IT-auditing in het kader van de jaarrekeningcontrole?

C.F. van Bommel RE en drs. H.M. van Goor RE CISA

Onduidelijkheden over definities, begrippen en methoden voor het onderzoeken van general IT controls bewogen de auteurs ertoe de theorie en praktijk nader te analyseren. Centraal in dit artikel staat de selectiemethode die leidt tot een onderbouwde invulling van de general IT controls die in het kader van de jaarrekeningcontrole dienen te worden onderzocht.

Inleiding

Bij publicatieplichtige ondernemingen moeten accountants conform de wet- en regelgeving in hun accountantsverslag een zinsnede wijden aan de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, tenminste als zij bij hun controle hieraan aandacht besteden. In onze externe en interne IT-auditpraktijkervaringen zien wij dat die zinsnede vaak het resultaat is van specialistisch onderzoek door de IT-auditor die apart is toegevoegd aan het accountantsteam. Onze ervaringen met verschillende benaderingswijzen en werkwijzen die wij de afgelopen jaren zijn tegengekomen, waren reden ons te bezinnen op de toegevoegde waarde van de verschillende benaderingen voor deze ondernemingen en op de doelmatigheid van de controle van de jaarrekening. Daarbij hebben wij binnen PGGM Internal Audit een aanzet gegeven de wettelijk voorgeschreven zinsnede te onderbouwen met een gestructureerde aanpak voor de onderhavige IT-audit. Omdat binnen de controle van de jaarrekening de externe accountant en IT-auditor beperkt tijd heeft voor een specifiek onderzoek naar de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, steunt hij bij het functioneren van een interne accountantsdienst vaak dankbaar op het werk van de interne IT-auditors. In die interactie is een goede onderlinge afstemming van het normenkader, de omvang en diepgang van het benodigde onderzoek en de auditaanpak essentieel.

In dit artikel behandelen wij het vraagstuk vanuit het algemeen aanvaarde CobIT-raamwerk voor de beheersing van IT. CobIT (Governance, Control and Auditing for Information en Related Technology ([Cobi00])) richt zich met name op wat wordt verstaan onder ‘general IT controls’ en is een internationaal veelgebruikte best practice voor IT-audits (zie voor de relatie tussen accountantscontrole, COSO en CobIT [Koop98] en voor benchmarking op basis van CobIT [Boer04]).

C.F. van Bommel RE
is als IT-auditor werkzaam bij de afdeling Internal Audit van de Stichting Pensioenfonds voor de Gezondheid, Geestelijke en Maatschappelijke Belangen (PGGM). Hij houdt zich onder andere bezig met het uitvoeren van interne risk-based audits op IT-gebied. Daarnaast is hij betrokken bij de IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole binnen PGGM.

stan.van.bommel@pggm.nl

Drs. H.M. van Goor RE CISA
is als IT-auditor werkzaam bij de afdeling Internal Audit van PGGM. Hij houdt zich onder andere bezig met het uitvoeren van interne risk-based audits op IT-gebied. Belangrijke aandachtsgebieden daarbij zijn de kwaliteit van ICT-processen, de betrouwbaarheid van interne applicaties en de implementatie van maatregelen met betrekking tot informatiebeveiliging. Daarnaast is hij betrokken bij een aantal interne IT-projecten en bij de IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole binnen PGGM.

mark.van.goor@pggm.nl

Een ander onderdeel van IT-auditing ten dienste van de jaarrekeningcontrole betreft het onderzoek naar de betrouwbaarheid van functionaliteit van geautomatiseerde informatiesystemen die onderdeel uitmaken van het 'financial reporting system' van organisaties. Dit zijn de zogenaamde application controls. Dit onderdeel hebben wij niet in dit artikel betrokken.

Onze vraagstelling

Bij aanvang van een jaarrekeningcontrole begint de accountant met het verzamelen en kennisnemen van informatie van de betreffende organisatie. Deze informatie gebruikt hij voor het vaststellen van de jaarrekeningposten en primaire bedrijfsprocessen. Als volgende stap inventariseert de accountant welke IT-objecten de primaire bedrijfsprocessen ondersteunen en welke IT-objecten relevant zijn in het kader van de jaarrekeningcontrole. Op basis van deze informatie bepaalt de accountant de mate van invloed van IT op de verwerking, opslag en communicatie van financiële informatie, administratieve organisatie en interne controle en op de beheersing van de onderneming. Deze werkzaamheden voert hij normaliter uit met behulp van de risicoanalyse van het NIVRA ([Nivr03]). Als resultaat van de risicoanalyse bestaat inzicht in de afhankelijkheden die specifieke jaarrekeningposten hebben ten opzichte van IT-objecten en daarmee de IT-risico's die een organisatie loopt.

Na afronding van de risicoanalyse stelt de accountant en/of IT-auditor vast welke beheersingsdoelstellingen van toepassing zijn rekening houdend met de relevante IT-objecten. Deze beheersingsdoelstellingen worden aangeduid als de general IT controls. Zowel uit eigen ervaringen, uit ervaringen van enkele vakgenoten, als uit eerdere publicaties (o.a. [Fijn00] en [Nivr95]) blijkt dat dit deel van het proces in het kader van de jaarrekeningcontrole een belangrijke vraag oproept:

Welke aspecten met betrekking tot general IT controls dienen te worden onderzocht in het kader van de jaarrekeningcontrole?

Om antwoord te krijgen op deze vraag hebben wij getracht via literatuurstudie en gedachtewisselingen met beroepsgenoten de volgende achterliggende vragen te beantwoorden:

- Wat vermeldt de wet- en regelgeving over IT-beoordeling in het kader van de jaarrekeningcontrole?
- Hoe hebben de beroepsorganisaties de wet- en regelgeving voor praktijktoepassing vertaald?
- Wat zijn general IT controls en welke kwaliteitsaspecten van general IT controls zijn object van onderzoek voor de jaarrekeningcontrole?
- Hoe kan invulling worden gegeven aan het IT-onderzoek in het kader van de jaarrekeningcontrole?

Het resultaat van onze studie is verwoord in dit artikel. De hierboven geformuleerde vragen zullen in het artikel worden beantwoord.

IT-beoordeling volgens wet- en regelgeving en beroepsorganisaties

Al in het begin van de jaren zeventig onderkende het NIVRA de invloed van de geautomatiseerde gegevensverwerking. Vanaf die tijd is een aantal NIVRA-geschriften en publicaties over dit onderwerp verschenen.

Een belangrijke ontwikkeling voor het vakgebied van IT-auditing is het per 1 maart 1993 van kracht worden van de Wet computercriminaliteit. De uitwerking van deze wet betreft onder meer artikel 393 lid 4 uit het Burgerlijk Wetboek deel 2. Dit artikel stelt dat '... de accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij tenminste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking ...'. De wetgever gaat er hierbij van uit dat de jaarrekeningcontrole een zekere beoordeling van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking omvat. De gevolgen van de Wet computercriminaliteit waren voor het NIVRA aanleiding om het geschrift 62 *Computercriminaliteit – De wetgeving, de gevolgen voor bedrijven en accountant* ([Nivr93]) op te stellen. Het doel van deze publicatie was de lezers inzicht te verschaffen in het fenomeen computercriminaliteit, de inhoud en de consequenties van de Wet computercriminaliteit en de rol die de accountant kan vervullen in het kader van de bestrijding van computercriminaliteit.

Vanwege de ontwikkelingen op IT-gebied werd in de loop der tijd de behoefte aan een eenduidig en algemeen aanvaardbaar kwaliteitsnormenstelsel binnen het vakgebied steeds groter. Om tegemoet te komen aan deze behoefte bracht het NIVRA in 1995 studierapport 34 uit, getiteld *Normatieve maatregelen voor de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole* ([Nivr95]). Het studierapport bevat een referentiekader voor general IT controls en application controls binnen automatiseringsorganisaties. Het begrip general IT controls wordt daarbij omschreven als: de maatregelen van interne controle in de automatiseringsorganisatie en in de systeemprogramma's, die ervoor zorgen dat de application controls blijvend en juist functioneren. Application controls omschrijft men als: de in de toepassingsprogramma's opgenomen maatregelen van interne controle. Met studierapport 34 beoogt het NIVRA richting te geven aan de beroepsuitoefening van de accountant die in het kader van de jaarrekeningcontrole geconfronteerd wordt met geautomatiseerde systemen. Studierapporten hebben echter geen dwingend karakter, wat betekent dat in de praktijk ook

andere benaderingswijzen acceptabel zijn. Hoewel studierapport 34 een belangrijke bijdrage levert aan de verdere professionalisering van het vakgebied van IT-auditors, is sinds het verschijnen van het studierapport het onderzoeksgebied van general IT controls nauwelijks verder uitgewerkt door beroepsorganisaties (zoals het NIVRA en de NOREA).

Sinds het verschijnen van studierapport 34 is het onderzoeksgebied van general IT controls nauwelijks verder uitgewerkt door beroepsorganisaties

Voorzover mogelijk maakt de accountant gebruik van een risicoanalyse conform de Richtlijnen Accountantscontrole ([Nivr03]) om invulling te geven aan de jaarrekeningcontrole. Specifiek geldt hiervoor de richtlijn 401 'Controle in een omgeving waarin gebruik wordt gemaakt van geautomatiseerde informatiesystemen', die ten doel heeft de grondslagen vast te stellen en aanwijzingen te geven met betrekking tot te verrichten werkzaamheden indien een controle wordt uitgevoerd in een omgeving waar van geautomatiseerde informatiesystemen gebruik wordt gemaakt. De richtlijn beschrijft onder andere het inschatten van het inherente risico en het interne beheersingsrisico met betrekking tot beweringen in de jaarrekening die van materieel belang zijn. Deze inschatting dient conform de richtlijn 400 'Risicoanalyse en interne beheersing' te worden gemaakt. Een direct verband tussen de posten in de jaarrekening en de concrete invulling van het general IT controls-onderzoek bevat de richtlijn niet. Door het ontbreken van een richtlijn op dit gebied zal iedere accountant en IT-auditor de invulling naar beste weten moeten geven.

Jaarrekeningcontrole en general IT controls

De theoretische invulling van general IT controls

Hoewel binnen de Nederlandse beroepsorganisaties geen eenduidige afbakening van het begrip general IT controls voorhanden is, vormen general IT controls binnen de vakgebieden van de accountant en IT-auditor een algemeen gehanteerd begrip. Zoals reeds eerder in dit artikel is aangegeven, ontleent het begrip zijn bestaansrecht aan de wettelijke taak van de accountant (BW2 artikel 393 lid 4).

Het NIVRA heeft in studierapport 34 ([Nivr95]) een definitie en een afbakening opgenomen van het begrip general IT controls. Als componenten van general IT controls beschouwt het NIVRA de volgende onderwerpen:
- logische toegangsbeveiliging;
- change en problem management;
- testproces;
- fysieke beveiliging;
- back-up, recovery en uitwijk.

Echter, gezien de vrijblijvende aard van het studierapport is deze opsomming niet als 'zaligmakend' bedoeld. De door het NIVRA verwachte brede discussie in de beroepsgroep en met de gebruikers van zijn rapportages over de exacte inhoud en de reikwijdte van de 'IT-audit ten dienste van de controle van de jaarrekening' is echter grotendeels uitgebleven.

Het boek *Elementaire theorie accountantscontrole* ([Deck98]), een boek dat wordt gebruikt bij één van de drie IT-auditopleidingen, beschrijft in aanvulling op de in studierapport 34 genoemde componenten van general IT controls ook:
- de organisatorische plaats van de afdeling Automatisering;
- de gebruikte apparatuur en programmatuur;
- de taakverdeling binnen de afdeling Automatisering;
- het beveiligingsbeleid.

Door de auteur wordt in het boek opgemerkt dat fysieke beveiliging, back-up, recovery en uitwijk alleen in opzet worden beoordeeld in het kader van de natuurlijke adviesfunctie.

In het *Handboek EDP-auditing* is een hoofdstuk gewijd aan general IT controls ([Hart00]). In dit hoofdstuk benoemt de schrijver een aantal onderwerpen dat onder het begrip general IT controls valt:
- functiescheiding en (logische) toegangsbeveiliging;
- wijzigingenbeheer (change management, inclusief problem management);
- continuïteit (fysieke beveiliging, back-up, recovery en uitwijk).

De genoemde onderwerpen komen grotendeels overeen met het eerdergenoemde studierapport 34, maar de opsommingen zijn niet volledig identiek: het testproces wordt niet expliciet genoemd.

Ook hebben wij geïnventariseerd wat de internationale beroepsorganisatie van accountants, de International Federation of Accountants (IFAC), meldt over general IT controls. In het boek *Principles of Auditing* ([Haye99]) zijn de volgende onderwerpen opgenomen die het begrip general IT controls afdekken:
- development (ontwikkeling);
- modification (wijziging);
- access (toegang);
- monitoring (bewaking).

Wanneer de hierboven vermelde opsommingen van componenten van general IT controls naast elkaar worden gelegd, blijkt dat ze niet volledig overeenkomen. Er is sprake van overlap, maar ook zijn er duidelijke verschillen te onderkennen.

De theorie van general IT controls toegepast in de praktijk

Niet alleen 'vanuit de beroepsorganisaties' komen we verschillende afbakeningen tegen van het begrip general IT controls. Ook in de praktijk bestaan diverse opvattingen over de wijze waarop dit begrip moet worden ingevuld. Zo worden general IT controls vaak gelijkgesteld met de volledige set van onderwerpen uit de Code voor Informatiebeveiliging, met delen van ITIL, of met de volledige set van beheersingsmaatregelen conform CobIT. Ook accountantskantoren hanteren in de praktijk verschillende benaderingswijzen en werkwijzen.

Tevens blijkt uit artikelen over jaarrekeningcontrole en IT-audit dat in de praktijk ook weer nieuwe onderwerpen aan de general IT controls worden gekoppeld, zoals het onderwerp gebruikerssatisfactie ([Kort99]). De vraag is echter of al deze één-op-één vertalingen en clusteringen wel terecht zijn. Binnen ons beroep wordt de basis voor het begrip general IT controls immers gelegd door wet- en regelgeving.

Relevante kwaliteitsdoelstellingen in het kader van de jaarrekeningcontrole

Het feit dat een concrete methode voor het afbakenen van het onderzoek van general IT controls ontbreekt en er geen directe relatie tussen de wet- en regelgeving en het begrip general IT controls is, heeft ons doen besluiten een andere invalshoek te zoeken, namelijk de invalshoek vanuit kwaliteitsdoelstellingen. De wet schrijft immers voor dat de accountant zijn bevindingen over de kwaliteitsdoelstellingen betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole kenbaar moet maken aan de Raad van Commissarissen en het bestuur. De schakel tussen deze wettelijke taak en de invulling van deze taak in de praktijk wordt derhalve gelegd door de begrippen betrouwbaarheid en continuïteit. Spijtig genoeg is in de wet geen toelichting opgenomen met een interpretatie van deze begrippen.

Uit literatuuronderzoek is gebleken dat ook binnen de beroepsorganisaties geen eenduidige terminologie over deze begrippen bestaat. Feitelijk hanteert de NOREA het begrip betrouwbaarheid niet. Daarnaast gebruiken het NIVRA en de NOREA de begrippen beschikbaarheid en continuïteit veelal als synoniem. In diverse publicaties van de beroepsorganisaties komen de begrippen als volgt terug:

- De NIVRA-geschriften 26 ([Nivr82]) en 53 ([Nivr89]) en het *Handboek EDP-auditing* ([Zwar92]) splitsen het begrip betrouwbaarheid op in de kwaliteitscriteria integriteit, exclusiviteit en controleerbaarheid. In plaats van de term continuïteit is gekozen voor beschikbaarheid; de termen zijn inhoudelijk echter synoniem. Het handboek bevat tevens definities van de genoemde criteria.
- Het NOREA Studierapport 2 ([Nore97]) vermeldt de begrippen betrouwbaarheid en continuïteit niet expliciet. Volgens dit studierapport hanteren IT-auditors alleen de kwaliteitscriteria integriteit, exclusiviteit, beschikbaarheid, controleerbaarheid, effectiviteit, efficiency en bescherming van waarden.
- Het NOREA Studierapport 3 ([Nore02]) vermeldt dat binnen de context van de NOREA de kwaliteitscriteria effectiviteit, efficiency, exclusiviteit, integriteit, controleerbaarheid, continuïteit en beheersbaarheid worden gehanteerd. Tevens wordt in dit studierapport opgemerkt dat in de literatuur de kwaliteitscriteria exclusiviteit, integriteit en controleerbaarheid ook wel worden aangeduid onder de gemeenschappelijke noemer betrouwbaarheid.
- In de handleiding *ZekeRE-business* ([Nore01]) wordt opgemerkt dat in de literatuur de kwaliteitscriteria continuïteit, exclusiviteit en integriteit ook wel worden aangetroffen onder de noemer beveiliging. Dit begrip heeft qua reikwijdte echter veelal betrekking op de meer fysieke en technische aspecten die met IT te maken hebben.

Een eenduidige terminologie voor de begrippen betrouwbaarheid en continuïteit ontbreekt

Uit het voorgaande blijkt dat een eenduidige terminologie voor de begrippen betrouwbaarheid en continuïteit binnen de wet- en regelgeving en de beroepsorganisaties ontbreekt. Ons inziens bevat studierapport 34 van het NIVRA de meest concrete en logische indeling, waarbij onderscheid wordt gemaakt tussen kwaliteitsdoelstellingen en kwaliteitscriteria.

- De *kwaliteitsdoelstelling* betrouwbaarheid omvat de *kwaliteitscriteria* exclusiviteit, integriteit en controleerbaarheid.
- De *kwaliteitsdoelstelling* continuïteit omvat het *kwaliteitscriterium* beschikbaarheid.

Het bovengenoemde onderscheid sluit aan op de wet- en regelgeving en komt grotendeels overeen met de visies van de beroepsorganisaties. Wij hanteren de genoemde kwaliteitscriteria daarom als uitgangspunt om de omvang van het onderzoek naar de geautomatiseerde gegevensverwerking nader te bepalen.

CobIT-beheersingsdoelstellingen		Kwaliteitsdoelstellingen en -criteria			
		Betrouwbaarheid			Continuïteit
		Confi.	Integ.	Relia.	Avail.
Planning & Organisation					
PO1	Define Strategic Information Technology Plan				
PO2	Define Information Architecture	S	S		
PO3	Determine Technological Direction				
PO4	Define ICT Organisation and Relationships				
PO5	Manage ICT Investment			S	
PO6	Communicate Management Aims and Direction				
PO7	Manage Human Resources				
PO8	Ensure Compliance with External Requirements			S	
PO9	Assess Risks	P	P	S	P
PO10	Manage Projects				
PO11	Manage Quality		P	S	
Acquisition & Implementation					
AI1	Identify Automated Solutions				
AI2	Acquire and Maintain Application Software		S	S	
AI3	Acquire and Maintain Technology Infrastructure		S		
AI4	Develop and Maintain Procedures		S	S	
AI5	Install and Accredit Systems		S		S
AI6	Manage Changes		P	S	P
Delivery & Support					
DS1	Define and Manage Service Levels	S	S	S	S
DS2	Manage Third-Party Services	S	S	S	S
DS3	Manage Performance and Capacity				S
DS4	Ensure Continuous Service				P
DS5	Ensure Systems Security	P	P	S	S
DS6	Identify and Allocate Costs			P	
DS7	Educate and Train Users				
DS8	Assist and Advise Customers				
DS9	Manage Configuration			S	S
DS10	Manage Problem and Incidents				S
DS11	Manage Data		P	P	
DS12	Manage Facilities		P		P
DS13	Manage Operations		S		S
Monitoring					
M1	Monitor Processes	S	S	S	S
M2	Assess Internal Control Adequacy	S	S	S	S
M3	Obtain Independant Assurance	S	S	S	S
M4	Provide for Independent Audit	S	S	S	S

P Primair
S Secundair

Confi Confidentiality
Integ Integrity
Relia Reliability
Avail Availability

Tabel 1. CobIT-beheersingsdoelstellingen gekoppeld aan kwaliteitscriteria.

Betrouwbaarheid, continuïteit en general IT controls

Binnen het vakgebied IT-auditing is CobIT een veelgebruikte 'best practice'-standaard. CobIT beschrijft een set van beheersingsprocessen en -maatregelen 'met als doelstelling om op een gestructureerde wijze een overzicht te bieden van de maatregelen voor de beveiliging van de IT' ([Coum99]). Vanwege het totaaloverzicht van beheersingsdoelstellingen ten aanzien van IT-processen en de in kaart gebrachte relaties tussen IT-beheersingsdoelstellingen en kwaliteitscriteria binnen CobIT leent deze standaard zich uitstekend voor het invullen van het onderzoek naar de general IT controls.

Het CobIT-model hanteert onder andere de kwaliteitscriteria confidentiality, integrity, reliability of information en availability. Deze criteria dekken volgens ons de begrippen betrouwbaarheid en continuïteit af, die de wet- en regelgeving hanteert. Door vervolgens een selectie te maken van de beheersingsdoelstellingen die een relatie hebben met de genoemde kwaliteitscriteria, kan op inzichtelijke wijze een afbakening van het begrip general IT controls worden vastgesteld.

In tabel 1 hebben wij de door CobIT onderkende beheersingsdoelstellingen (in de eerste kolom) opgenomen, evenals de relaties met de kwaliteitscriteria betrouwbaarheid (tweede, derde en vierde kolom) en continuïteit (vijfde kolom). Voor het koppelen van de beheersingsdoelstellingen aan de kwaliteitscriteria maakt CobIT

gebruik van een 'P' (Primair) en een 'S' (Secundair). 'Primair' houdt in dat de beheersingsdoelstelling direct van invloed is op een kwaliteitscriterium en in geval van 'Secundair' is de invloed op een kwaliteitscriterium beperkter of indirect. Alle beheersingsdoelstellingen waarachter een 'P' of een 'S' staat bij één of meer van de kwaliteitscriteria, maken deel uit van het totale begrip general IT controls. Uiteindelijk zal de concrete selectie van de beheersingsdoelstellingen afhankelijk zijn van de IT-objecten die binnen een organisatie worden gebruikt en de beheersingsdoelstellingen die hierbij relevant zijn.

Invulling van beoordeling van general IT controls in de praktijk

Op basis van de hiervoor omschreven gedachtegang en gebruikmakend van CobIT hebben wij een methode ontwikkeld waarmee, op basis van kwaliteitsaspecten en een risico-inschatting, inzichtelijk en onderbouwd invulling kan worden gegeven aan de planning van het beoordelen van general IT controls in het kader van de jaarrekeningcontrole. De methode beschrijven wij hierna.

Eerder in dit artikel hebben wij aangegeven op welke wijze de accountant inzicht verkrijgt in het belang van de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking, namelijk door de eerder omschreven risicoanalyse van het NIVRA. Met behulp van de resultaten van een dergelijke risicoanalyse kan vervolgens een selectie worden gemaakt van IT-objecten die relevant zijn voor de jaarrekeningcontrole. De accountant dient inzicht te verkrijgen in de opbouw en de afhankelijkheden van deze IT-objecten, al dan niet met behulp van een ingeschakelde IT-auditor. Het volledige inzicht in de opbouw van de IT-objecten leidt tot een volledige selectie van relevante onderzoeksobjecten. Om vervolgens de diepgang en omvang van de jaarrekeningcontrole naar de general IT controls te bepalen, dienen de beheersingsdoelstellingen voor de IT-processen aan de controleobjecten te worden gekoppeld. Hierbij geldt:

- een toename van de diversiteit aan typen onderzoeksobjecten leidt met name tot een grote omvang (meer general IT controls) van de controle;
- een toename in aantal van één type onderzoeksobject leidt met name tot meer diepgang (per general IT control gedetailleerder onderzoek, bijvoorbeeld met meer tests) van de controle.

In tabel 2 is een fictief voorbeeld uitgewerkt dat deze afhankelijkheden tussen de relevante general IT controls (zie tabel 1) en relevante objecten van onderzoek[1] inzichtelijk maakt. Overigens merken wij op dat de plaatsing van de '✓' in deze tabel louter illustratief en derhalve volkomen willekeurig is.

Relevante onderzoeksobjecten	Relevante general IT controls (CobIT-beheersingsdoelstellingen)							
	PO2	PO5	PO9	PO11	AI1	AI2	AI3	...
Pc				✓				
Server					✓		✓	
Database	✓							
Maatwerkpakket				✓			✓	
End user computing		✓	✓	✓				
Standaardpakket				✓				
Webapplicatie		✓						
Netwerk								
Batchproces						✓		
E-commerce		✓						
Rekencentrum			✓					
...								

Tabel 2. Selectie van general IT controls en onderzoeksobjecten.

Vanwege het feit dat binnen een controlejaar niet alle relevante general IT controls onderzoeksobjecten kunnen worden beoordeeld, dient ieder jaar opnieuw een selectie te worden gemaakt. Voor het maken van de selectie kan gebruik worden gemaakt van een balans tussen de diverse kwaliteitscriteria, waarbij tevens rekening wordt gehouden met de mate van invloed (Primair of Secundair) van de beheersingsdoelstellingen (de general IT controls) op de kwaliteitscriteria. Vervolgens kan bijvoorbeeld een meerjarencyclus worden ingesteld, waarbij onderscheid wordt gemaakt naar de volgende onderzoeken: het eerste jaar vindt een diepgaand onderzoek plaats, het tweede jaar een follow-up onderzoek en het derde jaar geen onderzoek.

Naast het hanteren van de bovengenoemde selectiemethode als methode om relevante IT-objecten van onderzoek en IT-beheersingsdoelstellingen vast te stellen in het kader van de jaarrekeningcontrole, dient de methode ook een ander doel. Vanuit de methodisch onderbouwde selectie zijn de IT-auditor en accountant in staat aan gebruikers en andere belanghebbenden voor het jaarrekeningproces uit te leggen waarom bepaalde onderzoeken noodzakelijk zijn. Dat komt doordat met deze selectiemethode een directe en gemotiveerde koppeling wordt aangebracht tussen jaarrekeningposten, de geautomatiseerde gegevensverwerking en general IT controls.

Conclusie

Uit eigen ervaring en vernomen ervaringen van vakgenoten merken wij dat er veel onduidelijkheid is over de precieze uitleg en benadering van begrippen als general IT controls, betrouwbaarheid en continuïteit, alsmede de afbakening van relevante IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole. Een oorzaak hiervan is het ontbreken van eenduidige literatuur, definities en gehanteerde terminologie. Daarnaast hebben op IT-gebied zodanige ontwikkelingen plaatsgevonden, dat de theorie niet meer volledig aansluit op de huidige prak-

1) Opgemerkt wordt dat de genoemde relevante objecten van onderzoek niet moeten worden gelezen als categorie-aanduiding, maar als specifieke objecten. Dit houdt in dat de genoemde objecten concreet benoemd dienen te worden, zoals server UX001, server W2K01, de database XYZ voor grootboek en het standaard-softwarepakket voor Electronic Banking.

tijk. Denk bijvoorbeeld aan het toepassen van e-business op steeds grotere schaal, waarbij handmatige handelingen nauwelijks meer voorkomen of waarbij organisaties gebruikmaken van elders – via het internet ter beschikking staande – opgestelde IT-toepassingen.

Ons inziens dienen beroepsorganisaties de vertaalslag tussen jaarrekeningposten, de geautomatiseerde gegevensverwerking en de general IT controls nader uit te werken en te actualiseren. Om invulling te geven aan deze vertaalslag pleiten wij voor het hanteren van een methodische benadering. Daardoor wordt het mogelijk te komen tot een inzichtelijke en onderbouwde selectie van IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole, waarmee de IT-auditor en de accountant verantwoording richting de cliënt en andere betrokkenen afleggen. Met dit artikel stellen wij een dergelijke methodische benadering voor en willen wij een bijdrage leveren aan de verdere professionalisering van het IT-vakgebied. Wij houden ons aanbevolen voor uw reacties en verdere discussie over dit belangrijke onderwerp!

Literatuur

[Boer04] J.C. de Boer en K.M. Lof, *Benchmarking op basis van standaarden als CobIT en Code voor Informatiebeveiliging*, Compact 2004/1.

[Cobi00] IT Governance Institute, *CobIT 3rd Edition*, 2000.

[Coum99] C.J. Coumou en J.W.R. Schoemaker, *Het managen van IT-risico's: over de onderhandelbaarheid van risico's en maatregelen*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Deck98] F.B.M. Deckers en J.C.E. van Kollenburg, *Elementaire theorie accountantscontrole*, 1998.

[Fijn00] Dr. R.G.A. Fijneman RE RA, *Automatiseringskennis bij accountants belicht of onderbelicht*, De Accountant, 2000.

[Hart00] Drs. S.J. Hartjes RE RA, *EDP-audit in het kader van de jaarrekeningcontrole*, in: Handboek EDP-auditing, C.6.1, 2000.

[Haye99] R. Hayes, A. Schilder, R. Dassen en P. Wallage, *Principles of Auditing*, 1999.

[Koop98] Mw. drs. A.J.M. Koopman, *Accountantscontrole, COSO en CobIT*, Compact 1998/2.

[Kort99] W. de Korte, *EDP-auditor en jaarrekeningcontrole van verregaand geautomatiseerde organisaties*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Neis01] Prof. A.W. Neisingh RE RA, *Ongedeelde verantwoordelijkheid RA ter discussie: IT-auditor krijgt (eindelijk) erkenning!*, Compact 2001/3.

[Neis02] Prof. A.W. Neisingh RE RA, *Accountantscontrole en informatietechnologie: 'bij elkaar deugen ze niet en van elkaar meugen ze niet'*, Compact 2002/4.

[Nivr82] NIVRA, Geschrift 26 Automatisering en controle deel IV, *Mededelingen door de Accountant met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking*, 1982.

[Nivr89] NIVRA, Geschrift 53 Automatisering en controle deel VII, *Kwaliteitsoordelen over informatievoorziening*, 1989.

[Nivr93] NIVRA, Geschrift 62 *Computercriminaliteit*, 1993.

[Nivr95] NIVRA, Studierapport 34 *Normatieve maatregelen voor de geautomatiseerde gegevensverwerking*, 1995.

[Nivr03] NIVRA, *Richtlijnen voor de Accountantscontrole*, 2003.

[Nore97] NOREA, Studierapport 2 *Een kwaliteitsmodel voor Register EDP-auditor*, 1997.

[Nore01] NOREA, Handleiding *ZekeRE-business*, 2001.

[Nore02] NOREA, Studierapport 3 *Raamwerk voor ontwikkeling normenstelsels en standaarden*, 2002.

[Zwar92] H. de Zwart RA, *Rapportering door EDP-auditors*, in: Handboek EDP-auditing, C.4.4, 1992.