscriteria maken deel uit van het totale begrip general IT-controls.

Tabel 3. CobIT-beheersdoelstellingen gekoppeld aan onderzoeksobjecten en aan kwaliteitsdoelstellingen en -criteria

					Kwaliteitsdoelstellingen en –criteria			
	Onderzoeksobjecten				*Betrouwbaarheid*			*Continuïteit*
CobIT-beheersdoelstelling	Appli-cations	Techno-logy	Data	Facilities	Confiden-tiality	Integrity	Reliability	Availability
PLANNING & ORGANISATIE								
PO1 Define a Strategic Information Technology Plan	X	X	X	X				
PO2 Define the Information Architecture	X		X		S	S		
PO3 Determine Technological Direction		X		X				
PO4 Define the ICT Organisation and Relationships								
PO5 Manage the ICT Investment	X	X		X			S	
PO6 Communicate Management Aims and Direction								
PO7 Manage Human Resources								
PO8 Ensure Compliance with External Requirements	X		X				S	
PO9 Assess Risks	X	X	X	X	P	P	S	P
PO10 Manage Projects	X	X		X				
PO11 Manage Quality	X	X		X		P	S	
ACQUISITION & IMPLEMENTATION								
AI1 Identify Automated Solutions	X	X		X				
AI2 Acquire and Maintain Application Software	X					S	S	
AI3 Acquire and Maintain Technology Infrastructure		X				S		
AI4 Develop and Maintain Procedures	X	X		X		S	S	
AI5 Install and Accredit Systems	X	X	X	X		S		S
AI6 Manage Changes	X	X	X	X		P	S	P
DELIVERY & SUPPORT								
DS1 Define and Manage Service Levels	X	X	X	X	S	S	S	S
DS2 Manage Third-Party Services	X	X	X	X	S	S	S	S
DS3 Manage Performance and Capacity	X	X		X				S
DS4 Ensure Continuous Service	X	X	X	X				P
DS5 Ensure Systems Security	X	X	X	X	P	P	S	S
DS6 Identify and Allocate Costs	X	X	X	X			P	
DS7 Educate and Train Users								
DS8 Assist and Advise Customers	X							
DS9 Manage the Configuration	X	X		X			S	S
DS10 Manage Problem and Incidents	X	X	X	X				S
DS11 Manage Data			X			P	P	
DS12 Manage Facilities				X		P		P
DS13 Manage Operations	X		X	X		S		S
MONITORING								
M1 Monitor the Processes	X	X	X	X	S	S	S	S
M2 Assess Internal Control Adequacy	X	X	X	X	S	S	S	S
M3 Obtain Independent Assurance	X	X	X	X	S	S	S	S
M4 Provide for Independent Audit	X	X	X	X	S	S	S	S