

COBIT

Opkomst, ondergang en opleving van een raamwerk voor informatiebeheersing

Edo Roos Lindgreen

SAMENVATTING Interne beheersingsmaatregelen zoals voorgeschreven door de Sarbanes-Oxley Act en de Code Tabaksblat omvatten tal van maatregelen die aan informatietechnologie gerelateerd zijn. Of het nu gaat om autorisaties en logische toegangsbeveiliging of om maatregelen die de continuïteit van de financiële rapportagesystemen moeten waarborgen, 'information technology general controls' vormen een integraal onderdeel van het raamwerk voor interne beheersing. Dit artikel gaat in op het gebruik van COBIT voor de invulling van deze controls. Dit uitgebreide normenkader biedt organisaties een praktische basis voor het inrichten en toetsen van aan informatietechnologie gerelateerde beheersingsmaatregelen. Hiervoor is het in de meeste gevallen wel nodig de COBIT-normen op maat te snijden. Een praktische aanzet hiertoe is gedaan door het IT Governance Institute, de bedenkers van COBIT.

1 Inleiding

Er is al veel geschreven over de opkomst van corporate governance begin jaren negentig, het COSO-rapport, de veertig aanbevelingen van de commissie Peters, de val van Enron, Worldcom en Andersen, de Sarbanes-Oxley Act en de corporate governance code van de commissie Tabaksblat. De lezer zij verwezen naar de uitstekende artikelen die over dit onderwerp zijn verschenen; zie bijvoorbeeld Emanuels, Van Leeuwen en Wallage (2004) en Renes (2004). Hier volstaan wij met de algemeen aanvaarde constatering dat het inrichten van een raamwerk voor interne beheersing, zoals sectie 404 van de Sarbanes-Oxley Act en artikel II.1.4 van

Tabaksblat voorschrijven, impliceert dat ook op het gebied van informatietechnologie maatregelen worden getroffen. Interne beheersingsmaatregelen zijn immers in zeer veel gevallen ingebed in of worden ondersteund door geautomatiseerde informatiesystemen. Om welke maatregelen het daarbij gaat, is onder meer beschreven door Vaassen (2000), die ze samenvat onder de noemer *informatiecontrole*; een alternatieve term is *informatiebeheersing*. In het algemeen wordt onderscheid gemaakt tussen algemene maatregelen (general controls) die betrekking hebben op de infrastructuur en de bijbehorende processen voor ontwikkeling, beheer en beveiliging, en applicatiespecifieke maatregelen (application controls), die betrekking hebben op specifieke toepassingen; zie bijvoorbeeld Arens, Elder en Beasley (2005).

Grote ontwikkelingen hebben vaak interessante bijeffecten. Eén van de bijeffecten van de huidige interne beheersingsrage is de opleving van een raamwerk dat al bijkans het loodje had gelegd: de Control Objectives for Information and related Technology (COBIT). In dit raamwerk hopen organisaties nu een antwoord te vinden op de vraag welke IT-maatregelen zij moeten inrichten om aan de eisen van tegenwoordig te kunnen voldoen.

Zo'n wederopstanding vraagt om een nadere analyse. In dit artikel staan we stil bij de vragen: Hoe is COBIT ontstaan? Wat is COBIT en wat kunnen wij ermee? En hoe wordt COBIT in de praktijk gebruikt? Paragraaf 2 gaat in op de achtergrond van COBIT. Paragraaf 3 beschrijft het COBIT-normenkader zelf. In paragraaf 4 gaan wij in op de praktische toepasbaarheid van COBIT. Paragraaf 5 beschrijft enkele toepassingen van COBIT in de praktijk. Het artikel besluit met een aantal conclusies.

2 Achtergrond

In 1976 richt de internationale vereniging van IT-auditors, de Information Systems Audit and Control

Prof. Dr. E.E.O. Roos Lindgreen RE is partner bij KPMG Information Risk Management en hoogleraar IT & Auditing aan de Universiteit van Amsterdam.

Association (ISACA), in de Verenigde Staten een afzonderlijke stichting op. Deze stichting, de Information Systems Audit and Control Foundation (ISACF), wordt mede gefinancierd door het bedrijfsleven en heeft het ontwikkelen van producten op het gebied van de beheersing en de controle van informatietechnologie tot doel.

Twintig jaar later produceert de ISACF de zogeheten Control Objectives for Information and related Technology, ofwel CobiT, met een hoofdletter aan het begin en het eind en kleine letters ertussenin, een wat merkwaardige schrijfwijze die wij in dit artikel niet zullen aanhouden.

Volgens de opstellers ervan is COBIT niets minder dan een algemeen toepasbare en geaccepteerde standaard voor een goede beveiliging en beheersing van de informatievoorziening. De standaard biedt een referentiekader voor management, gebruikers, auditors, beheerders en beveiligingsdeskundigen.

Een gebrek aan diepgang kan de opstellers van de nieuwe standaard niet worden verweten. COBIT bestaat uit een set van vijf publicaties, waarin de volgende onderdelen worden onderkend: een raamwerk, de beheersingsdoelstellingen ('control objectives'), de controlerichtlijnen, een managementsamenvatting en een leidraad voor het management. De publicatie over beheersingsdoelstellingen specificeert maar liefst 34 doelstellingen, die zijn gegroepeerd in vier domeinen: planning en organisatie, acquisitie en implementatie, levering en ondersteuning en monitoring. Wij gaan hier zo nog op in.

In tegenstelling tot wat soms wordt gedacht of beweerd (Stuiveling, 2004), is COBIT niet direct verwant aan het bekende COSO-rapport¹. De klankovereenkomst suggereert een inhoudelijke verwantschap, maar eigenlijk hebben COSO en COBIT niet zoveel met elkaar te maken. Eerder is sprake van een gelijktijdige ontwikkeling, waarbij de ontwikkelaars van COBIT handig gebruik hebben gemaakt van de aanwezige aandacht voor corporate governance door een aantal definities uit COSO te adopteren om hun product een aanvullende legitimatie te verschaffen. Dezelfde handigheid zien wij in Lainhart (1998) en andere artikelen, waarin zowat de hele wereld als inspiratiebron voor COBIT wordt genoemd. Volgens Lainhart is COBIT gebaseerd op ISO, EDIFACT, OECD, ISACA, ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, COSO, IFAC, IIA, AICPA, GAO, PCIE, ISACA, ESF, I4, IBAG, NIST en DTF. Zelfs de minder ingewijde lezer zal de beperkte rationaliteit van deze optisch indrukwekkende reeks aanvoelen.

Al die kunstmatige draagvlakverbreding levert bij de uitrol van COBIT in 1996 niet het gehoopte succes op. Aanvankelijk wordt COBIT wel gebruikt door enkele grote ondernemingen en overheidsinstellingen voor het plannen en structureren van de IT-auditwerkzaamheden. Een aantal auditafdelingen baseert het meerjarig IT-auditplan op de processen en objecten uit COBIT. Maar op het hoogtepunt van de internethype zit de oververhitte IT-sector bepaald niet te wachten op doorwrochte standaarden waarin 34 beheersingsdoelstellingen nu eens even stevig worden neergezet; time-to-market is op dat moment belangrijker dan interne beheersing. Algemeen geaccepteerd raakt de standaard dan ook niet en aan het begin van de eenentwintigste eeuw dreigt COBIT in de vergetelheid weg te zakken.

Totdat Enron valt, Sarbanes en Oxley hun inmiddels beroemde wetsvoorstel indienen en interne beheersing opnieuw op de kaart wordt gezet. Zoals bekend schrijft sectie 404 van Sarbanes-Oxley onder meer voor dat elke in de Verenigde Staten aan de effectenbeurs genoteerde onderneming over een raamwerk voor interne beheersing dient te beschikken. Niet iedereen realiseert zich op dat moment dat ook informatietechnologie hierin een rol zal spelen. En voor wie wel een idee heeft, blijft deze rol vooralsnog vaag.

Op 9 maart 2004 publiceert de Public Company Accounting Oversight Board (PCAOB), het orgaan dat toezicht houdt op accountants in het kader van de naleving van de Sarbanes-Oxley Act, de Auditing Standard No. 2, getiteld 'An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements'. Kern van deze standaard is dat de externe accountant de jaarrekeningcontrole en de beoordeling van de interne beheersing gelijktijdig dient uit te voeren, waarbij strenge eisen worden gesteld aan de wijze waarop deze beoordeling dient plaats te vinden. Bovendien stelt de standaard dat interne beheersing mede afhankelijk is van beheersingsmaatregelen in en rond informatietechnologie, zodat ook deze beoordeeld dienen te worden. Welke maatregelen dit zijn, specificeert Auditing Standard No. 2 helaas niet; wel worden in een bijzin enkele algemene categorieën van deze 'information technology general controls' als nogal willekeurig voorbeeld gegeven – maatregelen inzake programmaontwikkeling, wijzigingen, bediening en toegang tot programma's en gegevens. Kortom, het beeld wordt al iets minder vaag, maar van werkelijke helderheid is nog geen sprake.

De ISACF, in 1998 omgedoopt tot het IT Governance Institute, grijpt zijn kans. In april 2004 publiceert het instituut het document 'IT Control Objectives for Sarbanes-Oxley'. Bij het ontwikkelen van dit document wordt een select aantal beheersingsdoelstellingen uit COBIT afgebeeld op de voorbeelden uit de Auditing Standard No. 2, en worden de resulterende doelstellingen weer afgebeeld op het raamwerk voor interne beheersing zoals wij dat kennen uit COSO. Het is dit document dat de basis zal vormen voor de wederopstanding van COBIT, zij het in sterk vereenvoudigde vorm.

3 COBIT

Het COBIT-raamwerk is gebaseerd op drie dimensies. De eerste dimensie bestaat uit zeven bekende kwaliteitskenmerken van informatie en informatiesystemen, information criteria gedoopt: effectiviteit, efficiency, vertrouwelijkheid, integriteit, beschikbaarheid, naleving en betrouwbaarheid. Afgezien van de overlap tussen integriteit en betrouwbaarheid valt hier weinig op aan te merken.

De tweede dimensie bestaat uit vijf categorieën van informatiemiddelen: gegevens, applicatiesystemen, technologie, faciliteiten en mensen. Ook hier is weinig tegenin te brengen.

De derde dimensie bestaat uit vier domeinen, waarbinnen beheersingsmaatregelen kunnen worden gegroepeerd: (i) de planning en organisatie van de inzet van informatietechnologie, (ii) de acquisitie en implementatie van informatiesystemen, (iii) de levering van IT-diensten en de ondersteuning daarbij, en (iv) de bewaking van de voorgaande drie domeinen. De domeinen in deze dimensie komen op een logische manier overeen met de verschillende fasen in de levenscyclus van informatiesystemen: strategie en planning, ontwikkeling en invoering, en productie en onderhoud.

Binnen elk van de onderscheiden domeinen binnen de derde dimensie definieert COBIT een aantal imperatief gestelde beheersingsdoelstellingen op procesniveau. In totaal zijn er 34 beheersingsdoelstellingen op procesniveau; zie tabel 1 voor een vrij vertaald overzicht. De individuele beheersingsdoelstellingen zijn alleszins redelijk te noemen en sluiten goed aan op algemeen aanvaarde standaarden als de Information Technology Infrastructure Library (ITIL) of de Code voor Informatiebeveiliging (ISO/IEC 17799).

De 34 beheersingsdoelstellingen op procesniveau worden vervolgens verder uitgewerkt in doelstellin-

Tabel 1. Beheersingsdoelstellingen in COBIT (vrij vertaald)

Planning en Organisatie

- PO1. Definieer een strategisch IT-plan.
- PO2. Definieer de informatie-architectuur.
- PO3. Bepaal de technologische koers.
- PO4. Definieer de IT-organisatie en de bijbehorende relaties.
- PO5. Beheers de IT-investering.
- PO6. Communiceer de doelstellingen en de koers van het management.
- PO7. Beheers personele zaken.
- PO8. Zorg voor naleving van externe vereisten.
- PO9. Onderzoek relevante risico's.
- PO10. Beheers projecten.
- PO11. Beheers kwaliteit.

Acquisitie en Implementatie

- AI1. Identificeer mogelijke oplossingen voor het ondersteunen van de bedrijfsvoering.
- AI2. Acquireer en onderhoud de applicatiesoftware.
- AI3. Acquireer en onderhoud de technische infrastructuur.
- AI4. Ontwikkel en onderhoud procedures.
- AI5. Installeer en accrediteer systemen.
- AI6. Beheers wijzigingen.

Levering en Ondersteuning

- DS1. Definieer en beheers dienstenniveaus.
- DS2. Beheers diensten die door derden worden geleverd.
- DS3. Beheers prestaties en capaciteit.
- DS4. Zorg voor continue dienstverlening.
- DS5. Waarborg de systeemveiligheid.
- DS6. Identificeer de kosten en wijs deze toe.
- DS7. Leid gebruikers op.
- DS8. Assisteer en adviseer klanten.
- DS9. Beheers de configuratie.
- DS10. Beheers problemen en incidenten.
- DS11. Beheers gegevens.
- DS12. Beheers faciliteiten.
- DS13. Regel de dagelijkse bediening.

Bewaking

- M1. Bewaak de processen.
- M2. Beoordeel de effectiviteit van de interne beheersing.
- M3. Verkrijg zekerheid door het inschakelen van een onafhankelijke derde.
- M4. Zorg voor een onafhankelijke beoordeling.

gen op het niveau van activiteiten. Een groot aantal maatregelen is het gevolg; in totaal telt het raamwerk honderden maatregelen, die zijn gedocumenteerd in een document van maar liefst 155 pagina's (ITGI, 2000). Tenslotte definieert COBIT een verzameling algemene auditrichtlijnen, plus 34 specifieke audit-

richtlijnen die corresponderen met de beheersingsdoelstellingen op procesniveau.

Zoals gezegd vormt COBIT de basis voor de IT Control Objectives for Sarbanes-Oxley van het IT Governance Institute. Dit document is tot stand gekomen door het oude raamwerk uit 1996 sterk in omvang te reduceren. Allereerst zijn alleen die beheersingsdoelstellingen uit COBIT geselecteerd, die nodig zijn voor de financiële rapportage. Daarbij is een groot aantal minder relevant geachte beheersingsdoelstellingen uit COBIT geschrapt of ingeruild voor een simpele vragenlijst. Op andere punten is het document uitgebreid ten opzichte van COBIT, bijvoorbeeld met nuttige suggesties voor het beoordelen van beheersingsmaatregelen ('tests of controls'). Ten slotte werd de structuur van het document gebaseerd op de hierboven genoemde voorbeelden van de 'IT general controls' in de PCAOB Auditing Standard No. 2. Of dit een briljante keuze is, valt te betwisten. De voorbeelden in de PCAOB-standaard hebben een nogal arbitrair karakter; de originele COBIT-domeinen lijken beter doordacht.

4 Praktische toepasbaarheid

Het bovenstaande roept de vraag op: hoe toepasbaar is COBIT nu in de praktijk? Het antwoord op deze vraag is afhankelijk van de beoogde toepassingen en vooral van degenen die COBIT toepassen: managers, accountants en operational auditors, IT-managers en IT-auditors.

Voor de meeste *managers* is COBIT een grote onbekende. Dat is jammer, omdat de 34 beheersingsdoelstellingen van COBIT niet alleen een uitstekende basis, maar in feite zelfs een minimumeis vormen voor het inrichten van de 'IT governance'. Elke zichzelf respecterende onderneming zal deze 34 beheersingsdoelstellingen willen realiseren. Dit betekent niet dat alle uit de beheersingsdoelstellingen voortvloeiende maatregelen in alle diepgang hoeven worden ingevoerd. Het is aan de organisatie een evenwichtige keuze te maken uit de maatregelen die nodig zijn om zo efficiënt mogelijk aan de beheersingsdoelstellingen te kunnen voldoen.

Ook *accountants* en *operational auditors* zouden hun voordeel met COBIT kunnen doen; zij ervaren het normenkader in de praktijk echter niet alleen als te omvangrijk, maar vooral ook als te technisch. De 34 beheersingsdoelstellingen van COBIT zullen de gemiddelde IT-auditor op zichzelf niet veel problemen opleveren, maar voor een accountant of opera-

tional auditor zijn Service Level Agreements, netwerkbeveiliging of capaciteitsmanagement nu eenmaal geen dagelijkse kost. Dit maakt COBIT minder geschikt voor het beoordelen van IT general controls door de accountant of operational auditor zelf.

Ook door *IT-managers* wordt COBIT niet met gejuich ontvangen. Het raamwerk sluit niet goed aan op de bestaande werkprocessen in de IT-sector, die vaak zeer pragmatisch en informeel van aard zijn. Veel IT-managers zijn ook nog niet overtuigd van het belang van interne beheersingsmaatregelen waarvan de betrouwbare werking hard kan worden aangetoond. Veel IT-professionals herkennen zich tenslotte niet in het gehanteerde jargon en vinden het hele raamwerk eigenlijk maar overbodige bureaucratie.

Dus blijven de *IT-auditors* over. Dat zij redelijk met COBIT uit de voeten kunnen, is niet verwonderlijk; het raamwerk is immers door henzelf voortgebracht. Toch blijkt COBIT ook voor veel IT-auditors erg complex en omvangrijk. De driedimensionale indeling maakt het mogelijk beheersingsmaatregelen vanuit verschillende perspectieven te bezien, maar wekt ook verwarring. In de praktijk wordt daarom meestal de derde dimensie gebruikt, de indeling volgens de beheersingsdomeinen. Om COBIT werkelijk praktisch toepasbaar te maken, is het nodig de omvang en de complexiteit van het normenkader verder te reduceren door de maatregelen op maat te snijden en aan te passen aan de specifieke situatie.

Wordt COBIT vergeleken met andere normenkaders voor beheersingsmaatregelen, zoals de Code voor Informatiebeveiliging (ISO 17799) of de Information Technology Infrastructure Library (ITIL), dan blijkt dat COBIT niet alleen goed op deze standaarden aansluit, maar deze ook in ruime mate overdekt (Leicester, 2001).

5 Toepassingen in de praktijk

In hoeverre worden COBIT, respectievelijk de IT Control Objectives for Sarbanes-Oxley in de praktijk toegepast? Hiervan bestaat helaas geen volledig beeld. Uit recent wereldwijd onderzoek van het IT Governance Institute en PricewaterhouseCoopers onder 335 topmanagers blijkt dat 5% van de onderzochte organisaties COBIT gebruikt (ITGI, 2004). De acceptatiegraad van COBIT lijkt hiermee beperkter dan bijvoorbeeld die van de Code voor Informatiebeveiliging ofwel ISO/IEC 17799, die rond de 20% bedraagt (KPMG, 2002). In Nederland gebruikt een aantal grote ondernemingen en instel-

lingen COBIT voor het structureren van interne auditwerkzaamheden; voorbeelden zijn PGGM (Van Bommel en Van Goor, 2004) en UWV (Van Staveren, 2002). Andere ondernemingen gebruiken COBIT als basis voor het inrichten van het stelsel van informatiebeheersingsmaatregelen dat tegenwoordig ook wel met de term IT-governance wordt aangeduid. Voorbeelden hiervan zijn Philips (Van Gils, 2001) en Fortis en Akzo Nobel (NOREA, 2004). Daarnaast wordt COBIT onder meer toegepast voor het ontwikkelen van self assessments en normenkaders voor IT-auditors; zie bijvoorbeeld (Van der Geest en Mantelaers, 2004). Een groot aantal bedrijven en instellingen gebruikt COBIT niet direct, maar neemt er kennis van, zoals zij kennisnemen van andere relevante standaarden. Verder is de term COBIT een onmisbaar bestanddeel in de marketingmix van adviesbureaus, softwareleveranciers, accountantskantoren en andere partijen die mee-eten uit de interne beheersingsruif. De conclusie is dat er veel over COBIT wordt gepraat, maar dat er eigenlijk nog niet zo heel veel mee wordt gedaan.

Dit kan veranderen door de impact van Sarbanes-Oxley, de PCAOB Auditing Standard No. 2 en de IT Control Objectives van het IT Governance Institute. Grote ondernemingen hebben dit laatste document inmiddels geadopteerd voor het inrichten van de IT general controls om een efficiënte audit mogelijk te maken. De grote accountantskantoren hebben het document gebruikt als basis voor de werkinstructies voor accountants die de integrated audit conform PCAOB Auditing Standard No. 2 moeten uitvoeren bij ondernemingen die onder de Sarbanes-Oxley Act vallen. Het ligt voor de hand te veronderstellen dat deze 'working papers' ook zullen doorsijpelen naar de accountantscontrole van ondernemingen die niet onder de Sarbanes-Oxley Act vallen. Dan wordt er wellicht niet meer alleen over COBIT gepraat, maar ook mee gewerkt. Vanzelfsprekend is dit echter niet. Volgens sommige deskundigen hebben de IT Control Objectives ervoor gezorgd dat het uitgebreide COBIT-normenstelsel niet meer wordt gebruikt en voorgoed in de vergetelheid zal geraken. De tijd zal het leren. De ervaringen met ISO 17799 en ITIL hebben uitgewezen dat de introductie van een korte, pragmatische lijst met 'key controls' de drempel voor het toepassen van een normenkader kan verlagen en hierdoor de acceptatie van het normenkader zelf kan stimuleren. De IT Control Objectives zijn in ieder geval toegankelijk genoeg om communicatie en discussie over dit onderwerp op gang te brengen (Duijs, 2005).

6 Conclusies

De Sarbanes-Oxley Act en de PCAOB Auditing Standard No. 2 hebben geleid tot een hernieuwde belangstelling voor COBIT, een raamwerk voor de beheersing van informatietechnologie uit de vorige eeuw. COBIT zelf is een uitgebreid, doch bruikbaar raamwerk, dat op bescheiden schaal integraal wordt toegepast. Een op maat gesneden versie van COBIT, de IT Control Objectives for Sarbanes-Oxley, is in korte tijd breed geaccepteerd en mag zich in een grote populariteit verheugen. De term COBIT is het afgelopen jaar uitgegroeid tot een heus 'buzzword' dat ook buiten de wereld van de IT-auditing rond zingt. Dit zal de opmars van dit raamwerk en zijn afgeleiden zonder enige twijfel verder stimuleren.

Voor integrale toepassing is COBIT in veel gevallen te omvangrijk. Het normenkader kan dan ook vooral dienen als basis voor het inrichten van de informatiebeheersing nadat het op maat is gesneden en is aangepast aan de specifieke eisen van de organisatie. Ontdaan van onnodige dimensies en teruggebracht tot zijn essentie is COBIT een volledig, evenwichtig en actueel raamwerk dat een wederopstanding verdient. ■

Literatuur

- Arens, A.A., R.J. Elder en M.S. Beasley, (2005), *Auditing and Assurance Services – An Integrated Approach*, Tenth Edition, Pearson Education.
- Bommel, C.F. van en H.M. van Goor, (2004), IT-auditing in het kader van de jaarrekeningcontrole?, in: *Compact*, jg. 31, no. 2, pp. 10-16.
- Dassen, R., S.J. Maijor en Ph. Wallage, (2002), *Control & Assurance*, Reed Business Information.
- Duijs, I., (2005), *IT Control Objectives for Sarbanes-Oxley*, personal communication, Universiteit van Amsterdam.
- Emanuels, J., O. van Leeuwen en Ph. Wallage, (2004), Internal Control volgens Sarbanes-Oxley, in: *Maandblad voor Accountancy en Bedrijfs-economie*, jg. 78, no. 7/8, pp. 348-356.
- Ernst & Young (2004), *Global Information Security Survey*, [http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/\\$file/2004_Global_Information_Security_Survey_2004.pdf](http://www.ey.com/global/download.nsf/Austria/2004_global_info_sec_survey/$file/2004_Global_Information_Security_Survey_2004.pdf)
- Geest, H. van der en P. Mantelaers, (2004), De hand in eigen boezem – Europese rekenkamers bepalen hun IT-volwassenheidsniveau, in: *EDP-Auditor*, no. 4, pp. 6-11.
- Gils, A. van, (2001), Implementation of the COBIT-3 Maturity Model in Royal Philips Electronics, in: Gertz, M., E. Guldentops en L. Strous (eds.), *Integrity, Internal Control and Security in Information Systems: Connecting Governance and Technology*, IFIP TC11/WG11.5 Fourth Working Conference on Integrity, Internal Control and Security in Information Systems, 2001, Brussels, nov. 15-16, pp. 161-174.
- IT Governance Institute, (2000), COBIT, *Third Edition – Control Objectives*, www.itgi.org.
- IT Governance Institute, (2004), *IT Governance Global Status Report*, 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.
- KPMG, (2002), *Global Information Security Survey*, <http://www.kpmg.com/microsite/informationsecurity/pdf/giss.pdf>,
- Lainhart IV, J.W., (1998), *COBIT: An International Source For Information Technology Controls*, www.isaca.org.
- Leicester, E.F., (2001), *In welke mate sluiten ITIL en COBIT op elkaar aan?*, afstudeerscriptie, Universiteit van Amsterdam.
- Nederlandse Orde van Register EDP-Auditors, (2004), *IT-Governance – een verkenning*, <http://www.norea.nl/download/IT%20Governance.pdf>.
- Public Company Accounting Oversight Board, (2004), *Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, http://www.pcaobus.org/Rules_of_the_Board/Documents/Rules_of_the_Board/Auditing_Standard_2.pdf.
- Renes, R., (2004), Zonder interne beheersing geen corporate governance, in: *Accounting*, jg. 108, no. 9, pp. 20-26.
- Staveren, B.J. van, (2002), *COBIT in de praktijk bij UWV*, lezing voor het Platform Informatiebeveiliging, Utrecht, 19 maart.
- Stuiveling, S.J., (2004), Even bijpraten, lezing op het congres *Een beetje integer bestaat niet*, Centrum voor Arbeidsverhoudingen (CAOP), Den Haag, 24 mei.
- Vaassen, E. en E. Roos Lindgreen, (2000), Informatiecontrole en e-business, in: *Tijdschrift voor Bedrijfsadministratie*, jg. 104, no. 1237, pp. 407-412.

Noten

- 1 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) werd in 1985 opgericht om de Amerikaanse National Commission on Fraudulent Financial Reporting te steunen. Deze National Commission, geleid door James C. Treadway, Jr., had tot doel om de factoren te onderzoeken die kunnen leiden tot fraude in financiële verslaggeving. COSO bestaat uit de volgende beroepsorganisaties: the American Institute of Certified Public Accountants (AICPA), the American Accounting Association (AAA), the Financial Executives International (FEI), the Institute of Internal Auditors (IIA) en the Institute of Management Accountants (IMA). De belangrijkste en bekendste publicatie van COSO is het COSO-rapport uit 1992; zie Dassen, Maijor en Wallage (2002) voor een goede samenvatting en behandeling van dit rapport.
- 2 Deze opsomming bestaat uit een bonte mengeling van beroepsorganisaties, commerciële ondernemingen en internationale samenwerkingsverbanden, alsmede standaarden en referentiedocumenten voor uiteenlopende zaken als informatiebeveiliging, IT-beheer, kwaliteitszorg, enzovoort, en zegt weinig meer dan dat de opstellers van COBIT zich breed hebben georiënteerd.